(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월11일
(11) 등록번호 10-2190268
(24) 등록일자 2020년12월07일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/102 (2013.01)
H04L 63/083 (2013.01)
(21) 출원번호 10-2019-0071542
(22) 출원일자 2019년06월17일
심사청구일자 2019년06월17일
(56) 선행기술조사문헌
US20070094716 A1*
오세라 외 1인, '이종 사물인터넷 플랫폼 간 보안 상호운용을 위한 프레임워크', KIPS transactions on computer and communication systems 컴퓨터 및 통신 시스템 v.7 no.3, 2018년, pp.81 - 90 (2018.03.31.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
김영갑
서울특별시 광진구 능동로 209, 세종대학교 행복기숙사 220호(군자동)
오세라
서울특별시 광진구 능동로 209, 세종대학교 율곡관 702호(군자동)
(74) 대리인
양성보

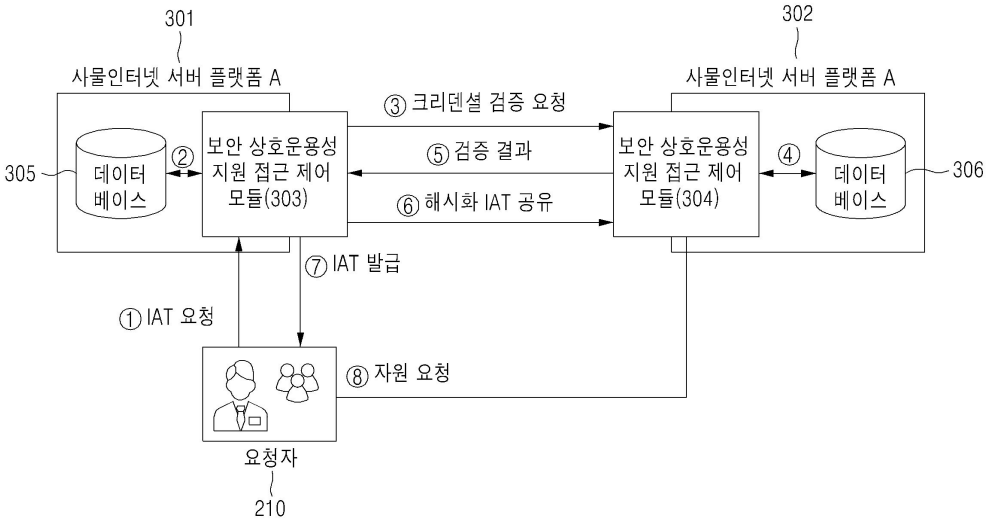
전체 청구항 수 : 총 11 항 심사관 : 오수정

(54) 발명의 명칭 **이종 사물인터넷 플랫폼을 위한 보안 상호운용성 지원 접근 제어 프레임워크**

(57) 요 약

이종 사물인터넷 플랫폼을 위한 보안 상호운용성 지원 접근 제어 프레임워크가 개시된다. 일 실시예에 따른 상호운용성 지원 접근 제어 방법은, 접근 제어를 위한 계층을 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 단계; 및 상기 가상화된 계층에 기반한 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 이종의 사물인터넷 플랫폼 간에 상호운용성을 지원하는 단계를 포함할 수 있다.

대 표 도



(52) CPC특허분류
H04L 63/0876 (2013.01)

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

상호운용성 지원 접근 제어 방법에 있어서,

접근 제어를 위한 계층을 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 단계; 및

상기 가상화된 계층에 기반한 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 이종의 사물인터넷 서버 플랫폼 간에 상호운용성을 지원하는 단계

를 포함하고,

상기 상호운용성을 지원하는 단계는,

상기 사물인터넷 서버 플랫폼에서 상호운용 접근 토큰(IAT)을 기반으로 상호운용성을 지원하고, 상기 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 ACMD(Authorization Code for Multiple Domains), IMD(Implicit for Multiple Domains), MROPC(Multiple Resource Owners' Password Credentials), MCC(Multiple Clients' Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급하고, 요청자로부터 복수 개의 사물인터넷 서버 플랫폼에 등록한 요청자의 크리덴셜을 이용하여 상기 복수 개의 사물인터넷 서버 플랫폼에 접근 가능한 권한을 가진 상호운용 접근 토큰(IAT)을 요청하고, 제1 사물인터넷 서버 플랫폼이 상기 요청자로부터 전달된 크리덴셜 중 상기 제1 사물인터넷 서버 플랫폼의 크리덴셜을 검증하고, 상기 제1 사물인터넷 서버 플랫폼에서 상기 요청자로부터 전달된 크리덴셜 중 제2 사물인터넷 서버 플랫폼으로 크리덴셜 검증 요청을 전송함에 따라 상기 제2 사물인터넷 서버 플랫폼에서 상기 제1 사물인터넷 서버 플랫폼으로부터 전송된 크리덴셜을 검증하여 상기 제1 사물인터넷 서버 플랫폼에게 크리덴셜 검증을 수행한 크리덴셜 검증 결과를 전달하고, 상기 제1 사물인터넷 서버 플랫폼에서 상기 제1 사물인터넷 서버 플랫폼과 상기 제2 사물인터넷 서버 플랫폼에 접근 가능한 글로벌 접근 범위를 가진 상호운용 접근 토큰(IAT)을 생성하고, 상기 제1 사물인터넷 서버 플랫폼 또는 상기 제2 사물인터넷 서버 플랫폼에서의 크리덴셜 검증 결과에 따라 자원에 접근 가능한 영역이 제한되고, 상기 제1 사물인터넷 서버 플랫폼에서 요청자에게 상기 제1 사물인터넷 서버 플랫폼 또는 상기 제2 사물인터넷 서버 플랫폼 중 어느 하나 이상의 사물인터넷 서버 플랫폼에 접근 가능한 상호운용 접근 토큰(IAT)을 발급하고, 상기 발급된 상호운용 접근 토큰(IAT)을 상기 요청자에게 전달하고, 상기 요청자로부터 상기 제1 사물인터넷 서버 플랫폼으로부터 발급받은 상호운용 접근 토큰(IAT)을 기반으로 상기 제1 사물인터넷 서버 플랫폼 또는 제2 사물인터넷 서버 플랫폼에 접근되는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 2

제1항에 있어서,

상기 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 단계는,

인증(Authentication), 인가(Authorization), 감사(Auditing)의 접근 제어를 위한 계층을 하나의 계층으로 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 상기 사물인터넷 서버 플랫폼에 제공하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

제1항에 있어서,

상기 상호운용성을 지원하는 단계는,

A3FaaS(A3 Framework as a Service)를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 ACMD(Authorization Code for Multiple Domains)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 11

제10항에 있어서,

상기 상호운용성을 지원하는 단계는,

클라이언트로부터 접근하기 위한 자원들이 명시되어 상호운용 접근 토큰(IAT)의 발급이 요청됨에 따라 상기 접근을 요청한 자원에 대한 권한을 획득하기 위해 자원 소유자들의 허가를 획득하고, 상기 획득된 허가를 A3 서버에게 전송하고, 상기 A3 서버에서 상기 클라이언트로부터 전송된 허가들을 검증을 수행한 검증 결과를 통하여 상기 클라이언트에게 인가 코드를 발급하고, 상기 클라이언트에서 상기 A3로부터 발급받은 인가 코드를 다시 상기 A3 서버에게 전달하고, 상기 A3서버에서 상기 클라이언트로부터 전달받은 인가 코드를 검증한 뒤, 상기 클라이언트에게 상호운용 접근 토큰(IAT)을 발급하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 12

제1항에 있어서,

상기 상호운용성을 지원하는 단계는,

A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 IMD(Implicit for Multiple Domains)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 13

제12항에 있어서,

상기 상호운용성을 지원하는 단계는,

클라이언트로부터 요청된 자원의 접근 범위와 상호운용 접근 토큰(IAT)을 발급받을 리다이렉션 URI가 전달됨에 따라 로그인 과정을 통하여 상기 요청된 자원의 접근 범위에 대한 권한을 획득하기 위하여 자원 소유자들의 허

가를 받고, 상기 허가를 A3 서버에 전달하고, 상기 A3 서버에서 상기 클라이언트로부터 요청된 자원, 상기 요청된 자원이 위치한 도메인의 상호운용 정책 및 상기 요청된 자원의 크리덴셜을 검증한 뒤, 상기 클라이언트에게 상호운용 접근 토큰(IAT)을 전달하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 14

제1항에 있어서,

상기 상호운용성을 지원하는 단계는,

A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 MROPC(Multiple Resource Owners' Password Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 15

제14항에 있어서,

상기 상호운용성을 지원하는 단계는,

클라이언트로부터 기 저장된 자원 소유자들의 크리덴셜 또는 자원을 요청하기 위한 자원 소유자들의 크리덴셜들을 전달받고, 요청된 자원의 접근 범위 및 상기 자원 소유자 크리덴셜을 A3 서버에 전송하고, 상기 A3 서버에서 상기 클라이언트로부터 요청된 자원의 접근 범위와 상기 자원 소유자 크리덴셜을 검증하여 상호운용 접근 토큰(IAT)을 발급하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 16

제1항에 있어서,

상기 상호운용성을 지원하는 단계는,

A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 MCC(Multiple Clients' Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 17

제1항에 있어서,

상기 상호운용성을 지원하는 단계는,

클라이언트에서 자원의 접근 범위와 관련된 클라이언트들의 크리덴셜들을 A3 서버에 전달하고, 상기 A3 서버에서 전달된 클라이언트 크리덴셜들을 검증하고, 상기 자원의 접근 범위를 갱신한 뒤 상호운용 접근 토큰(IAT)을 발급하는 단계

를 포함하는 상호운용성 지원 접근 제어 방법.

청구항 18

상호운용성 지원 접근 제어를 위한 제어 시스템에 있어서,

접근 제어를 위한 계층을 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 프레임워크 제공부; 및

상기 가상화된 계층에 기반한 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 이종의 사물인터넷 서버 플랫폼 간에 상호운용성을 지원하는 상호운용성 지원부

를 포함하고,

상기 상호운용성 지원부는,

상기 사물인터넷 서버 플랫폼에서 상호운용 접근 토큰(IAT)을 기반으로 상호운용성을 지원하고, 상기 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 ACMD(Authorization Code for Multiple Domains), IMD(Implicit for Multiple Domains), MROPC(Multiple Resource Owners' Password Credentials), MCC(Multiple Clients' Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급하고, 요청자로부터 복수 개의 사물인터넷 서버 플랫폼에 등록한 요청자의 크리덴셜을 이용하여 상기 복수 개의 사물인터넷 서버 플랫폼에 접근 가능한 권한을 가진 상호운용 접근 토큰(IAT)을 요청하고, 제1 사물인터넷 서버 플랫폼이 상기 요청자로부터 전달된 크리덴셜 중 상기 제1 사물인터넷 서버 플랫폼의 크리덴셜을 검증하고, 상기 제1 사물인터넷 서버 플랫폼에서 상기 요청자로부터 전달된 크리덴셜 중 제2 사물인터넷 서버 플랫폼으로 크리덴셜 검증 요청을 전송함에 따라 상기 제2 사물인터넷 서버 플랫폼에서 상기 제1 사물인터넷 서버 플랫폼으로부터 전송된 크리덴셜을 검증하여 상기 제1 사물인터넷 서버 플랫폼에게 크리덴셜 검증을 수행한 크리덴셜 검증 결과를 전달하고, 상기 제1 사물인터넷 서버 플랫폼에서 상기 제1 사물인터넷 서버 플랫폼과 상기 제2 사물인터넷 서버 플랫폼에 접근 가능한 글로벌 접근 범위를 가진 상호운용 접근 토큰(IAT)을 생성하고, 상기 제1 사물인터넷 서버 플랫폼 또는 상기 제2 사물인터넷 서버 플랫폼에서의 크리덴셜 검증 결과에 따라 자원에 접근 가능한 영역이 제한되고, 상기 제1 사물인터넷 서버 플랫폼에서 요청자에게 상기 제1 사물인터넷 서버 플랫폼 또는 상기 제2 사물인터넷 서버 플랫폼 중 어느 하나 이상의 사물인터넷 서버 플랫폼에 접근 가능한 상호운용 접근 토큰(IAT)을 발급하고, 상기 발급된 상호운용 접근 토큰(IAT)을 상기 요청자에게 전달하고, 상기 요청자로부터 상기 제1 사물인터넷 서버 플랫폼으로부터 발급받은 상호운용 접근 토큰(IAT)을 기반으로 상기 제1 사물인터넷 서버 플랫폼 또는 제2 사물인터넷 서버 플랫폼에 접근되는

제어 시스템.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 이종 사물인터넷 플랫폼을 위한 보안 상호운용성 지원 접근 제어 기술에 관한 것이다.

배 경 기 술

[0003] 사물인터넷(Internet of Things; IoT)이 미래에 중요한 기술로써 각광받으면서 Watson IoT, IoTivity, ARTIK 등의 사물인터넷 플랫폼이 개발되고 있으며, 각 플랫폼 내의 자원을 보호하기 위한 접근 제어(인증 및 인가) 프레임워크 또한 개별적으로 개발되고 있다. 하지만, 접근 제어 프레임워크들은 어디까지나 각 사물인터넷 플랫폼에서 사용되는 것을 가정하여 개발되고 있으며 이종의 사물인터넷 플랫폼들 간의 상호운용성은 고려되고 있지 않다. 예를 들어, 현재는 다섯 가지의 사물인터넷 플랫폼 내에 존재하는 자원을 이용하고 싶다면 해당 플랫폼들에서 요구하는 각각의 인증 및 인가 과정을 거친 후 자원을 이용해야 하는 문제가 존재한다. 이는 초연결성(Hyper-Connectivity)이 강조되는 사물인터넷 환경에서는 향후 해결되어야 할 중요한 이슈 중 하나이다.

발명의 내용

해결하려는 과제

[0005] 접근 제어를 위한 계층을 가상화하여 다양한 사물인터넷 플랫폼에 공통적으로 보안 상호운용성 지원 접근 제어 프레임워크를 제공할 수 있다.

[0006] 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 이종의 사물인터넷 플랫폼 간에 상호운용성을 지원할 수 있다.

과제의 해결 수단

[0008] 상호운용성 지원 접근 제어 방법은, 접근 제어를 위한 계층을 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 단계; 및 상기 가상화된 계층에 기반한 보안 상호운용성 지원 접근 제어 프레임워크를 통하여

이종의 사물인터넷 플랫폼 간에 상호운용성을 지원하는 단계를 포함할 수 있다.

[0009] 상기 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 단계는, 인증(Authentication), 인가(Authorization), 감사(Auditing)의 접근 제어를 위한 계층을 하나의 계층으로 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 상기 사물인터넷 서버 플랫폼에 제공하는 단계를 포함할 수 있다.

[0010] 상기 상호운용성을 지원하는 단계는, 상기 사물인터넷 서버 플랫폼에서 상호운용 접근 토큰(Interoperable Access Token; IAT)을 기반으로 상호운용성을 지원하는 단계를 포함할 수 있다.

[0011] 상기 상호운용성을 지원하는 단계는, 상기 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 MCC(Multiple Clients' Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0012] 상기 상호운용성을 지원하는 단계는, 요청자로부터 복수 개의 사물인터넷 서버 플랫폼에 등록한 요청자의 크리덴셜을 이용하여 상기 복수 개의 사물인터넷 서버 플랫폼에 접근 가능한 권한을 가진 상호운용 접근 토큰(IAT)을 요청하는 단계를 포함할 수 있다.

[0013] 상기 상호운용성을 지원하는 단계는, 제1 사물인터넷 서버 플랫폼이 상기 요청자로부터 전달된 크리덴셜 중 상기 제1 사물인터넷 서버 플랫폼의 크리덴셜을 검증하고, 상기 제1 사물인터넷 서버 플랫폼에서 상기 요청자로부터 전달된 크리덴셜 중 제2 사물인터넷 서버 플랫폼으로 크리덴셜 검증 요청을 전송함에 따라 상기 제2 사물인터넷 서버 플랫폼에서 상기 제1 사물인터넷 서버 플랫폼으로부터 전송된 크리덴셜을 검증하여 상기 제1 사물인터넷 서버 플랫폼에게 크리덴셜 검증을 수행한 크리덴셜 검증 결과를 전달하는 단계를 포함할 수 있다.

[0014] 상기 상호운용성을 지원하는 단계는, 상기 제1 사물인터넷 서버 플랫폼에서 상기 제1 사물인터넷 서버 플랫폼과 상기 제2 사물인터넷 서버 플랫폼에 접근 가능한 글로벌 접근 범위를 가진 상호운용 접근 토큰(IAT)을 생성하는 단계를 포함할 수 있다.

[0015] 상기 상호운용성을 지원하는 단계는, 상기 제1 사물인터넷 서버 플랫폼 또는 상기 제2 사물인터넷 서버 플랫폼에서의 크리덴셜 검증 결과에 따라 자원에 접근 가능한 영역이 제한되는 단계를 포함할 수 있다.

[0016] 상기 상호운용성을 지원하는 단계는, 상기 제1 사물인터넷 서버 플랫폼에서 상기 요청자에게 상기 제1 사물인터넷 서버 플랫폼 또는 상기 제2 사물인터넷 서버 플랫폼 중 어느 하나 이상의 사물인터넷 서버 플랫폼에 접근 가능한 상호운용 접근 토큰(IAT)을 발급하고, 상기 발급된 상호운용 접근 토큰(IAT)을 상기 요청자에게 전달하고, 상기 요청자로부터 상기 제1 사물인터넷 서버 플랫폼으로부터 발급받은 상호운용 접근 토큰(IAT)을 기반으로 상기 제2 사물인터넷 서버 플랫폼에 접근되는 단계를 포함할 수 있다.

[0017] 상기 상호운용성을 지원하는 단계는, A3FaaS(A3 Framework as a Service)를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 ACMD(Authorization Code for Multiple Domains)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0018] 상기 상호운용성을 지원하는 단계는, 클라이언트로부터 접근하기 위한 자원들이 명시되어 상호운용 접근 토큰(IAT)의 발급이 요청됨에 따라 상기 접근을 요청한 자원에 대한 권한을 획득하기 위해 자원 소유자들의 허가를 획득하고, 상기 획득된 허가를 A3 서버에게 전송하고, 상기 A3 서버에서 상기 클라이언트로부터 전송된 허가들을 검증을 수행한 검증 결과를 통하여 상기 클라이언트에게 인가 코드를 발급하고, 상기 클라이언트에서 상기 A3로부터 발급받은 인가 코드를 다시 상기 A3 서버에게 전달하고, 상기 A3서버에서 상기 클라이언트로부터 전달받은 인가 코드를 검증한 뒤, 상기 클라이언트에게 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0019] 상기 상호운용성을 지원하는 단계는, A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 IMD(Implicit for Multiple Domains)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0020] 상기 상호운용성을 지원하는 단계는, 클라이언트로부터 요청된 자원의 접근 범위와 상호운용 접근 토큰(IAT)을 발급받을 리다이렉션 URI가 전달됨에 따라 로그인 과정을 통하여 상기 요청된 자원의 접근 범위에 대한 권한을 획득하기 위하여 자원 소유자들의 허가를 받고, 상기 허가를 A3 서버에 전달하고, 상기 A3 서버에서 상기 클라이언트로부터 요청된 자원, 상기 요청된 자원이 위치한 도메인의 상호운용 정책 및 상기 요청된 자원의 크리덴셜을 검증한 뒤, 상기 클라이언트에게 상호운용 접근 토큰(IAT)을 전달하는 단계를 포함할 수 있다.

[0021] 상기 상호운용성을 지원하는 단계는, A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안

상호운용성 지원 접근 제어 프레임워크를 통하여 MROPC(Multiple Resource Owners' Password Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0022] 상기 상호운용성을 지원하는 단계는, 상기 클라이언트로부터 기 저장된 자원 소유자들의 크리덴셜 또는 자원을 요청하기 위한 자원 소유자들의 크리덴셜들을 전달받고, 요청된 자원의 접근 범위 및 상기 자원 소유자 크리덴셜을 A3 서버에 전송하고, 상기 A3 서버에서 상기 클라이언트로부터 요청된 자원의 접근 범위와 상기 자원 소유자 크리덴셜을 검증하여 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0023] 상기 상호운용성을 지원하는 단계는, A3FaaS(A3 Framework as a Service)를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 MCC(Multiple Clients' Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0024] 상기 상호운용성을 지원하는 단계는, 클라이언트에서 자원의 접근 범위와 관련된 클라이언트들의 크리덴셜들을 A3 서버에 전달하고, 상기 A3 서버에서 전달된 클라이언트 크리덴셜들을 검증하고, 상기 자원의 접근 범위를 갱신한 뒤 상호운용 접근 토큰(IAT)을 발급하는 단계를 포함할 수 있다.

[0025] 상호운용성 지원 접근 제어를 위한 제어 시스템은, 접근 제어를 위한 계층을 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 프레임워크 제공부; 및 상기 가상화된 계층에 기반한 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 이종의 사물인터넷 플랫폼 간에 상호운용성을 지원하는 상호운용성 지원부를 포함할 수 있다.

발명의 효과

[0027] 상호운용성을 고려한 접근 제어 계층을 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 이종의 사물인터넷 플랫폼 간에 보안 상호운용성을 제공할 수 있다.

[0028] 상호운용 접근 토큰을 이용하여 여러 도메인에 접근이 가능하기 때문에 토큰 관리가 간편하다.

[0029] 사물 인터넷 기기들이 사물인터넷 플랫폼에 인증 및 인가 과정을 위임하여 상호운용을 위한 인증 및 인가 과정에 필요한 성능적 부담을 최소화할 수 있다.

도면의 간단한 설명

[0031] 도 1은 일 실시예에 있어서 접근 제어를 위한 계층을 가상화하여 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 것을 나타낸 도면이다.

도 2는 일 실시예에 따른 제어 시스템의 보안 상호운용성 지원 접근 제어 프레임워크를 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 제어 시스템에서 사물 인터넷 서버 플랫폼 간의 보안 상호운용성 지원 접근 제어를 위한 동작을 설명하기 위한 흐름도이다.

도 4는 일 실시예에 따른 제어 시스템의 보안 상호운용성 지원 접근 제어 프레임워크의 또 다른 예이다.

도 5는 내지 도 10은 일 실시예에 따른 제어 시스템에서 IAT를 발급하는 방법을 설명하기 위한 다양한 예이다.

도 11은 일 실시예에 따른 제어 시스템의 구성을 설명하기 위한 블록도이다.

도 12는 일 실시예에 따른 제어 시스템에서 보안 상호운용성 지원 접근 제어 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0032] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0034] 도 1은 일 실시예에 있어서 접근 제어를 위한 계층을 가상화하여 보안 상호운용성 지원 접근 제어 프레임워크를 제공하는 것을 나타낸 도면이다.

[0035] 상호운용성을 고려한 접근 제어 프레임워크는 인증, 인가 및 감사 계층이 가상화되어 사물인터넷 플랫폼에 일괄적으로 제공될 수 있다. 도 1은 인증, 인가, 감사 계층의 개요를 나타낸 것으로, A3(Authentication, Authorization, Auditing; A3) 계층에서 상호운용 가능한 접근 제어를 제공하기 위해서 기존의 OAuth 2.0 표준을 확장하여 적용할 수 있다. 기존의 OAuth 2.0 표준은 명확한 인가 서버 기능(authorization capability)이

나 토큰의 구조 등을 정의하고 있지 않기 때문에 각 사물인터넷 플랫폼들에서 OAuth 2.0을 구현하면 인가 서버 기능이나 토큰의 구조 등이 상이할 수밖에 없으므로 상호운용성이 부족해지는 문제가 존재한다. 실시예에서는 인증, 인가 및 감사 기능을 하나의 계층으로 가상화하여 핵심 기능이나 토큰의 구조 등이 동일하여 이종의 사물인터넷 플랫폼 간에 상호운용성을 지원할 수 있다.

[0036] 실시예에서는 상호운용 접근 토큰(interoperable access token; IAT)을 기반으로 상호운용이 이루어질 수 있다. 기존의 OAuth 2.0을 기반으로 발급되는 접근 토큰은 하나의 도메인(예를 들어, ARTIK 사물인터넷 플랫폼)에 제한된 접근 스코프(access scope)를 가지지만, 실시예에 따른 IAT는 복수 개의 도메인(예를 들면, ARTIK과 FIWARE 사물인터넷 플랫폼)에 걸친 글로벌 접근 스코프(global access scope)를 가질 수 있다. 이를 통해서 복수 개의 토큰 대신 단일 토큰만 관리하면 되므로, 토큰 관리(토큰 생성, 갱신, 폐기)가 간단해지며, 이종의 사물인터넷 플랫폼 간의 상호운용성을 제공할 수 있게 된다.

[0037] 성능이 제한적인 사물인터넷 기기들은 사물인터넷 플랫폼의 인증 및 인가 계층에 인증과 인가 과정을 위임하기 때문에 상호운용을 위한 인증 및 인가 과정에 필요한 성능적 부담을 최소화할 수 있다.

[0038] 도 2는 일 실시예에 따른 제어 시스템의 보안 상호운용성 지원 접근 제어 프레임워크를 설명하기 위한 도면이다.

[0039] 사물인터넷 플랫폼(100)에 보안 상호운용성 지원 접근 제어 프레임워크(200)가 제공될 수 있다. 도 2에서는 하나의 사물인터넷 플랫폼을 대상으로 동작하는 보안 상호운용성 지원 제어 프레임워크의 동작을 설명하기로 한다.

[0040] 일반적으로 사물인터넷 서버 플랫폼의 자원들은 도메인마다 개별적으로 관리된다. 사물인터넷 서버 플랫폼의 자원에 대한 접근 권한이 접근 토큰을 기반으로 검증될 수 있다. OAuth 표준에서는 접근 토큰의 발급을 위하여 사용자 또는 클라이언트에 관련된 크리덴셜을 사용하거나 자원 소유자의 허가(grant)를 받아야 한다.

[0041] 구체적으로, 사물인터넷 서버 플랫폼(100)에 접근하고자 하는 요청자는 웹 서버 등을 통해 제공되는 인터페이스를 사용하여 보안 상호운용성 지원 접근 제어 프레임워크(200)에 사용자/클라이언트 정보를 등록할 수 있다(1). 보안 상호운용성 지원 접근 제어 프레임워크(200)는 OAuth 2.0 표준에 명시된 인가 코드(Authorization Code) 등의 과정을 통해서 요청자(210)를 인증하고 인가할 수 있다(2). 보안 상호운용성 지원 접근 제어 프레임워크(200)는 접근 토큰(access token)을 발급할 수 있다(3). 보안 상호운용성 지원 접근 제어 프레임워크(200)는 만약 인증 및 인가 과정에 실패할 경우, 토큰을 발급하지 않고 세션을 종료할 수 있다. 요청자가 발급받은 토큰으로 사물인터넷 서버 플랫폼(100)의 자원이 요청될 수 있다(4). 보안 상호운용성 지원 접근 제어 프레임워크(200)는 요청자로부터 자원이 요청되면서 제시된 토큰을 검증할 수 있다(5). 보안 상호운용성 지원 접근 제어 프레임워크(200)에서 접근 토큰의 검증으로 자원의 사용 권한 여부를 검증하는 것을 예를 들어 설명하였으나, 역할(role)과 같은 속성(attribute) 등을 기반으로 추가적인 인증/인가 과정이 추가될 수도 있다. 보안 상호운용성 지원 접근 제어 프레임워크(200)는 토큰이 정상적으로 검증될 경우, 사물인터넷 서버 플랫폼(100)의 자원을 검색할 수 있다(6). 보안 상호운용성 지원 접근 제어 프레임워크(200)는 요청자(210)로부터 요청된 자원이 사물인터넷 서버 플랫폼(100)에 존재할 경우, 상기 요청된 자원을 요청자(210)에게 전달할 수 있다(7).

[0042] 도 3은 일 실시예에 따른 제어 시스템에서 사물 인터넷 서버 플랫폼 간의 보안 상호운용성 지원 접근 제어를 위한 동작을 설명하기 위한 흐름도이다.

[0043] 도 3에서는 복수 개의 사물인터넷 서버 플랫폼 간의 보안 상호운용성 접근 제어 동작을 설명하기로 한다. 이때, 이종의 사물인터넷 서버 플랫폼에서 제공되는 데이터나 서비스에 접근 가능하도록 하는 IAT(상호운용 접근 토큰) 발급부터 자원 요청까지의 동작을 설명하기로 한다. IAT 발급을 위하여 기존의 Client Credentials(CC)를 확장한 Multiple Clients' Credentials(MCC) 방식을 사용하는 것을 예를 들어 설명하기로 한다. 요청자가 제일 처음 IAT를 요청할 때, 여러 도메인의 크리덴셜들을 전송하고, 크리덴셜의 검증을 위해 사물인터넷 서버 플랫폼 간의 통신이 이루어질 수 있다.

[0044] 우선적으로, 제어 시스템을 구성하고 있는 구성 요소에 대하여 설명하기로 한다. 요청자(210)는 이종의 사물인터넷 서버 플랫폼에서 제공되는 자원들에 접근 가능한 IAT와 상기 접근 가능한 IAT를 사용하여 자원을 요청하는 주체를 의미한다. 사물인터넷 서버 플랫폼 A(제1 사물인터넷 서버 플랫폼)(301)는 신뢰할 수 있는 사물인터넷 서버 플랫폼으로서, 요청자의 IAT 발급 요청에 따라 사물인터넷 서버 플랫폼 A(301)와 사물 인터넷 서버 플랫폼 B(302)에 접근 가능한 IAT를 발급할 수 있다. 사물인터넷 서버 플랫폼 B(제2 사물인터넷 서버 플랫폼)(302)는

신뢰할 수 있는 사물인터넷 서버 플랫폼로서, 사물인터넷 서버 플랫폼 A(301)의 크리덴셜 검증 요청을 처리하고, 자원 요청을 처리할 수 있다.

[0045] 보안 상호운용성 지원 접근 제어 모듈(303, 304)은 가상화된 보안 상호운용성 지원 접근 제어 프레임워크를 기반으로 인증, 인가, 감사를 제공하는 보안 모듈이다. 보안 상호운용성 지원 접근 제어 모듈(303, 304)은 확장된 OAuth 2.0을 기반으로 서버에 접근하려는 클라이언트에 대해서 접근 제어(인증과 인가)를 수행하여 서버 내부의 자원을 보호할 수 있다. 인가는 기본적으로 토큰 기반으로 수행되지만, 유연성과 상황 인지적 접근 제어를 위해서 ABAC과 같은 접근 제어 모델이 추가적으로 사용될 수 있다. 데이터베이스(305, 306)는 사물인터넷 서버 플랫폼의 자원이나 크리덴셜들을 저장할 수 있다. 데이터베이스(305, 306) 내에 저장된 데이터들은 보안 상호운용성 지원 접근 제어 모듈(303, 304)에 의해서 적절한 인증과 인가를 받은 사용자/클라이언트에 대해서만 접근이 허용될 수 있다.

[0046] OAuth 2.0 사용을 위해 필요한 사용자/클라이언트 등록 과정은 도 2에서 설명한 것과 동일하다. 도 3에서는 사물인터넷 서버 플랫폼 A(301)와 사물인터넷 서버 플랫폼 B(302) 간의 동작 과정을 설명하기로 한다. 요청자(210)는 적어도 하나 이상의 사물인터넷 서버 플랫폼에 등록한 요청자의 크리덴션을 이용하여 적어도 하나 이상의 사물인터넷 서버 플랫폼에 접근 가능한 권한을 가진 IAT를 요청할 수 있다(1). 예를 들면, 요청자(210)는 사물인터넷 서버 플랫폼 A(301)와 사물인터넷 서버 플랫폼 B(302)에 등록한 요청자의 크리덴셜을 이용하여 사물인터넷 서버 플랫폼 A(301) 및 사물인터넷 서버 플랫폼 B(302)에 접근 가능한 권한을 가진 IAT를 요청할 수 있다. 이때, 크리덴셜은 기밀성을 유지하기 위하여 해시화될 수 있다. IAT는 기존의 OAuth 표준에서 사용되는 접근 토큰과는 달리 여러 도메인에 접근 가능하도록 글로벌 접근 범위를 가질 수 있다. 글로벌 접근 범위는 "access scope: {"도메인 정보 1": "자원 정보 1", "도메인 정보 2": "자원 정보 2"}와 같은 형태로 설정될 수 있다. 예를 들면 글로벌 접근 범위는 "access scope: {"Domain A": "Resource 1", "Domain B": "Resource 2"}와 같이 설정될 수 있다.

[0047] 사물인터넷 서버 플랫폼 A(301)는 요청자(210)로부터 전달받은 크리덴셜 중 사물인터넷 서버 플랫폼 A(301)의 크리덴션을 검증할 수 있다(2). 사물인터넷 서버 플랫폼 A(301)는 사물인터넷 서버 플랫폼 A(301)에 저장된 크리덴셜을 해시화하여 요청자로부터 전달된 해시화된 크리덴셜과 비교함으로써 검증을 수행할 수 있다.

[0048] 사물인터넷 서버 플랫폼 A(301)는 요청자로부터 전달된 크리덴셜 중 사물인터넷 서버 플랫폼 B(302)의 크리덴션을 사물인터넷 서버 플랫폼 A(301)가 대신 검증할 수 없기 때문에, 사물인터넷 서버 플랫폼 B(302)에 크리덴셜 검증 요청을 전송할 수 있다(3). 이때, 사물인터넷 서버 플랫폼 B(302)에 전달된 크리덴셜은 요청자(210)로부터 전달된 해시화된 크리덴셜이다.

[0049] 사물인터넷 서버 플랫폼 B(302)는 사물인터넷 서버 플랫폼 A(301)로부터 전송된 크리덴셜을 검증할 수 있다(4). 사물인터넷 서버 플랫폼 B(302)는 사물인터넷 서버 플랫폼 B(302)에 저장된 크리덴셜을 해시화하여 사물인터넷 서버 플랫폼 A(301)로부터 전달된 해시화된 크리덴셜, 다시 말해서, 요청자가 보낸 해시화된 크리덴셜과 비교함으로써 검증을 수행할 수 있다.

[0050] 사물인터넷 서버 플랫폼 B(302)는 크리덴셜 검증을 수행한 크리덴셜 검증 결과를 사물인터넷 서버 플랫폼 A(301)에게 전달할 수 있다(5).

[0051] 사물인터넷 서버 플랫폼 A(301)는 사물인터넷 서버 플랫폼 A(301)와 사물인터넷 서버 플랫폼 B(302)에 접근 가능한 글로벌 접근 범위(global access scope)를 가진 IAT를 생성할 수 있다(6). 이때, 사물인터넷 서버 플랫폼 A(301) 또는 사물인터넷 서버 플랫폼 B(302)의 크리덴셜 검증 결과에 따라 접근 가능한 영역이 제한될 수 있다. 예를 들면, 사물인터넷 서버 플랫폼 B(302)의 크리덴셜 검증이 실패한 경우, 요청자(210)가 사물인터넷 서버 플랫폼 B(302)에 대한 접근 권한을 요청했어도 이를 무시하고 사물인터넷 서버 플랫폼 A(301)에만 접근이 가능한 IAT가 생성될 수 있다. 크리덴셜 검증에 모두 실패할 경우 IAT를 생성하지 않지만, 일단 IAT가 생성되면 사물인터넷 서버 플랫폼 A(301)는 검증 용도로만 사용되는 해시화된 IAT를 사물인터넷 서버 플랫폼 B(302)에 공유할 수 있다. 이를 통해 사물인터넷 서버 플랫폼 B(302)는 향후 요청자(210)가 자원을 요청할 때 전달되는 IAT(사물인터넷 서버 플랫폼 A(301)로부터 발급된 원본 IAT)를 검증할 수 있다. 해시화된 IAT는 오직 자원 요청 시 전달되는 (원본) IAT의 검증 용도로만 사용되기 때문에 공격자가 중간에 탈취하더라도 사물인터넷 서버 플랫폼 A(301)나 사물인터넷 서버 플랫폼 B(302)의 자원에는 접근할 수 없다.

[0052] 사물인터넷 서버 플랫폼 A(301)는 요청자(210)에게 사물인터넷 서버 플랫폼 A(301)와 사물인터넷 서버 플랫폼 B(302)에 접근 가능한 (원본) IAT를 전달할 수 있다(7). 이때, IAT는 기밀성과 무결성을 보장하기 위하여

DTLS, TLS와 같은 기술이 사용되어 전달될 수 있다. IAT는 기본적으로 OAuth 표준에서 사용하는 Bearer 타입이며, 접근할 수 있는 범위가 하나의 도메인이 아니라 복수의 도메인인 점이 일반적인 접근 토큰과 다르다. 만약 Bearer 토큰 대신, JWT와 HMAC을 활용하면, 토큰 자체의 무결성도 제공할 수 있다.

[0053] 요청자(210)는 사물인터넷 서버 플랫폼 A(301)로부터 발급받은 원본 IAT를 기반으로 사물인터넷 서버 플랫폼 B(302)에 접근할 수 있다(8). 이때, 사용된 IAT는 사물인터넷 서버 플랫폼 A(301)에서 발급된 것으로, 사물인터넷 서버 플랫폼 A(301)로의 접근도 가능하다.

[0054] 도 4는 일 실시예에 따른 제어 시스템의 보안 상호운용성 지원 접근 제어 프레임워크의 또 다른 예이다.

[0055] 도 3에서는 MCC를 기반으로 IAT를 발급받는 것을 설명하였으나, 보안 상호운용성 지원 접근 제어 프레임워크는 클라이언트 크리덴셜(Client Credentials)을 확장한 MCC 외에 Authorization Code를 확장한 Authorization Code for Multiple Domains(ACMD), Implicit를 확장한 Implicit for Multiple Domains(IMD), Resource Owner Password Credentials를 확장한 Multiple Resource Owners' Password Credentials(MROPC) 방식을 통해서 IAT 발급을 수행할 수 있다.

[0056] 보안 상호운용성 지원 접근 제어 프레임워크(200)는 A3 Framework as a Service(A3FaaS)(400)를 통해 가상화되어 각 사물인터넷 플랫폼(예를 들면, 사물인터넷 서버 플랫폼)에 배치될 수 있다. 상호운용성 지원 접근 제어 프레임워크의 IAT 발급 등의 상호운용성 지원 접근 제어 기능은 A3 서버에서 제공된다. 또한, A3 서버에서 사용되는 크리덴셜(사용자/클라이언트 크리덴셜, 토큰 등)과 상호운용성 지원을 위한 보안 정책(Domain Level Interoperability Policy (DL-IP) 및 Resource Level Interoperability Policy(RL-IP))들은 각각 데이터베이스에 저장되어 사용될 수 있다. 이에, A3에 기반한 IAT 발급 방식의 다양한 방법을 설명하기로 한다.

[0057] 도 5는 내지 도 10은 일 실시예에 따른 제어 시스템에서 IAT를 발급하는 방법을 설명하기 위한 다양한 예이다.

[0058] 도 5를 참고하면, ACMD(Authorization Code for Multiple Domains)에 기반하여 IAT를 발급하는 방식에 대하여 설명하기로 한다. ACMD는 사용자의 로그인 과정을 통해 발급된 인가 코드를 이용하여 IAT를 발급하는 방식을 의미한다. 클라이언트는 접근하기 위한 자원들을 명시하여 IAT 발급을 요청할 수 있다(1). 클라이언트는 접근을 요청한 자원에 대한 권한을 획득하기 위해 자원 소유자들(요청된 접근 범위의 자원을 소유한 사용자들)로부터 허가들을 받을 수 있고, 허가를 A3 서버에게 전송할 수 있다(2). A3 서버는 클라이언트로부터 전송된 허가들을 검증할 수 있고, 검증 결과를 통하여 클라이언트에게 인가 코드를 발급할 수 있다(3). 클라이언트는 A3로부터 발급받은 인가 코드를 다시 A3 서버에게 전달할 수 있다(4). A3 서버는 클라이언트로부터 전달받은 인가 코드를 검증한 뒤, 클라이언트에게 IAT를 발급할 수 있다(5).

[0059] 구체적으로, 도 6을 참고하면, 클라이언트(602)는 IAT 발급을 위한 ACMD를 시작할 수 있다(1). 사용자 에이전트(601)는 클라이언트(602)가 요구하는 접근 범위(예를 들어, "access scope": {"domain A": "resource A", "domain B": "resource B"})와 리다이렉션 URI를 기반으로 도메인 A의 A3 서버 1(603)의 토큰 엔드포인트에 IAT를 요청할 수 있다(2). 이때, 각 도메인들의 A3 서버들은 동일한 A3FaaS로부터 가상화된 서버로, 어느 A3 서버든 동일한 상호운용 접근 제어 기능을 제공할 수 있다. 이에 따라, 사용자 에이전트(601)는 도메인 A의 A3 서버 1(603)에 IAT 발급 요청을 보냈으나, 도메인 B의 A3 서버 2(604)에 IAT 발급 요청을 보내도 동일한 기능을 수행할 수 있다.

[0060] 도메인 A의 A3 서버 1(603)은 IAT 발급을 요청한 사용자 에이전트(601)를 로그인 페이지로 리다이렉트할 수 있다(3). 사용자 에이전트(601)는 클라이언트(602)로부터 요청된 접근 범위와 관련된 자원들의 자원 소유자(사용자)(600)에게 로그인을 요청할 수 있다. 기존의 Authorization Code 방식은 단일 자원 소유자의 크리덴셜만을 요구하지만 ACMD는 복수 개의 도메인에 해당하는 자원 소유자들의 크리덴셜을 요구하기 때문에, 로그인 페이지는 다수의 계정 입력 필드를 가질 수 있다(4). 자원 소유자(600)는 자원 소유자의 계정 정보(아이디 및 패스워드)로 로그인하여 클라이언트(602)의 자원 접근에 대해서 허가할 수 있다(5). 예를 들면, 자원 소유자(600)는 자원 소유자의 크리덴셜을 입력하여 자원 접근을 허가할 수 있다. 사용자 에이전트(601)는 자원 소유자(600)로부터 입력된 크리덴셜을 도메인 A의 A3 서버 1(603)에 전달할 수 있다(6). 도메인 A의 A3 서버 1(603)은 도메인 A와 자원 A에 해당하는 상호운용 접근 정책(DL-IP와 RL-IP), 및 사용자 에이전트(601)로부터 전달받은 크리덴셜 중 도메인 A에 해당하는 크리덴셜을 검증할 수 있다(7). 또한, 도메인 B의 자원 B에 대한 정책과 자원 B에 대한 자원 소유자의 크리덴셜은 도메인 B의 A3 서버 2(604)가 검증할 수 있기 때문에, 도메인 A의 A3 서버 1(603)은 도메인 B의 A3 서버 2(604)에게 도메인 B와 자원 B에 대한 정책과 크리덴셜 검증을 요청할 수 있다(8).

[0061] 도메인 B의 A3 서버 2(604)는 클라이언트(602)로부터 요청된 자원 B와 자원 B가 위치한 도메인 B의 상호운용 정책(DL-IP와 RL-IP), 및 자원 B에 대한 자원 소유자의 크리덴셜을 검증할 수 있다(9). 도메인 B의 A3 서버 2(604)는 자원 B와 자원 B가 위치한 도메인 B의 상호운용 정책(DL-IP와 RL-IP) 및 자원 B에 대한 자원 소유자의 크리덴셜을 검증한 검증 결과를 도메인 A의 A3 서버 1(603)에게 전달할 수 있다(10). 도메인 A의 A3 서버 1(603)은 자원 정책과 크리덴셜 검증 결과를 기반으로 클라이언트가 요청한 접근 범위를 갱신할 수 있다(11). 예를 들면, 도메인 A의 A3 서버 1(603)은 도메인 B의 A3 서버 2(604)의 크리덴셜 검증 결과가 실패한 것으로 판단됨에 따라 자원 B를 제외한 자원 A에만 접근 가능하도록 접근 범위("access scope": {"domain A": "resource A"})를 수정할 수 있다. 도메인 A의 A3 서버 1(603)은 리다이렉션 URI를 이용하여 사용자 에이전트(601)에 인가 코드를 전달할 수 있고, 사용자 에이전트(601)는 클라이언트(602)에게 도메인 A로부터 발급받은 인가 코드를 전달할 수 있다(12, 13). 클라이언트(602)는 전달받은 인가 코드를 통해 도메인 A의 A3 서버 1(603)에 IAT 발급을 요청할 수 있다(14). 도메인 A의 A3 서버 1(603)은 상기 인가 코드를 검증하고, IAT를 발급할 수 있다(15).

[0062] 도 7을 참고하면, IMD(Implicit for Multiple Domains)에 기반하여 IAT를 발급하는 방식에 대하여 설명하기로 한다. IMD는 도 6의 ACMD의 과정을 축소한 인가 과정으로, 인가 코드의 발급 단계에서 인가 코드가 아닌 IAT를 곧바로 발급하는 것이다. 상세하게는, 클라이언트가 IMD를 시작할 수 있다(1). 클라이언트가 접근을 원하는 자원의 접근 범위와 IAT를 발급받을 리다이렉션 URI를 함께 전달할 수 있다. 클라이언트는 로그인 과정을 통해서 요청한 자원의 접근 범위에 대한 권한을 획득을 수 있도록 자원 소유자들의 허가를 받고, 상기 허가를 A3 서버에 전달할 수 있다(2). A3 서버는 클라이언트로부터 요청된 자원과 상기 자원이 위치한 도메인의 상호운용 정책, 및 상기 자원의 크리덴셜을 검증한 뒤, 클라이언트에게 IAT를 전달할 수 있다(3). 다시 말해서, IMD에 기반한 IAT 발급 과정은 ACMD에 기반한 IAT 발급 과정과 달리, 도 6의 (12), (13)과정이 생략되어, 인가 코드가 아닌 IAT가 직접 발급된다.

[0063] 도 8을 참고하면, MROPC(Multiple Resource Owners' Password Credentials)에 기반하여 IAT를 발급하는 방식에 대하여 설명하기로 한다. MROPC는 ACMD나 IMD에 비교적 간단한 방식으로, 사용자 에이전트나 로그인 과정이 존재하지 않고, 직접적으로 자원 소유자의 크리덴셜을 전달하여 IAT를 발급받는 것이다. 클라이언트는 기존에 자원 소유자들의 크리덴셜을 소유하고 있거나, 자원을 요청할 때 자원 소유자의 크리덴셜들을 전달받아야 한다(1). 클라이언트는 MROPC 요청과 함께 원하는 자원의 접근 범위 및 상기 접근 범위에 대한 권한을 대체할 수 있는 자원 소유자 크리덴셜을 A3 서버에 전송할 수 있다(2). MROPC 요청을 받은 A3 서버는 클라이언트로부터 요청된 자원의 접근 범위와 크리덴셜을 검증하고 IAT를 발급할 수 있다(3).

[0064] 구체적으로, 도 9를 참고하면, 도메인 A의 자원 소유자 1(901)과 도메인 B의 자원 소유자 2(902)는 자원 소유자 각각의 크리덴셜(도메인 A의 자원 소유자 1의 크리덴셜, 도메인 B의 자원 소유자 2의 크리덴셜)을 클라이언트(602)에게 전달할 수 있다(1, 2). 클라이언트(602)는 자원 소유자 크리덴셜을 기반으로 접근을 원하는 자원들의 접근 범위(예를 들어, "access scope": {"domain A": "resource A", "domain B": "resource B"})를 설정하여 MROPC를 시작할 수 있다(3). 클라이언트의 요청을 받은 도메인 A의 A3 서버 1(603)은 도메인 A와 자원 A에 해당하는 상호운용 정책(DL-IP와 RL-IP), 및 자원 소유자 크리덴셜을 검증할 수 있다(4). 도메인 A의 A3 서버 1(603)은 자체적으로 검증이 불가능한 도메인 B의 상호운용 정책과 도메인 B에 등록된 자원 소유자 크리덴셜을 검증하기 위해서 도메인 B의 A3 서버 2(604)에 정책 및 크리덴셜 검증 요청을 전송할 수 있다(5). 도메인 B의 A3 서버 2(604)는 도메인 A의 A3 서버 1(603)로부터 전송된 검증 요청에 따라 도메인 B와 자원 B에 해당하는 상호운용 보안 정책, 및 자원 소유자 크리덴셜을 검증할 수 있다(6). 도메인 B의 A3 서버 2(604)는 도메인 A의 A3 서버 1(603)에게 도메인 B와 자원 B에 해당하는 상호운용 보안 정책, 및 자원 소유자 크리덴셜 검증을 수행한 검증 결과를 전달할 수 있다(7). 도메인 A의 A3 서버 1(603)은 도메인 A의 A3 서버 1(603)과 도메인 B의 A3 서버 2(604)의 상호운용 보안 정책 및 크리덴셜 검증 결과에 따라 접근 범위를 갱신할 수 있다(8). 예를 들면, 도메인 A의 A3 서버 1(603)은 도메인 B의 A3 서버 2(604)의 상호운용 정책 검증이나 자원 소유자 크리덴셜 검증이 실패하면, 자원 B에 접근이 불가능하도록 접근 범위(예를 들어, "access scope": {"domain A": "resource A"})를 갱신할 수 있다. 도메인 A의 A3 서버 1(603)은 갱신한 접근 범위를 기반으로 IAT를 생성하고, 생성된 IAT를 클라이언트(602)에 전달할 수 있다(9).

[0065] 도 10을 참고하면, MCC(Multiple Clients' Credentials) 에 기반하여 IAT를 발급하는 방식에 대하여 설명하기로 한다. MCC는 앞서 설명한 MROPC 방식과 유사하지만, IAT의 발급을 위해서 자원 소유자의 크리덴셜을 이용하는 것이 아니라 클라이언트 크리덴셜(즉, 클라이언트 ID와 Secret)을 이용하는 것이다. IAT를 발급받기 위해서 자원의 접근 범위와 관련된 클라이언트들의 크리덴셜들을 A3 서버에 전달할 수 있다(1). A3 서버는 전달된 클

라이언트 크리덴셜들을 검증하고, 접근 범위를 알맞게 갱신한 뒤 IAT를 발급할 수 있다(2).

[0066] 이와 같이, ACMD, IMD, MROPC 및 MCC는 이종의 도메인에 접근이 가능한 범위를 가지는 IAT를 발급하는데 사용되며, 각 방식들은 기존의 OAuth 2.0 표준에서 정의된 Authorization Code, Implicit, Resource Owner Password Credentials, Client Credentials들이 사용되는 환경이나 목적 등을 따른다.

[0067] 도 11은 일 실시예에 따른 제어 시스템의 구성을 설명하기 위한 블록도이고, 도 12는 일 실시예에 따른 제어 시스템에서 보안 상호운용성 지원 접근 제어 방법을 설명하기 위한 흐름도이다.

[0068] 제어 시스템(1100)의 프로세서는 프레임워크 제공부(1110) 및 상호운용성 지원부(1120)를 포함할 수 있다. 이러한 프로세서의 구성요소들은 제어 시스템(1100)에 저장된 프로그램 코드가 제공하는 제어 명령에 따라 프로세서에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다. 프로세서 및 프로세서의 구성요소들은 도 12의 보안 상호운용성 지원 접근 제어 방법이 포함하는 단계들(1210 내지 1220)을 수행하도록 제어 시스템을 제어할 수 있다. 이때, 프로세서 및 프로세서의 구성요소들은 메모리가 포함하는 운영체제의 코드와 적어도 하나의 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다.

[0069] 프로세서는 보안 상호운용성 지원 접근 제어 방법을 위한 프로그램의 파일에 저장된 프로그램 코드를 메모리에 로딩할 수 있다. 예를 들면, 제어 시스템에서 프로그램이 실행되면, 프로세서는 운영체제의 제어에 따라 프로그램의 파일로부터 프로그램 코드를 메모리에 로딩하도록 제어 시스템을 제어할 수 있다. 이때, 프로세서 및 프로세서가 포함하는 프레임워크 제공부(1110) 및 상호운용성 지원부(1120) 각각은 메모리에 로딩된 프로그램 코드 중 대응하는 부분의 명령을 실행하여 이후 단계들(1210 내지 1220)을 실행하기 위한 프로세서의 서로 다른 기능적 표현들일 수 있다.

[0070] 단계(1210)에서 프레임워크 제공부(1110)는 접근 제어를 위한 계층을 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 제공할 수 있다. 프레임워크 제공부(1110)는 인증(Authentication), 인가(Authorization), 감사(Auditing)의 접근 제어를 위한 계층을 하나의 계층으로 가상화한 보안 상호운용성 지원 접근 제어 프레임워크를 사물인터넷 서버 플랫폼에 제공할 수 있다.

[0071] 단계(1220)에서 상호운용성 지원부(1120)는 제공된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 이종의 사물인터넷 플랫폼 간에 상호운용성을 지원할 수 있다. 상호운용성 지원부(1120)는 사물인터넷 서버 플랫폼에서 확장된 OAuth 2.0(즉, ACMD, IMD, MROPC, MCC)에 기초하여 발급되는 상호운용 접근 토큰(IAT)을 기반으로 상호운용성을 지원할 수 있다. 일례로, 상호운용성 지원부(1120)는 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 MCC(Multiple Clients' Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급할 수 있다. 상호운용성 지원부(1120)는 요청자로부터 복수 개의 사물인터넷 서버 플랫폼에 등록한 요청자의 크리덴션을 이용하여 복수 개의 사물인터넷 서버 플랫폼에 접근 가능한 권한을 가진 상호운용 접근 토큰(IAT)을 요청할 수 있다. 상호운용성 지원부(1120)는 제1 사물인터넷 서버 플랫폼이 상기 요청자로부터 전달된 크리덴셜 중 제1 사물인터넷 서버 플랫폼의 크리덴셜을 검증하고, 제1 사물인터넷 서버 플랫폼에서 상기 요청자로부터 전달된 크리덴셜 중 제2 사물인터넷 서버 플랫폼으로 크리덴셜 검증 요청을 전송함에 따라 제2 사물인터넷 서버 플랫폼에서 제1 사물인터넷 서버 플랫폼으로부터 전송된 크리덴셜을 검증하여 제1 사물인터넷 서버 플랫폼에게 크리덴셜 검증을 수행한 크리덴셜 검증 결과를 전달할 수 있다. 상호운용성 지원부(1120)는 제1 사물인터넷 서버 플랫폼에서 제1 사물인터넷 서버 플랫폼과 제2 사물인터넷 서버 플랫폼에 접근 가능한 글로벌 접근 범위를 가진 상호운용 접근 토큰(IAT)을 생성할 수 있다. 이때, 제1 사물인터넷 서버 플랫폼 또는 제2 사물인터넷 서버 플랫폼에서의 크리덴셜 검증 결과에 따라 자원에 접근 가능한 영역이 제한될 수 있다. 상호운용성 지원부(1120)는 제1 사물인터넷 서버 플랫폼에서 요청자에게 제1 사물인터넷 서버 플랫폼 또는 제2 사물인터넷 서버 플랫폼 중 어느 하나 이상의 사물인터넷 서버 플랫폼에 접근 가능한 상호운용 접근 토큰(IAT)을 발급하고,요청자로부터 제1 사물인터넷 서버 플랫폼에서 발급받은 상호운용 접근 토큰(IAT)을 기반으로 제1 사물인터넷 서버 플랫폼이나 제2 사물인터넷 서버 플랫폼에 접근될 수 있다.

[0072] 다른 예로서, 상호운용성 지원부(1120)는 A3FaaS(A3 Framework as a Service)를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 ACMD(Authorization Code for Multiple Domains)를 기반으로 상호운용 접근 토큰(IAT)을 발급할 수 있다. 상호운용성 지원부(1120)는 클라이언트로부터 접근하기 위한 자원들이 명시되어 상호운용 접근 토큰(IAT)의 발급이 요청됨에 따라 상기 접근을 요청한 자원에 대한 권한을 획득하기 위해 자원 소유자들의 허가를 획득하고, 획득된 허가를 A3 서버에게 전송하고, A3 서버에서 클라이언트로부터 전송된 허가들을 검증을 수행한 검증 결과를 통하여 클라이언트에게 인가 코드를 발급하고, 클라이언트에서 A3로부터 발급받은 인가 코드를 다시 A3 서버에게 전달하고, A3서버에서

클라이언트로부터 전달받은 인가 코드를 검증한 뒤, 클라이언트에게 상호운용 접근 토큰(IAT)을 발급할 수 있다.

[0073] 또 다른 예로서, 상호운용성 지원부(1120)는 A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 IMD(Implicit for Multiple Domains)를 기반으로 상호운용 접근 토큰(IAT)을 발급할 수 있다. 상호운용성 지원부(1120)는 클라이언트로부터 요청된 자원의 접근 범위와 상호운용 접근 토큰(IAT)을 발급받을 리다이렉션 URI가 전달됨에 따라 로그인 과정을 통하여 요청된 자원의 접근 범위에 대한 권한을 획득하기 위하여 자원 소유자들의 허가를 받고, 허가를 A3 서버에 전달하고, A3 서버에서 클라이언트로부터 요청된 자원, 요청된 자원이 위치한 도메인의 상호운용 정책 및 상기 요청된 자원의 크리덴셜을 검증한 뒤, 클라이언트에게 상호운용 접근 토큰(IAT)을 전달할 수 있다.

[0074] 또 다른 예로서, 상호운용성 지원부(1120)는 A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 MROPC(Multiple Resource Owners' Password Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급할 수 있다. 상호운용성 지원부(1120)는 클라이언트로부터 기 저장된 자원 소유자들의 크리덴셜 또는 자원을 요청하기 위한 자원 소유자들의 크리덴셜들을 전달받고, 요청된 자원의 접근 범위 및 자원 소유자 크리덴셜을 A3 서버에 전송하고, A3 서버에서 클라이언트로부터 요청된 자원의 접근 범위와 자원 소유자 크리덴셜을 검증하여 상호운용 접근 토큰(IAT)을 발급할 수 있다.

[0075] 또 다른 예로서, 상호운용성 지원부(1120)는A3FaaS를 통해 가상화되어 각각의 사물인터넷 서버 플랫폼에 배치된 보안 상호운용성 지원 접근 제어 프레임워크를 통하여 MCC(Multiple Clients' Credentials)를 기반으로 상호운용 접근 토큰(IAT)을 발급할 수 있다. 상호운용성 지원부(1120)는 클라이언트에서 자원의 접근 범위와 관련된 클라이언트들의 크리덴셜들을 A3 서버에 전달하고, A3 서버에서 전달된 클라이언트 크리덴셜들을 검증하고, 자원의 접근 범위를 갱신한 뒤 상호운용 접근 토큰(IAT)을 발급할 수 있다.

[0076] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0077] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0078] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를

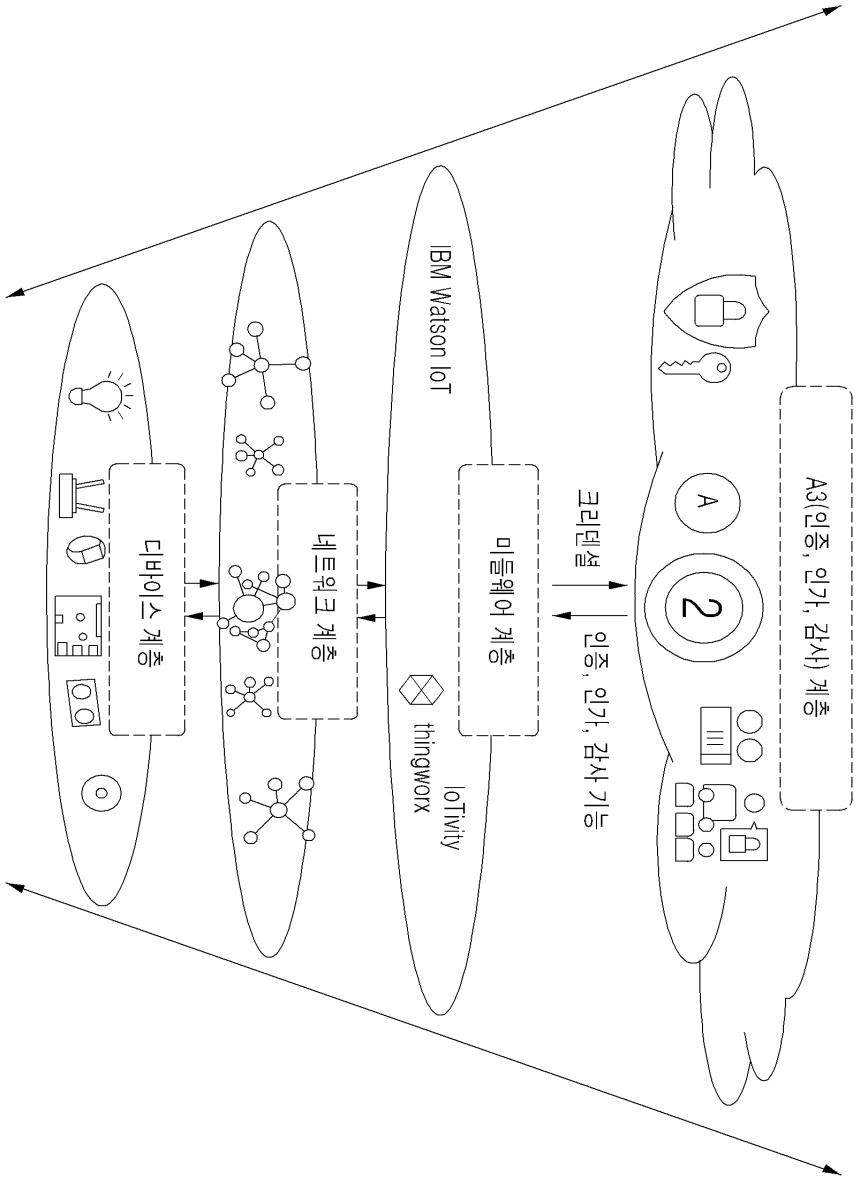
포함한다.

[0079] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

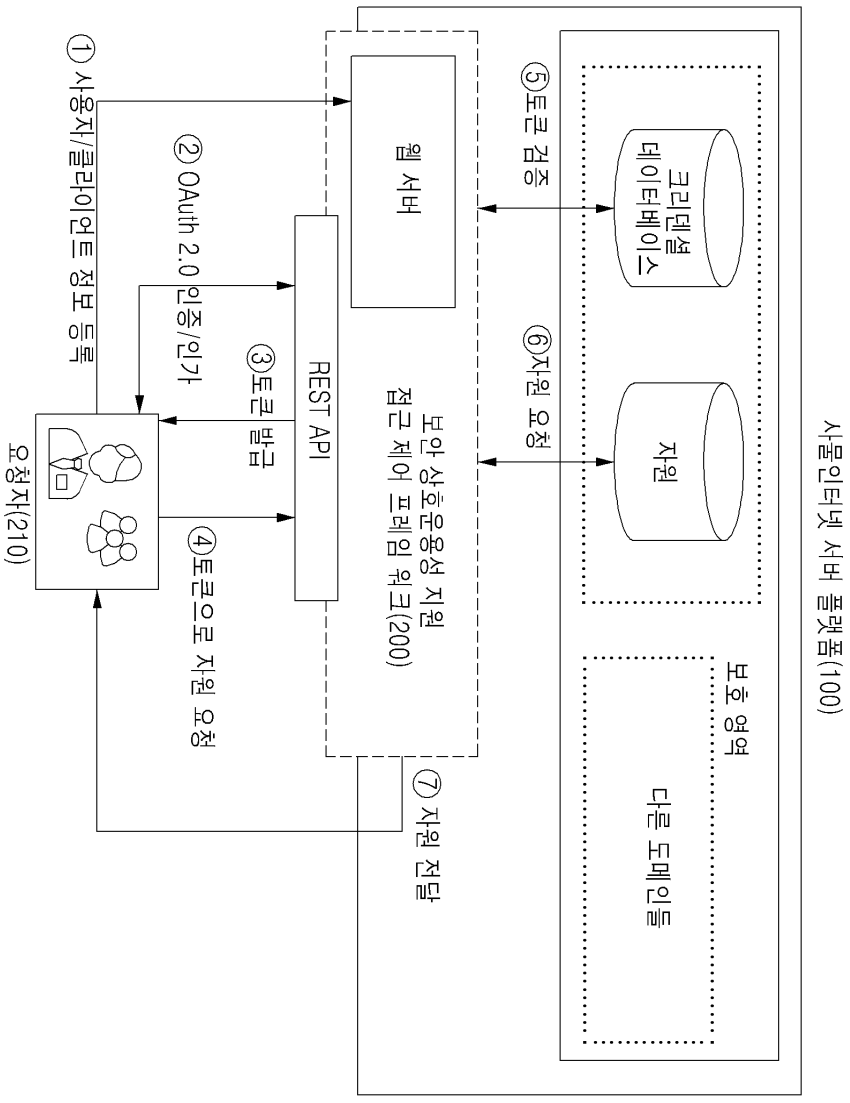
[0080] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

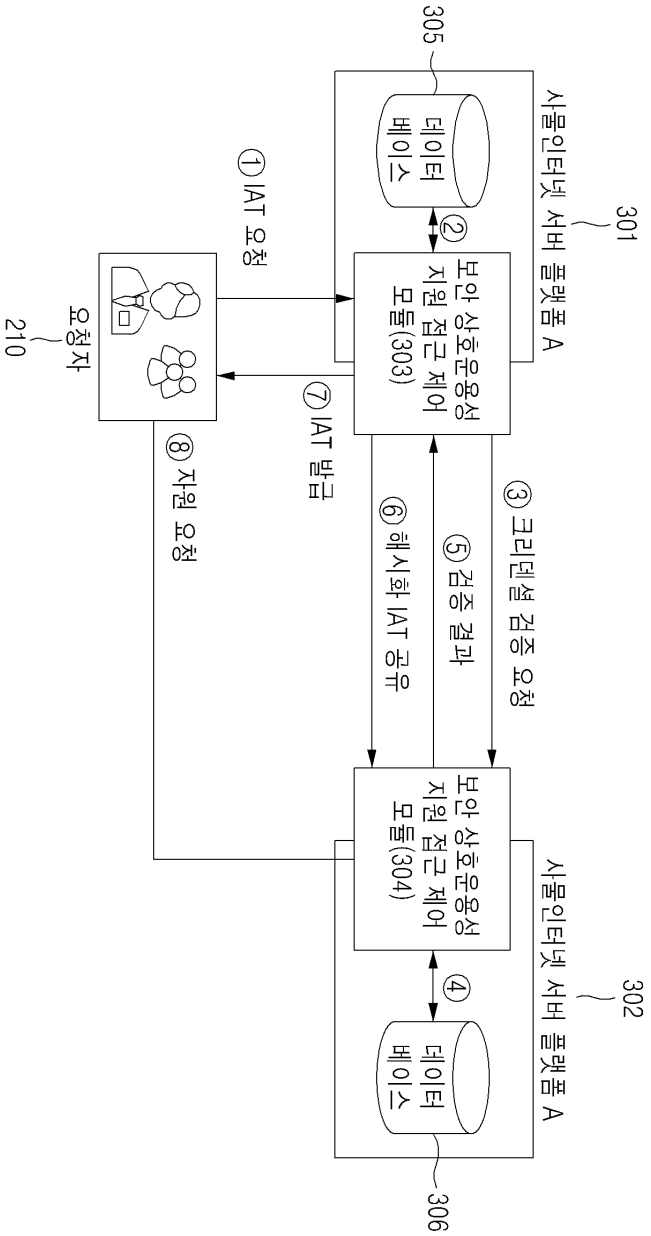
도면1



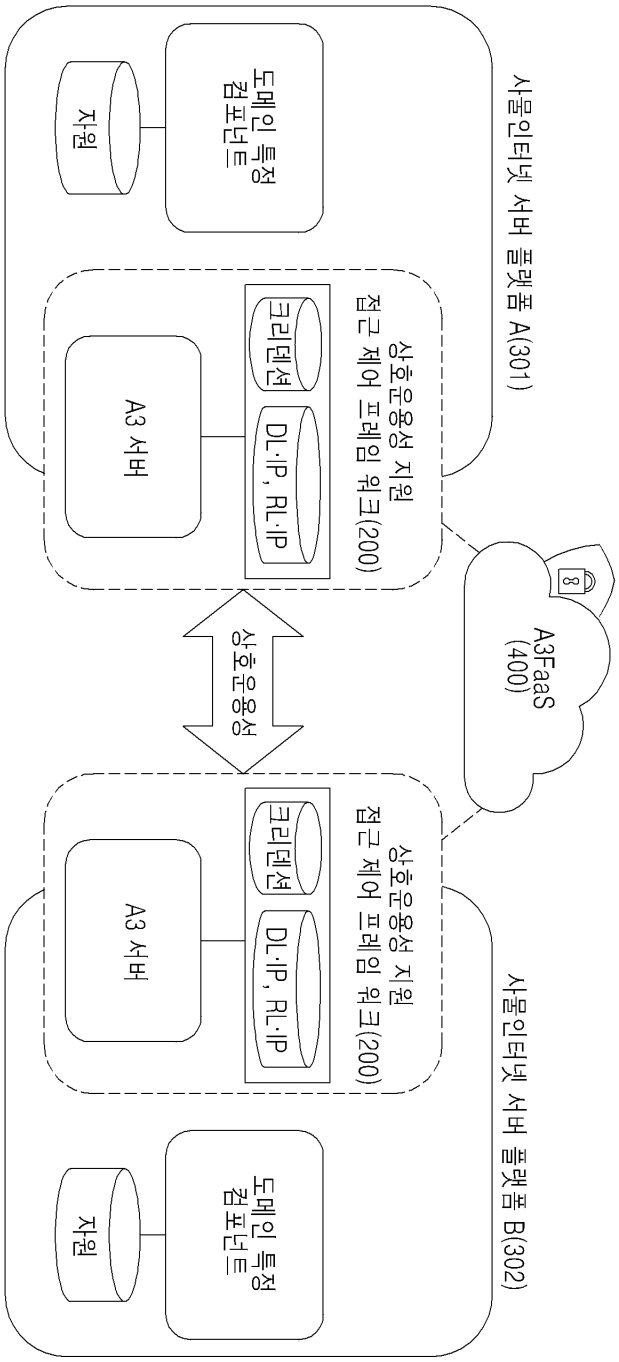
도면2


① 사용자/클라이언트 정보 등록
② OAuth 2.0 인증/인가
③토큰 발급
④토큰으로 자원 요청
요청자(210)
웹 서버
REST API
보안 상호운용성 지원
접근 제어 프레임 워크(200)
⑤토큰 검증
⑥자원 요청
⑦ 자원 전달
크리덴셜
데이터베이스
자원
보호 영역
다른 도메인들
사물인터넷 서버 플랫폼(100)

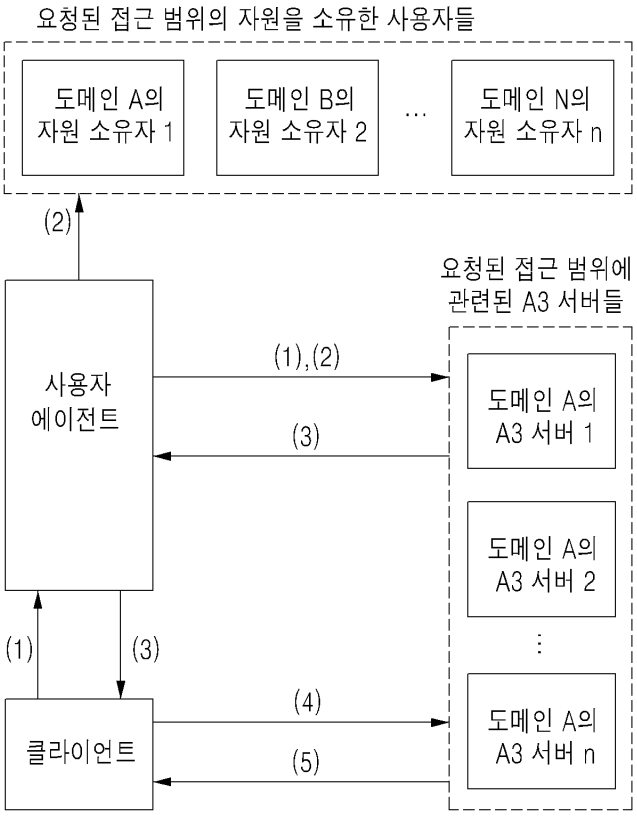
도면3


305
데이터베이스
사물인터넷 서버 플랫폼 A
301
① IAT 요청
②
보안 상호운용성 지원 접근 제어 모듈(303)
요청자
210
⑦ IAT 발급
⑧ 자원 요청
③ 크리덴셜 검증 요청
⑥ 해시화 IAT 공유
⑤ 검증 결과
보안 상호운용성 지원 접근 제어 모듈(304)
④
데이터베이스
306
사물인터넷 서버 플랫폼 A
302

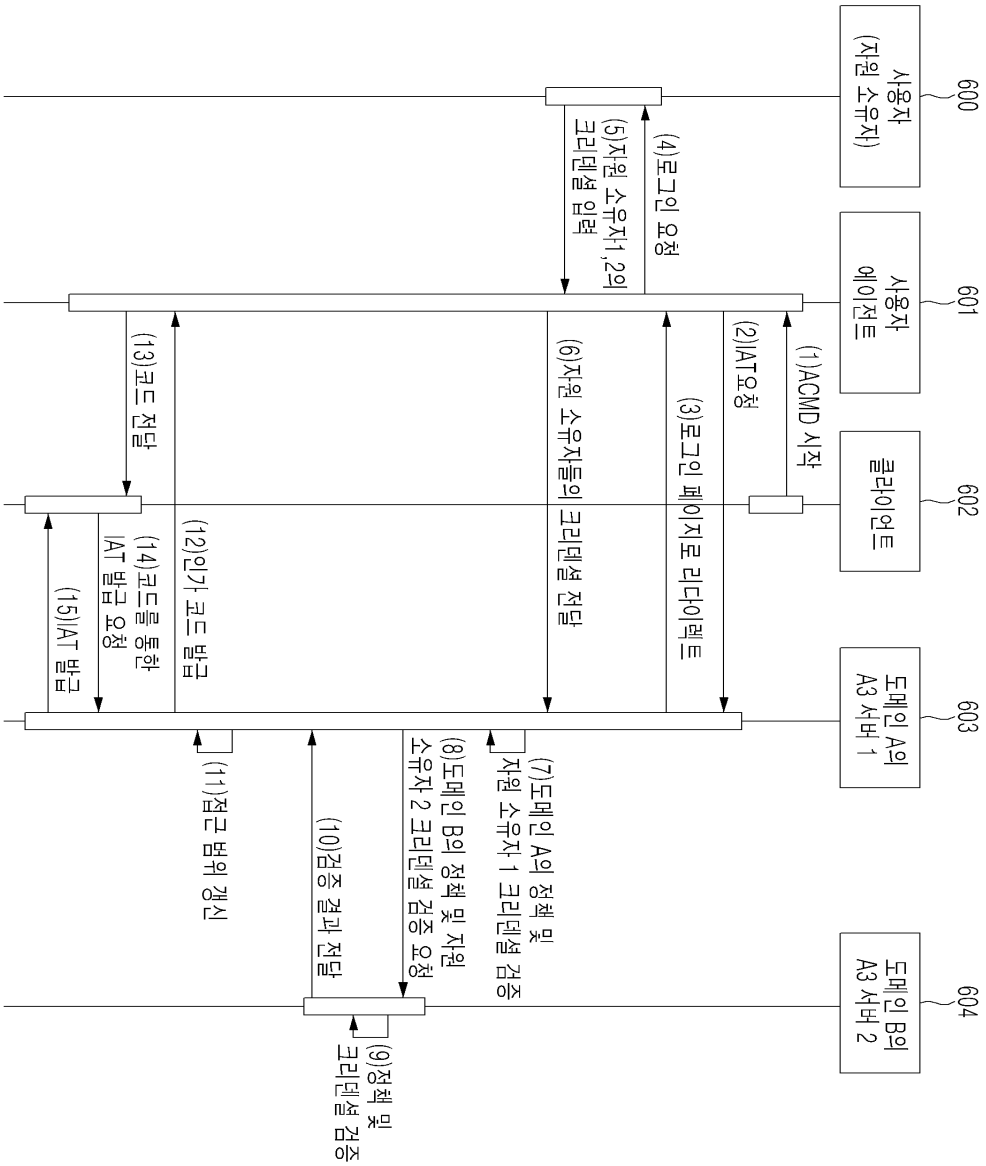
도면4


사물인터넷 서버 플랫폼 A(301)
도메인 특정 컴포넌트
자원
상호운용성 지원 접근 제어 프레임 워크(200)
A3 서버
크리덴셜
DL·IP, RL·IP
A3FaaS (400)
상호운용성
상호운용성 지원 접근 제어 프레임 워크(200)
A3 서버
크리덴셜
DL·IP, RL·IP
사물인터넷 서버 플랫폼 B(302)
도메인 특정 컴포넌트
자원

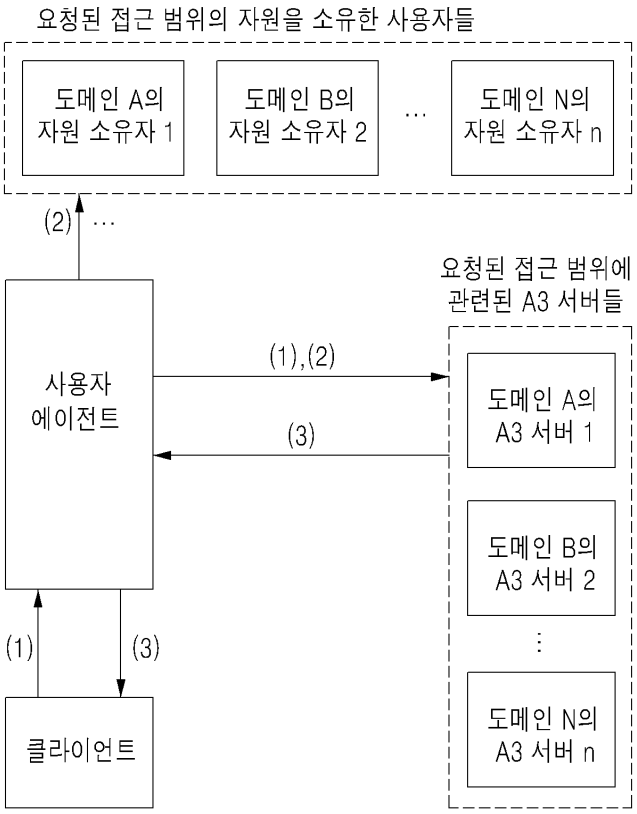
도면5


요청된 접근 범위의 자원을 소유한 사용자들
도메인 A의 자원 소유자 1
도메인 B의 자원 소유자 2
...
도메인 N의 자원 소유자 n
(2)
요청된 접근 범위에 관련된 A3 서버들
사용자 에이전트
(1),(2)
(3)
도메인 A의 A3 서버 1
도메인 A의 A3 서버 2
(1)
(3)
(4)
(5)
클라이언트
도메인 A의 A3 서버 n

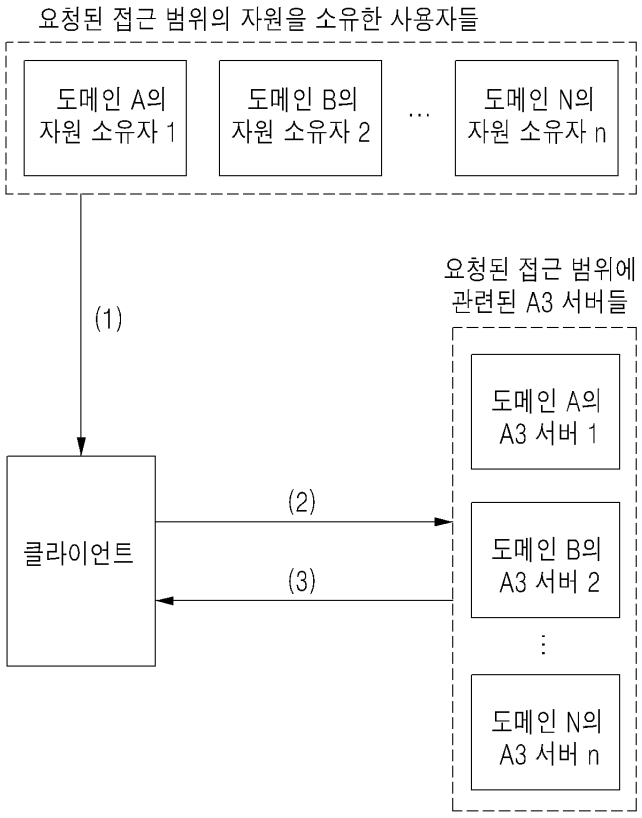
도면6


사용자
(자원 소유자)
600
사용자
에이전트
601
클라이언트
602
도메인 A의
A3 서버 1
603
도메인 B의
A3 서버 2
604
(1)ACMD 시작
(2)AT요청
(3)로그인 페이지로 리다이렉트
(4)로그인 요청
(5)자원 소유자1,2의
크리덴셜 입력
(6)자원 소유자들의 크리덴셜 전달
(7)도메인 A의 정책 및
자원 소유자 1 크리덴셜 검증
(8)도메인 B의 정책 및 자원
소유자 2 크리덴셜 검증 요청
(9)정책 및
크리덴셜 검증
(10)검증 결과 전달
(11)접근 범위 갱신
(12)인가 코드 발급
(13)코드 전달
(14)코드를 통한
AT 발급 요청
(15)AT 발급

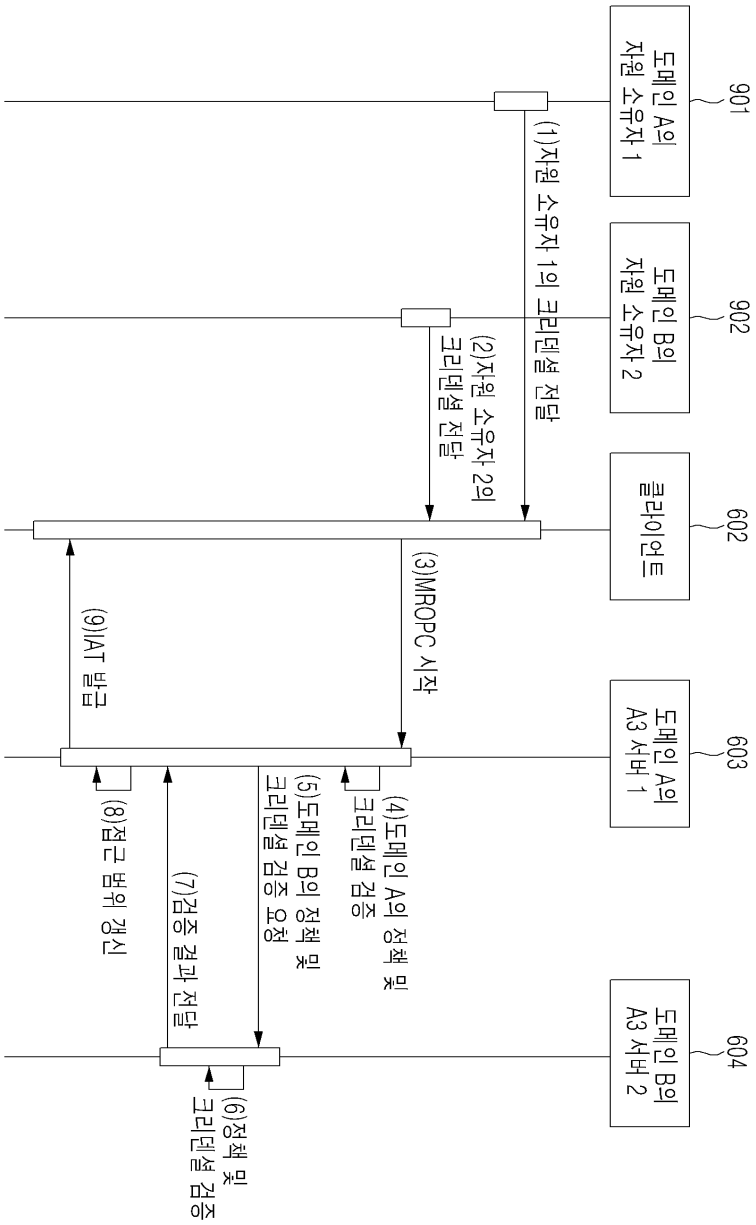
도면7


요청된 접근 범위의 자원을 소유한 사용자들
도메인 A의 자원 소유자 1
도메인 B의 자원 소유자 2
…
도메인 N의 자원 소유자 n
(2)
…
요청된 접근 범위에 관련된 A3 서버들
사용자 에이전트
(1),(2)
(3)
도메인 A의 A3 서버 1
도메인 B의 A3 서버 2
⋮
도메인 N의 A3 서버 n
(1)
(3)
클라이언트

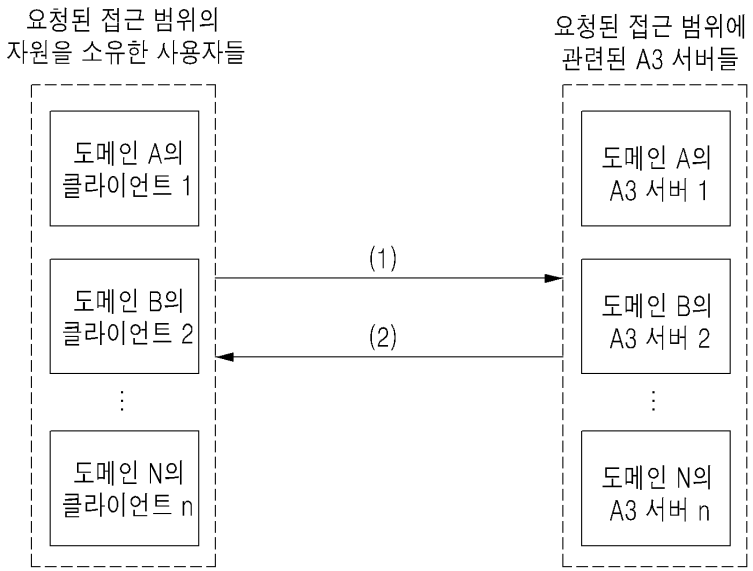
도면8


요청된 접근 범위의 자원을 소유한 사용자들
도메인 A의 자원 소유자 1
도메인 B의 자원 소유자 2
…
도메인 N의 자원 소유자 n
(1)
요청된 접근 범위에 관련된 A3 서버들
도메인 A의 A3 서버 1
클라이언트
(2)
(3)
도메인 B의 A3 서버 2
⋮
도메인 N의 A3 서버 n

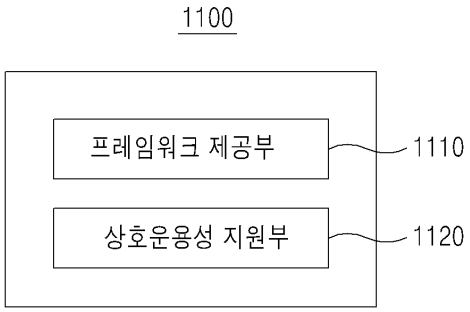
도면9


도메인 A의 자원 소유자 1
901
도메인 B의 자원 소유자 2
902
클라이언트
602
도메인 A의 A3 서버 1
603
도메인 B의 A3 서버 2
604
(1)자원 소유자 1의 크리덴셜 전달
(2)자원 소유자 2의 크리덴셜 전달
(3)MROPC 시작
(4)도메인 A의 정책 및 크리덴셜 검증
(5)도메인 B의 정책 및 크리덴셜 검증 요청
(6)정책 및 크리덴셜 검증
(7)검증 결과 전달
(8)접근 범위 갱신
(9)AT 발급

도면10



도면11



도면12