(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0098677
(43) 공개일자 2024년06월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 63/205 (2013.01)
(21) 출원번호 10-2022-0180651
(22) 출원일자 2022년12월21일
심사청구일자 2022년12월21일

(71) 출원인
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
양효식
서울특별시 광진구 광나루로 369, 101동 901호(군자동, 광진두산위브파크)
박명주
경기도 용인시 수지구 수풍로 38, 201동 103호(풍덕천동, 수지2차 삼성래미안)
신수현
서울특별시 광진구 능동로23길 15, B04호(군자동, KS금성빌)
(74) 대리인
양성보

전체 청구항 수 : 총 14 항

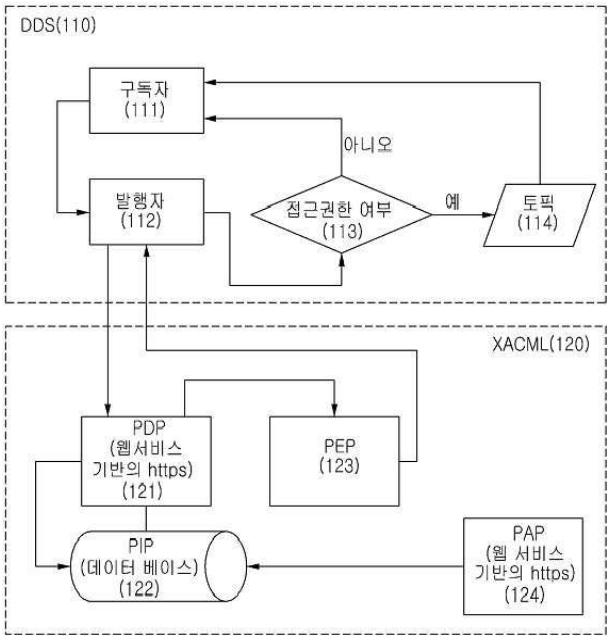
(54) 발명의 명칭 **XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법 및 시스템**

(57) 요 약

XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법 및 시스템이 제시된다. 본 발명에서 제안하는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법은 스마트그리드 통신에서 사용되는 구독 및 발행 기반 오픈 소프트웨어 DDS를 기반으로 구독자가 토픽을 요청하는 단계, 발행자가 상기 요청된

(뒷면에 계속)

대 표 도 - 도1



토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)에 요청하는 단계, 정책결정지점을 통해 정책정보지점(Policy Information Point; PIP)에 저장된 구독자의 역할 및 속성을 조회하는 단계, 정책정보지점을 통해 조회 결과를 상기 정책결정지점로 반환하는 단계, 정책결정지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 단계, 정책실행지점(Policy Enforcement Point; PEP)을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 단계, 발행자가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하는 단계 및 상기 분석 결과에 따라 구독자에게 데이터를 전송하는 단계를 포함한다.

이 발명을 지원한 국가연구개발사업

과제고유번호	1711154282
과제번호	2021M1A2A2065447
부처명	기획재정부
과제관리(전문)기관명	한국연구재단
연구사업명	기후변화대응기술개발
연구과제명	나노 전력그리드 시스템용 동적 전력관리시스템 개발
기 여 율	1/1
과제수행기관명	세종대학교 산학협력단
연구기간	2022.02.24 ~ 2023.02.23

명 세 서

청구범위

청구항 1

스마트그리드 통신에서 사용되는 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어 DDS를 기반으로 구독자가 토픽을 요청하는 단계;

발행자가 상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)에 요청하는 단계;

정책결정지점을 통해 정책정보지점(Policy Information Point; PIP)에 저장된 구독자의 역할 및 속성을 조회하는 단계;

정책정보지점을 통해 조회 결과를 상기 정책결정지점로 반환하는 단계;

정책결정지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 단계;

정책실행지점(Policy Enforcement Point; PEP)을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 단계;

발행자가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하는 단계; 및

상기 분석 결과에 따라 구독자에게 데이터를 전송하는 단계

를 포함하는 스마트그리드 통신 응용프로그램 수준의 보안 방법.

청구항 2

제1항에 있어서,

상기 발행자가 상기 요청된 토픽에 대하여 해당 구독자의 역할 및 속성을 분석하고, 역할 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점에 요청하는 단계는,

구독자로부터 정보 제공을 요청 받은 발행자는 XACML 포맷으로 요청 내용을 명시화하고, 해당 구독자의 정보 열람 권한을 확인하기 위하여 접근 정책에 대한 평가 및 결정을 담당하는 정책결정지점에 정책 결정을 의뢰하는

스마트그리드 통신 응용프로그램 수준의 보안 방법.

청구항 3

제1항에 있어서,

상기 정책정보지점을 통해 정책정보지점에 저장된 구독자의 역할 및 속성을 조회하는 단계는,

구독자의 모든 접근에 대한 권한 및 제어 정보가 저장되어 있는 정책정보지점에 정책결정지점이 정책정보 열람을 요청하는

스마트그리드 통신 응용프로그램 수준의 보안 방법.

청구항 4

제1항에 있어서,

상기 정책정보지점을 통해 조회 결과를 상기 정책결정지점로 반환하는 단계는,

정책정보지점이 접근 정책 관리를 수행하는 정책관리지점(Policy Administration Point; PAP)에서 지정한 구독자의 역할 및 권한에 대한 정보를 정책결정지점에 전송하는

스마트그리드 통신 응용프로그램 수준의 보안 방법.

청구항 5

제1항에 있어서,

상기 정책결정지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 단계는,

정책결정지점이 정책정보지점에서 전송된 구독자의 역할 및 권한에 대한 정보에 기초하여 접근 정책에 대한 평가 및 결정을 수행하고 평가 및 결과 정보를 정책실행지점에 전송하는

스마트그리드 통신 응용프로그램 수준의 보안 방법.

청구항 6

제1항에 있어서,

상기 정책실행지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 단계는,

정책실행지점이 정책결정지점의 평가 및 결과를 XACML 포맷으로 구조화 및 명문화하여 발행자에게 전송하는

스마트그리드 통신 응용프로그램 수준의 보안 방법.

청구항 7

제1항에 있어서,

상기 발행자가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하는 단계는,

평가 및 결과를 정책실행지점으로부터 전달 받은 발행자가 상기 평가 및 결과를 분석하고 분석한 결과에 따라 구독자에 대한 정보 제공 여부를 결정하는

스마트그리드 통신 응용프로그램 수준의 보안 방법.

청구항 8

스마트그리드 통신에서 사용되는 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어 DDS를 기반으로 토픽을 요청하는 구독자;

상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)에 요청하고, 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하며, 상기 분석 결과에 따라 구독자에게 데이터를 전송하는 발행자;

정책정보지점(Policy Information Point; PIP)에 저장된 구독자의 역할 및 속성을 조회하고, 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 정책결정지점;

조회 결과를 상기 정책결정지점로 반환하는 정책정보지점; 및

상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 정책실행지점(Policy Enforcement Point; PEP)

을 포함하는 스마트그리드 통신 응용프로그램 수준의 보안 시스템.

청구항 9

제8항에 있어서,

상기 발행자는,

구독자로부터 정보 제공을 요청 받아 XACML 포맷으로 요청 내용을 명시화하고, 해당 구독자의 정보 열람 권한을 확인하기 위하여 접근 정책에 대한 평가 및 결정을 담당하는 정책결정지점에 정책 결정을 의뢰하는

스마트그리드 통신 응용프로그램 수준의 보안 시스템.

청구항 10

제8항에 있어서,

상기 정책정보지점은,

구독자의 모든 접근에 대한 권한 및 제어 정보가 저장되어 있는 정책정보지점에 정책결정지점이 정책정보 열람을 요청하는

스마트그리드 통신 응용프로그램 수준의 보안 시스템.

청구항 11

제8항에 있어서,

상기 정책정보지점은,

접근 정책 관리를 수행하는 정책관리지점(Policy Administration Point; PAP)에서 지정한 구독자의 역할 및 권한에 대한 정보를 정책결정지점에 전송하는

스마트그리드 통신 응용프로그램 수준의 보안 시스템.

청구항 12

제8항에 있어서,

상기 정책결정지점은,

상기 정책정보지점에서 전송된 구독자의 역할 및 권한에 대한 정보에 기초하여 접근 정책에 대한 평가 및 결정을 수행하고 평가 및 결과 정보를 정책실행지점에 전송하는

스마트그리드 통신 응용프로그램 수준의 보안 시스템.

청구항 13

제8항에 있어서,

상기 정책실행지점은,

상기 정책결정지점의 평가 및 결과를 XACML 포맷으로 구조화 및 명문화하여 발행자에게 전송하는

스마트그리드 통신 응용프로그램 수준의 보안 시스템.

청구항 14

제8항에 있어서,

상기 발행자는,

상기 평가 및 결과를 상기 정책실행지점으로부터 전달 받아 상기 평가 및 결과를 분석하고 분석한 결과에 따라 구독자에 대한 정보 제공 여부를 결정하는

스마트그리드 통신 응용프로그램 수준의 보안 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 종래의 네트워크상 보안 기술은 단대단(End-to-End)에서 암호화와 복호화가 이루어지는 방식으로 이루어져 왔다. 이것과는 다르게 실제 각 단(End point)에서 수행되는 역할 또는 권한 및 책임에 대한 관리는 이러한 단대단 네트워크 통신상 보안 기술과 별도로 서버(Server)에서 각각의 클라이언트(Client)로 명시적이면서 유연하

게 제공하지 못해왔다. 해커가 특정 기기(예를 들어, 홈네트워크, 자동차, 지능형 검침인프라(Advanced Metering Infrastructure; AMI) 등)를 제어하고자 할 때 기기에서 제공하는 공개키를 이용하여 공개된 메시징 프로토콜(messaging protocol)에 따라 제어 명령을 암호화한 다음 해당 기기에 전송하면 데이터를 수신한 기기는 실제 사용자가 아닌 해커의 명령대로 조작이 가능해질 수 있다.

[0003] AMI-HES(Head End System)와 MDMS(Meter Data Management System) 사이의 데이터 통신에서 악의적인 의도를 가진 해커는 데이터(예를 들어, 사용량 데이터, 과금 데이터 등)를 조작하여 알려진 공개키로 암호화한 뒤 조작한 데이터를 HES로 전달 할 수 있다. 그렇기 때문에 IoT 통신에서는 데이터의 열람, 추가, 수정, 삭제 등에 대한 역할과 권한을 우선적으로 확인하고 평가하는 프로세스가 필요하다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 한국 공개특허 제10-2018-0016731호(2018.02.19)

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 기술적 과제는 스마트그리드에서 네트워크 통신을 이용한 자원의 접근 및 그 자원에 대한 역할과 권한을 제어하고 이러한 역할기반 제어를 통하여 해커가 부정한 방법으로 자원을 사용하는 것을 최소화 하는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법 및 시스템을 제공하는데 있다.

과제의 해결 수단

[0006] 일 측면에 있어서, 본 발명에서 제안하는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법은 스마트그리드 통신에서 사용되는 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어 DDS를 기반으로 구독자가 토픽을 요청하는 단계, 발행자가 상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)에 요청하는 단계, 정책결정지점을 통해 정책정보지점(Policy Information Point; PIP)에 저장된 구독자의 역할 및 속성을 조회하는 단계, 정책정보지점을 통해 조회 결과를 상기 정책결정지점로 반환하는 단계, 정책결정지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 단계, 정책실행지점(Policy Enforcement Point; PEP)을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 단계, 발행자가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하는 단계 및 상기 분석 결과에 따라 구독자에게 데이터를 전송하는 단계를 포함한다.

[0007] 상기 발행자가 상기 요청된 토픽에 대하여 해당 구독자의 역할 및 속성을 분석하고, 역할 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점에 요청하는 단계는 구독자로부터 정보 제공을 요청 받은 발행자는 XACML 포맷으로 요청 내용을 명시화하고, 해당 구독자의 정보 열람 권한을 확인하기 위하여 접근 정책에 대한 평가 및 결정을 담당하는 정책결정지점에 정책 결정을 의뢰한다.

[0008] 상기 정책정보지점을 통해 정책정보지점에 저장된 구독자의 역할 및 속성을 조회하는 단계는 구독자의 모든 접근에 대한 권한 및 제어 정보가 저장되어 있는 정책정보지점에 정책결정지점이 정책정보 열람을 요청한다.

[0009] 상기 정책정보지점을 통해 조회 결과를 상기 정책결정지점로 반환하는 단계는 정책정보지점이 접근 정책 관리를 수행하는 정책관리지점(Policy Administration Point; PAP)에서 지정한 구독자의 역할 및 권한에 대한 정보를 정책결정지점에 전송한다.

[0010] 상기 정책결정지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 단계는 정책결정지점이 정책정보지점에서 전송된 구독자의 역할 및 권한에 대한 정보에 기초하여 접근 정책에 대한 평가 및 결정을 수행하고 평가 및 결과 정보를 정책실행지점에 전송한다.

[0011] 상기 정책실행지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 단계는 정책실행지점이 정책결정지점의 평가 및 결과를 XACML 포맷으로 구조화 및 명문화하여 발행자에

게 전송한다.

[0012] 상기 발행자가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하는 단계는 평가 및 결과를 정책실행지점으로부터 전달 받은 발행자가 상기 평가 및 결과를 분석하고 분석한 결과에 따라 구독자에 대한 정보 제공 여부를 결정한다.

[0013] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템은 스마트그리드 통신에서 사용되는 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어 DDS를 기반으로 토픽을 요청하는 구독자, 상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)에 요청하고, 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하며, 상기 분석 결과에 따라 구독자에게 데이터를 전송하는 발행자, 정책정보지점(Policy Information Point; PIP)에 저장된 구독자의 역할 및 속성을 조회하고, 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 정책결정지점, 조회 결과를 상기 정책결정지점로 반환하는 정책정보지점 및 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 정책실행지점(Policy Enforcement Point; PEP)을 포함한다.

발명의 효과

[0014] 본 발명의 실시예들에 따르면 하는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법 및 시스템을 통해 스마트그리드에서 네트워크 통신을 이용한 자원의 접근 및 그 자원에 대한 역할과 권한을 제어하고 이러한 역할기반 제어를 통하여 해커가 부정한 방법으로 자원을 사용하는 것을 최소화할 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 모델의 개념도를 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법을 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템의 구성을 나타내는 도면이다.

도 4는 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 과정을 나타내는 도면이다.

도 5는 본 발명의 일 실시예에 따른 DDS 기반 DCPS 모델을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0016] 본 발명은 스마트그리드내에서의 통신에 대한 접근 통제를 IoT기반 응용프로그램인 DDS를 통하여 실행 가능한 모델 디자인 및 역할을 기반으로 한 접근 제어 방법에 관한 것이다. 구체적으로 각 역할들을 구조적으로 관리함과 동시에 XACML을 이용하여 명시적인 역할을 기반으로 한 접근 제어 및 이를 통한 구조적 시스템 보안에 관한 것이다.

[0017] 본 발명의 목적을 달성하기 위하여 IoT 통신 프로토콜을 위한 오픈소스 응용프로그램중에 하나인 DDS를 이용하여 구독자(subscriber) 및 발행자(publisher) 구조를 구현하고, 발행자와 구독자 사이에 RBAC(Role-Based Access Control)를 위한 정보 송/수신 규격으로써 XML 기반의 XACML을 기준 format으로 사용한다.

[0018] 본 발명의 실시예에 따른 RBAC는 역할 기반 접근제어를 위해 NIST에서 고안한 방법론이다. RBAC의 정보 보안 핵심은 사용자가 조직 내부에서 수행할 수 있는 역할에 따른 접근 제어를 기반으로 이루어진다. 본 발명에서는 IoT 통신을 구성하는 여러 가지 기기들 사이에서 지속적으로 증가하는 다량의 데이터 처리와 정보 보안을 위한 방법론으로써 XACML을 이용한 RBAC와 ABAC 방법론을 이용하려고 한다. 이러한 방법론의 구현을 위한 IoT 응용프로그램은 DDS를 이용할 수 있다. 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0020] 도 1은 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 모델의 개념도를 나타내는 도면이다.

[0021] 제안하는 XACML(eXtensible Access Control Markup Language)(120)ㄱ과 DDS(Data Distribution Service)(12

0)를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 모델을 이용하여 네트워크 통신을 이용한 스마트그리드에서의 접근 제어 및 역할을 기반으로 한 보안 방법을 제안한다.

[0022] 본 발명의 실시예에 따르면, 스마트그리드 통신에 사용이 가능한 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어인 DDS를 기반으로 구독자(subscriber)가 어떠한 토픽을 요청했을 때 해당 구독자(subscriber)의 역할(Role)을 분석하고 분석된 결과에 따라 접근을 제어하며 이러한 역할에 따른 제어를 통하여 스마트그리드 통신에서의 원활한 보안성을 제공한다.

[0023] DDS를 기반으로 구독자(subscriber)(111)가 어떠한 토픽을 요청하면, 요청을 받은 발행자(publisher)(112)는 XACML(120)의 PDP(Policy Decision Point)(121)에 구독자(subscriber)(111)의 역할(Role)을 요청한다. PDP(121)는 구독자(111)의 역할이 저장되어 있는 데이터베이스인 PIP(Policy Information Point)(122)를 조회한다.

[0024] 조회된 결과는 PEP(Policy Enforcement Point)(123)에서 구독자(111)의 역할을 평가한 뒤 XACML 포맷으로 명시하여 발행자(112)에게 전달한다. PAP(Policy Administration Point)(124)는 https를 기반으로 한 웹서비스이며 이곳에서 각 구독자(111)들의 역할을 관리한다.

[0025] 정책평가결과를 PEP(123)로부터 전달 받은 발행자(112)는 정책평가결과를 분석(113)하고 분석한 결과에 따라 구독자(111)에 대한 정보 제공(114) 여부를 결정한다.

[0027] 도 2는 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법을 설명하기 위한 흐름도이다.

[0028] 제안하는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 방법은 스마트그리드 통신에서 사용되는 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어 DDS를 기반으로 구독자가 토픽을 요청하는 단계(210), 발행자가 상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)에 요청하는 단계(220), 정책결정지점을 통해 정책정보지점(Policy Information Point; PIP)에 저장된 구독자의 역할 및 속성을 조회하는 단계(230), 정책정보지점을 통해 조회 결과를 상기 정책결정지점로 반환하는 단계(240), 정책결정지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송하는 단계(250), 정책실행지점(Policy Enforcement Point; PEP)을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송하는 단계(260), 발행자가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정하는 단계(270) 및 상기 분석 결과에 따라 구독자에게 데이터를 전송하는 단계(280)를 포함한다.

[0029] 단계(210)에서, 스마트그리드 통신에서 사용되는 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어 DDS를 기반으로 구독자가 토픽을 요청한다.

[0030] DDS의 구독자 및 발행자 간 네트워크 통신에서 역할기반접근제어(Role Base Access Control; RBAC)를 위해 정책결정지점에 정책결정을 요청할 정책요청부분을 포함할 수 있다. 본 발명의 실시예에 따른 DDS는 국제 표준화 기구 OMG(Object Management Group)에서 구현한 실시간 데이터 분산 서비스를 위한 표준 응용프로그램이다. 많은 수의 개체간 실시간 통신이 필요한 분야에서 사용이 가능한 미들웨어(middle-ware)이다.

[0031] 단계(220)에서, 발행자가 상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)에 요청한다.

[0032] 정책요청부분에서 XACML 포맷으로 요청 내용을 명시화하는 XACML 변환기를 포함할 수 있다.

[0033] 구독자로부터 정보 제공을 요청 받은 발행자는 XACML 포맷으로 요청 내용을 명시화하고, 해당 구독자의 정보 열람 권한을 확인하기 위하여 접근 정책에 대한 평가 및 결정을 담당하는 정책결정지점에 정책 결정을 의뢰한다.

[0034] 본 발명의 실시예에 따른 XACML은 요청한 권한과 역할에 대하여 여러가지 다양한 정책(policy)과 규칙(rule)을 하나의 XML을 기반으로 표현이 가능한 문서화 표준이다. 현재 XACML은 XML뿐만 아니라 HTTP 통신에서 REST(REpresentational State Transfer)를 이용한 JSON(JavaScript Object Notation) 형태의 표준화가 진행 되었다.

[0035] 단계(230)에서, 정책결정지점을 통해 정책정보지점(Policy Information Point; PIP)에 저장된 구독자의 역할 및

속성을 조회한다. 구독자의 모든 접근에 대한 권한 및 제어 정보가 저장되어 있는 정책정보지점에 정책결정지점이 정책정보 열람을 요청한다.

[0036] 단계(240)에서, 정책정보지점을 통해 조회 결과를 상기 정책결정지점로 반환한다.

[0037] 정책정보지점이 접근 정책 관리를 수행하는 정책관리지점(Policy Administration Point; PAP)에서 지정한 구독자의 역할 및 권한에 대한 정보를 정책결정지점에 전송한다. 정책관리지점은 https를 기반으로 한 웹서비스이며 이곳에서 각 구독자들의 역할을 관리한다.

[0038] 단계(250)에서, 정책결정지점을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송한다.

[0039] 정책결정지점이 정책정보지점에서 전송된 구독자의 역할 및 권한에 대한 정보에 기초하여 접근 정책에 대한 평가 및 결정을 수행하고 평가 및 결과 정보를 정책실행지점에 전송한다.

[0040] 단계(260)에서, 정책실행지점(Policy Enforcement Point; PEP)을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송한다.

[0041] 정책실행지점이 정책결정지점의 평가 및 결과를 XACML 포맷으로 구조화 및 명문화하여 발행자에게 전송한다.

[0042] 단계(270)에서, 발행자가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정한다.

[0043] 상기 정책실행지점 에서 전달받은 정책결정내용인 XACML 포맷을 분석하는 XACML 분석기를 포함할 수 있다. 평가 및 결과를 정책실행지점으로부터 전달 받은 발행자가 상기 평가 및 결과를 분석하고 분석한 결과에 따라 구독자에 대한 정보 제공 여부를 결정한다.

[0044] 단계(280)에서, 상기 분석 결과에 따라 구독자에게 데이터를 전송한다.

[0045] 상기 분석 결과에 따라 구독자에 대한 접근 권한 인정 여부를 판단하고(281), 구독자에 대한 접근 권한이 인정된 경우 토픽 데이터를 구독자에게 발행한다(282). 반면에, 구독자에 대한 접근 권한이 인정되지 않은 경우 '권한 없음'을 나타내는 메시지 또는 에러 메시지를 구독자에게 발행한다(283).

[0046] 본 발명의 실시예에 따라 정보에 대한 접근 통제 및 역할에 따른 권한 통제가 이뤄지면 해커에 의한 불법적인 정보 및 자원에 대한 접근 또는 열람을 방지할 수 있는 기술적 근거를 확보할 수 있다.

[0048] 도 3은 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템의 구성을 나타내는 도면이다.

[0049] 본 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)은 프로세서(310), 버스(320), 네트워크 인터페이스(330), 메모리(340) 및 데이터베이스(350)를 포함할 수 있다. 메모리(340)는 운영체제(341) 및 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 루틴(342)을 포함할 수 있다. 프로세서(310)는 PDP(Policy Decision Point)(311), PIP(Policy Decision Point)(312) 및 PEP(Policy Enforcement Point)(313)를 포함할 수 있다. 다른 실시예들에서 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)은 도 3의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)은 디스플레이나 트랜시버(transceiver)와 같은 다른 구성요소들을 포함할 수도 있다.

[0050] 메모리(340)는 컴퓨터에서 판독 가능한 기록 매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 또한, 메모리(340)에는 운영체제(341)와 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 루틴(342)을 위한 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 드라이브 메커니즘(drive mechanism, 미도시)을 이용하여 메모리(340)와는 별도의 컴퓨터에서 판독 가능한 기록 매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록 매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록 매체(미도시)를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록 매체가 아닌 네트워크 인터페이스(330)를 통해 메모리(340)에 로딩될 수도 있다.

[0051] 버스(320)는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)의 구성요소들간의

통신 및 데이터 전송을 가능하게 할 수 있다. 버스(320)는 고속 시리얼 버스(high-speed serial bus), 병렬 버스(parallel bus), SAN(Storage Area Network) 및/또는 다른 적절한 통신 기술을 이용하여 구성될 수 있다.

[0052] 네트워크 인터페이스(330)는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)을 컴퓨터 네트워크에 연결하기 위한 컴퓨터 하드웨어 구성요소일 수 있다. 네트워크 인터페이스(330)는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)을 무선 또는 유선 커넥션을 통해 컴퓨터 네트워크에 연결시킬 수 있다.

[0053] 스마트그리드 통신에서 사용되는 구독자(subscriber)(361) 및 발행자(publisher)(362)를 포함하는 오픈 소프트웨어 DDS(360)를 기반으로 구독자(361)가 발행자(362)에게 토픽을 요청한다. DDS의 구독자 및 발행자 간 네트워크 통신에서 역할기반접근제어(Role Base Access Control; RBAC)를 위해 정책결정지점에 정책결정을 요청할 정책요청부분을 포함할 수 있다. 발행자(362)가 상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 네트워크 인터페이스(330)를 통해 PDP(311)에 요청한다.

[0054] 데이터베이스(350)는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안을 위해 필요한 모든 정보를 저장 및 유지하는 역할을 할 수 있다. 도 3에서는 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)의 내부에 데이터베이스(350)를 구축하여 포함하는 것으로 도시하고 있으나, 이에 한정되는 것은 아니며 시스템 구현 방식이나 환경 등에 따라 생략될 수 있고 혹은 전체 또는 일부의 데이터베이스가 별개의 다른 시스템 상에 구축된 외부 데이터베이스로서 존재하는 것 또한 가능하다.

[0055] 프로세서(310)는 기본적인 산술, 로직 및 XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)의 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(340) 또는 네트워크 인터페이스(330)에 의해, 그리고 버스(320)를 통해 프로세서(310)로 제공될 수 있다. 프로세서(310)는 PDP(311), PIP(312) 및 PEP(313)를 위한 프로그램 코드를 실행하도록 구성될 수 있다. 이러한 프로그램 코드는 메모리(340)와 같은 기록 장치에 저장될 수 있다.

[0056] PDP(311), PIP(312) 및 PEP(313)는 도 2의 단계들(210~280)을 수행하기 위해 구성될 수 있다.

[0057] XACML과 DDS를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 시스템(300)은 PDP(311), PIP(312) 및 PEP(313)를 포함할 수 있다.

[0058] 스마트그리드 통신에서 사용되는 구독(subscriber) 및 발행(publisher) 기반 오픈 소프트웨어 DDS(360)를 기반으로 구독자(361)가 토픽을 요청한다.

[0059] DDS의 구독자(361) 및 발행자(362) 간 네트워크 통신에서 역할기반접근제어(Role Base Access Control; RBAC)를 위해 정책결정지점에 정책결정을 요청할 정책요청부분을 포함할 수 있다. 본 발명의 실시예에 따른 DDS는 국제 표준화 기구 OMG(Object Management Group)에서 구현한 실시간 데이터 분산 서비스를 위한 표준 응용프로그램이다. 많은 수의 개체간 실시간 통신이 필요한 분야에서 사용이 가능한 미들웨어(middle-ware)이다.

[0060] 발행자(362)가 상기 요청된 토픽에 대하여 해당 구독자의 역할(Role) 및 속성을 분석하고, 역할(Role) 및 속성에 대한 분석된 결과를 XACML로 구성하여 정책결정지점(Policy Decision Point; PDP)(311)에 요청한다.

[0061] 정책요청부분에서 XACML 포맷으로 요청 내용을 명시화하는 XACML 변환기를 포함할 수 있다.

[0062] 구독자(361)로부터 정보 제공을 요청 받은 발행자(362)는 XACML 포맷으로 요청 내용을 명시화하고, 해당 구독자(361)의 정보 열람 권한을 확인하기 위하여 접근 정책에 대한 평가 및 결정을 담당하는 정책결정지점)(311)에 정책 결정을 의뢰한다.

[0063] 본 발명의 실시예에 따른 XACML은 요청한 권한과 역할에 대하여 여러가지 다양한 정책(policy)과 규칙(rule)을 하나의 XML을 기반으로 표현이 가능한 문서화 표준이다. 현재 XACML은 XML뿐만 아니라 HTTP 통신에서 REST(REpresentational State Transfer)를 이용한 JSON(JavaScript Object Notation) 형태의 표준화가 진행 되었다.

[0064] 정책결정지점)(311)을 통해 정책정보지점(Policy Information Point; PIP)(312)에 저장된 구독자의 역할 및 속성을 조회한다. 구독자의 모든 접근에 대한 권한 및 제어 정보가 저장되어 있는 정책정보지점(312)에 정책결정지점(311)이 정책정보 열람을 요청한다.

[0065] 정책정보지점(312)을 통해 조회 결과를 상기 정책결정지점(311)로 반환한다.

[0066] 정책정보지점(312)이 접근 정책 관리를 수행하는 정책관리지점(Policy Administration Point; PAP)에서 지정한 구독자의 역할 및 권한에 대한 정보를 정책결정지점(311)에 전송한다. 정책관리지점은 https를 기반으로 한 웹 서비스이며 이곳에서 각 구독자들의 역할을 관리한다.

[0067] 정책결정지점(311)을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 전송한다.

[0068] 정책결정지점(311)이 정책정보지점(312)에서 전송된 구독자의 역할 및 권한에 대한 정보에 기초하여 접근 정책에 대한 평가 및 결정을 수행하고 평가 및 결과 정보를 정책실행지점에 전송한다.

[0069] 정책실행지점(Policy Enforcement Point; PEP)(313)을 통해 상기 구독자의 역할 및 속성에 대한 평가 및 결과를 XACML로 구성하여 발행자에게 전송한다.

[0070] 정책실행지점(313)이 정책결정지점의 평가 및 결과를 XACML 포맷으로 구조화 및 명문화하여 발행자에게 전송한다.

[0071] 발행자(362)가 상기 XACML로 구성된 평가 및 결과에 대해 분석하여 구독자의 접근권한을 결정한다.

[0072] 상기 정책실행지점(313)에서 전달받은 정책결정내용인 XACML 포맷을 분석하는 XACML 분석기를 포함할 수 있다. 평가 및 결과를 정책실행지점(313)으로부터 전달 받은 발행자(362)가 상기 평가 및 결과를 분석하고 분석한 결과에 따라 구독자에 대한 정보 제공 여부를 결정한다.

[0073] 상기 분석 결과에 따라 구독자(361)에게 데이터를 전송한다.

[0074] 발행자(362)는 상기 분석 결과에 따라 구독자(361)에 대한 접근 권한 인정 여부를 판단하고, 구독자에 대한 접근 권한이 인정된 경우 토픽 데이터를 구독자에게 발행한다. 반면에, 구독자에 대한 접근 권한이 인정되지 않은 경우 '권한 없음'을 나타내는 메시지 또는 에러 메시지를 구독자(361)에게 발행한다.

[0075] 본 발명의 실시예에 따라 정보에 대한 접근 통제 및 역할에 따른 권한 통제가 이뤄지면 해커에 의한 불법적인 정보 및 자원에 대한 접근 또는 열람을 방지할 수 있는 기술적 근거를 확보할 수 있다.

[0077] 도 4는 본 발명의 일 실시예에 따른 XACML과 DDS를 이용한 스마트그리드 통신 과정을 나타내는 도면이다.

[0078] 제안하는 DDS(Data Distribution Service)(410)과 XACML(eXtensible Access Control Markup Language)(420)를 이용한 스마트그리드 통신 응용프로그램 수준의 보안 모델을 이용하여 네트워크 통신을 이용한 스마트그리드에서의 접근 제어 및 역할을 기반으로 한 보안 방법을 제안한다.

[0079] 본 발명의 실시예에 따르면, 스마트그리드 통신에 사용이 가능한 구독자(411) 및 발행자(412) 기반 오픈 소프트웨어인 DDS(410)를 기반으로 구독자(411)가 어떠한 토픽을 요청했을 때 해당 구독자(411)의 역할(Role)을 분석하고 분석된 결과에 따라 접근을 제어하며 이러한 역할에 따른 제어를 통하여 스마트그리드 통신에서의 원활한 보안성을 제공한다.

[0080] DDS(410)를 기반으로 구독자(411)가 어떠한 토픽을 요청하면, 요청을 받은 발행자(412)는 XACML(420)의 PDP(Policy Decision Point)(421)에 구독자(411)의 역할(Role)을 요청한다. PDP(421)는 구독자(411)의 역할이 저장되어 있는 데이터베이스인 PIP(Policy Information Point)(422)를 조회한다.

[0081] 조회된 결과는 PEP(Policy Enforcement Point)(423)에서 구독자(411)의 역할을 평가한 뒤 XACML(420)으로 명시하여 발행자(412)에게 전달한다. PAP(Policy Administration Point)(424)는 https를 기반으로 한 웹서비스이며 이곳에서 각 구독자(411)들의 역할을 관리한다.

[0082] 본 발명의 실시예에 따른 XACML(420)은 요청한 권한과 역할에 대하여 여러가지 다양한 정책(policy)과 규칙(rule)을 하나의 XML을 기반으로 표현이 가능한 문서화 표준이다. 현재 XACML(420)은 XML뿐만 아니라 HTTP 통신에서 REST(REpresentational State Transfer)(430)를 이용한 JSON(JavaScript Object Notation) 형태의 표준화가 진행 되었다.

[0083] 정책평가결과를 PEP(423)로부터 전달 받은 발행자(412)는 정책평가결과를 분석(413)하고 분석한 결과에 따라 구독자(411)에 대한 정보 제공(다시 말해, 토픽) 여부를 결정한다.

[0085] 도 5는 본 발명의 일 실시예에 따른 DDS 기반 DCPS 모델을 설명하기 위한 도면이다.

[0086] DDS는 국제 표준화 기구 OMG(Object Management Group)에서 구현한 실시간 데이터 분산 서비스를 위한 표준 응용프로그램이다. 많은 수의 개체간 실시간 통신이 필요한 분야에서 사용이 가능한 미들웨어(middle-ware)이다. 일반적인 서버/클라이언트 방식이 아닌 발행자/구독자 방식의 메시징 프로토콜 구조를 가지고 있으며 QoS(Quality of Service) 파라미터를 제공한다. 많은 메시징 프로토콜 구조를 가진 응용프로그램/미들웨어들은 DCPS(Data-Centric Publish-Subscribe) 모델을 사용하고 있으며, DDS 또한 DCPS 모델을 사용하고 있다. 분산 공유 메모리(Distributed shared memory)가 오래된 모델이기는 하지만 네트워크에서 비효율적이고 확장성과 유연성을 지원하지 않기 때문에 DCPS모델을 많은 실시간 응용프로그램에서 사용하게 되었다고 본다. DDS에서 구현되는 DCPS의 기본 모델은 도 5와 같이 나타낼 수 있다.

[0087] 도 5와 같이, 복수의 도메인 참여자(540, 550)에 대한 발행자는 복수의 토픽(Topic)1, 2, 3에 메시지를 송신하고, 복수의 도메인 참여자(510, 520)에 대한 구독자는 토픽의 메시지를 수신한다. 발행자는 데이터 게시자(DataWriter) 개체를 통하여 메시지를 게시하며 데이터 게시자 또는 자신과 연결된 QoS(530)에 따라 메시지 게시를 수행한다. 구독자는 데이터 판독기(DataReader) 개체를 통하여 수신 된 메시지에 접근하며 데이터에 QoS(530)에 연결한다. 토픽은 도 5에서와 같이 연결된 영역에서 이름이 유일해야 하며, 메시지 데이터의 유형이나 데이터 자체와 연관된 QoS(530)를 연결한다. 토픽의 QoS(530) 외에도 연결된 데이터 게시자의 QoS(530)와 발행자의 QoS(530)는 발행자의 동작을 제어하며, 연결된 데이터 판독기의 QoS(530)와 구독자의 QoS(530)는 구독자의 동작을 제어하게 된다. OMG에서는 DDS의 커머셜(commercial) 버전과 오픈소스 버전을 제공하고 있으며, 본 발명의 실시예에서는 오픈소스 버전을 이용하여 구현하였다.

[0089] 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.

[0090] 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.

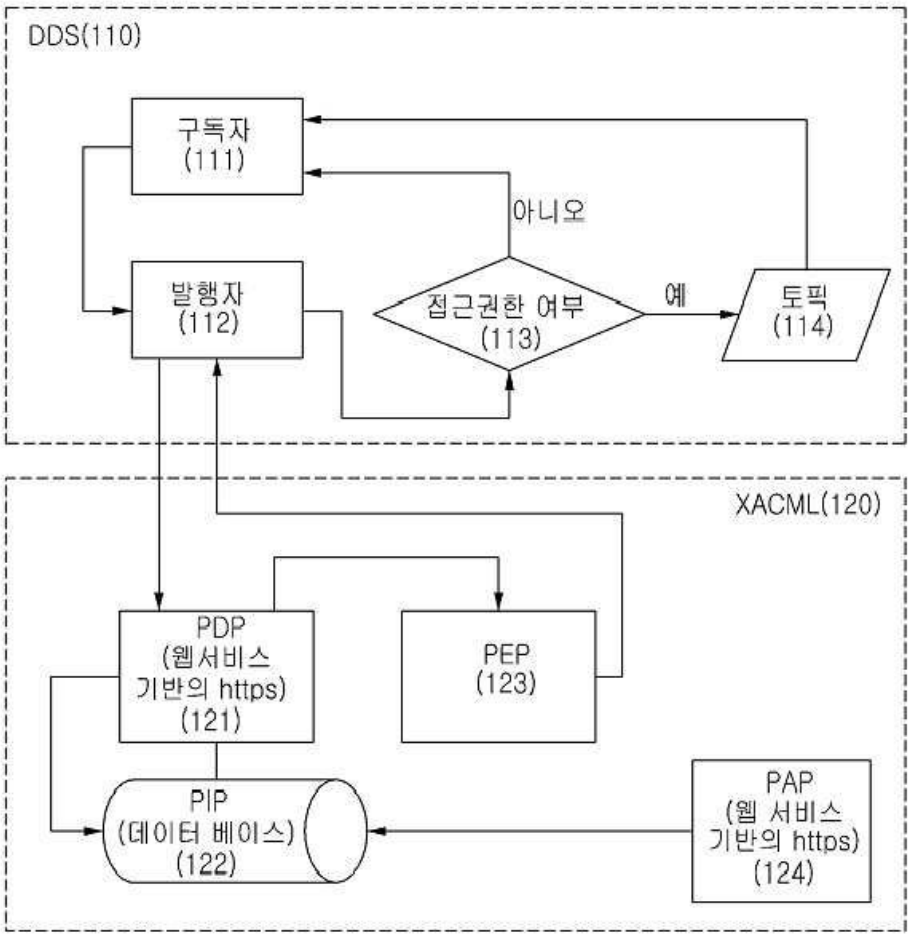
[0091] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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.

[0092] 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.

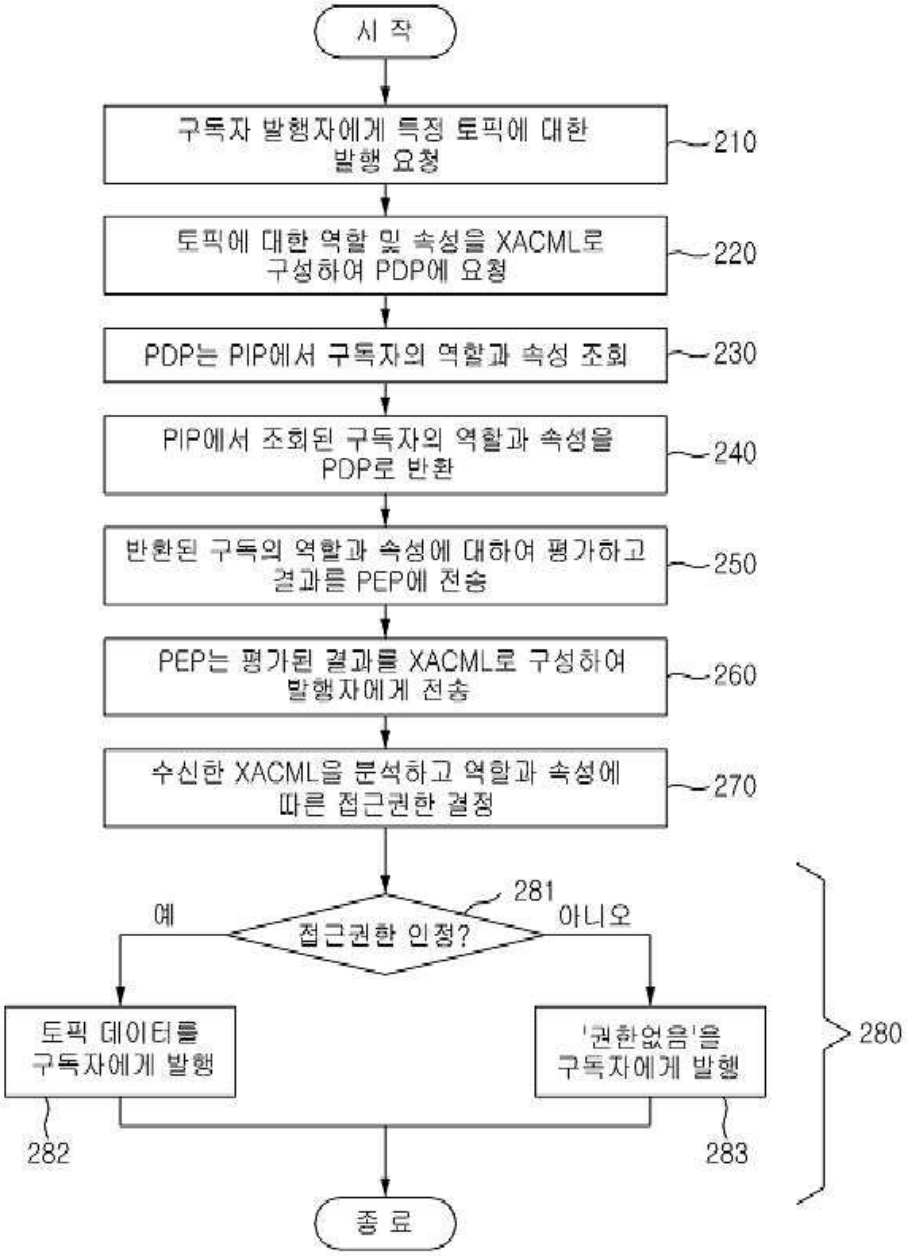
[0093] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

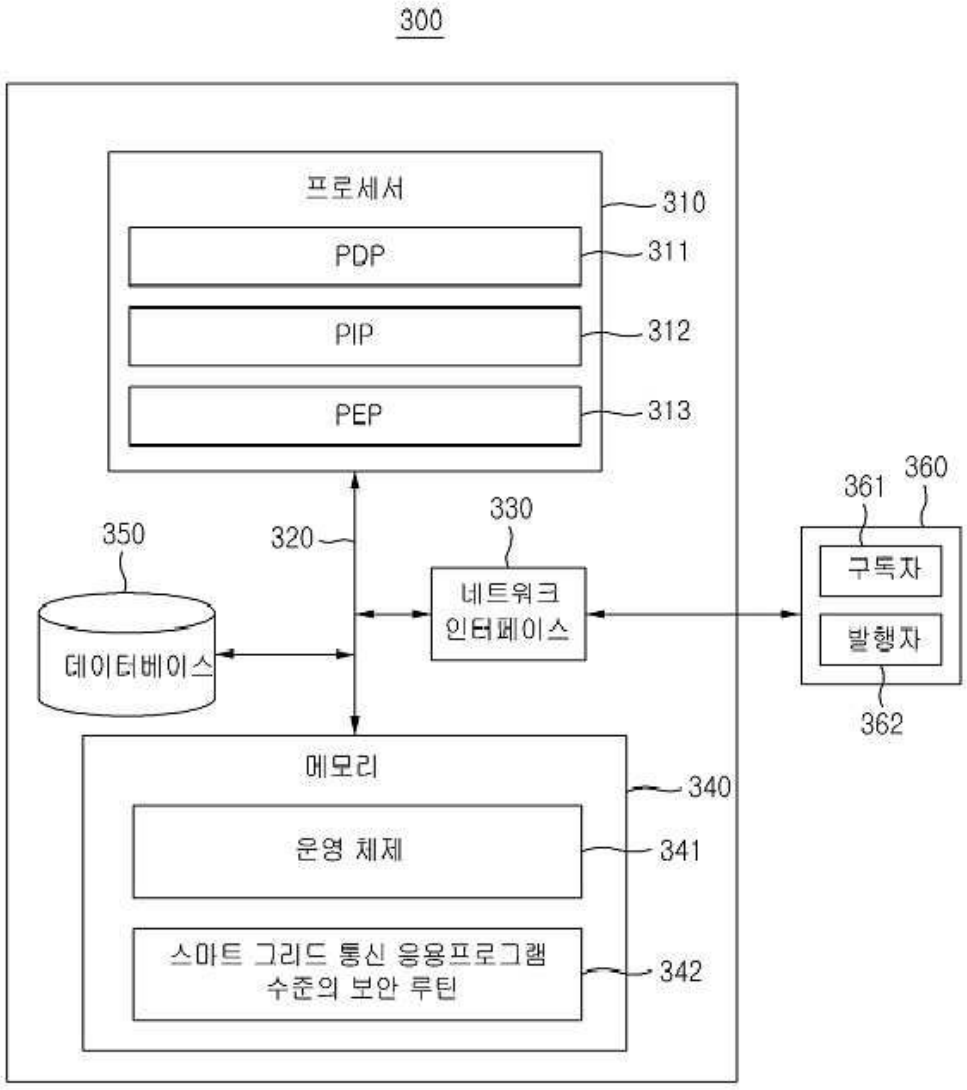
도면1



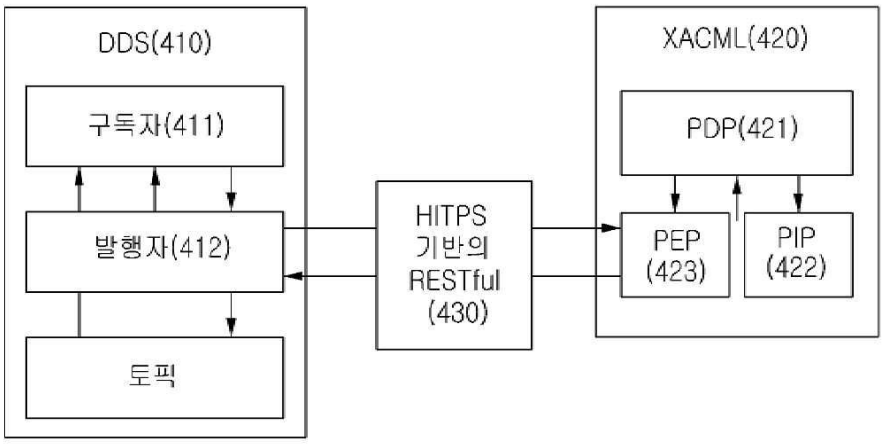
도면2


시 작
구독자 발행자에게 특정 토픽에 대한 발행 요청
210
토픽에 대한 역할 및 속성을 XACML로 구성하여 PDP에 요청
220
PDP는 PIP에서 구독자의 역할과 속성 조회
230
PIP에서 조회된 구독자의 역할과 속성을 PDP로 반환
240
반환된 구독의 역할과 속성에 대하여 평가하고 결과를 PEP에 전송
250
PEP는 평가된 결과를 XACML로 구성하여 발행자에게 전송
260
수신한 XACML을 분석하고 역할과 속성에 따른 접근권한 결정
270
281
예
접근권한 인정?
아니오
토픽 데이터를 구독자에게 발행
'권한없음'을 구독자에게 발행
280
282
283
종 료

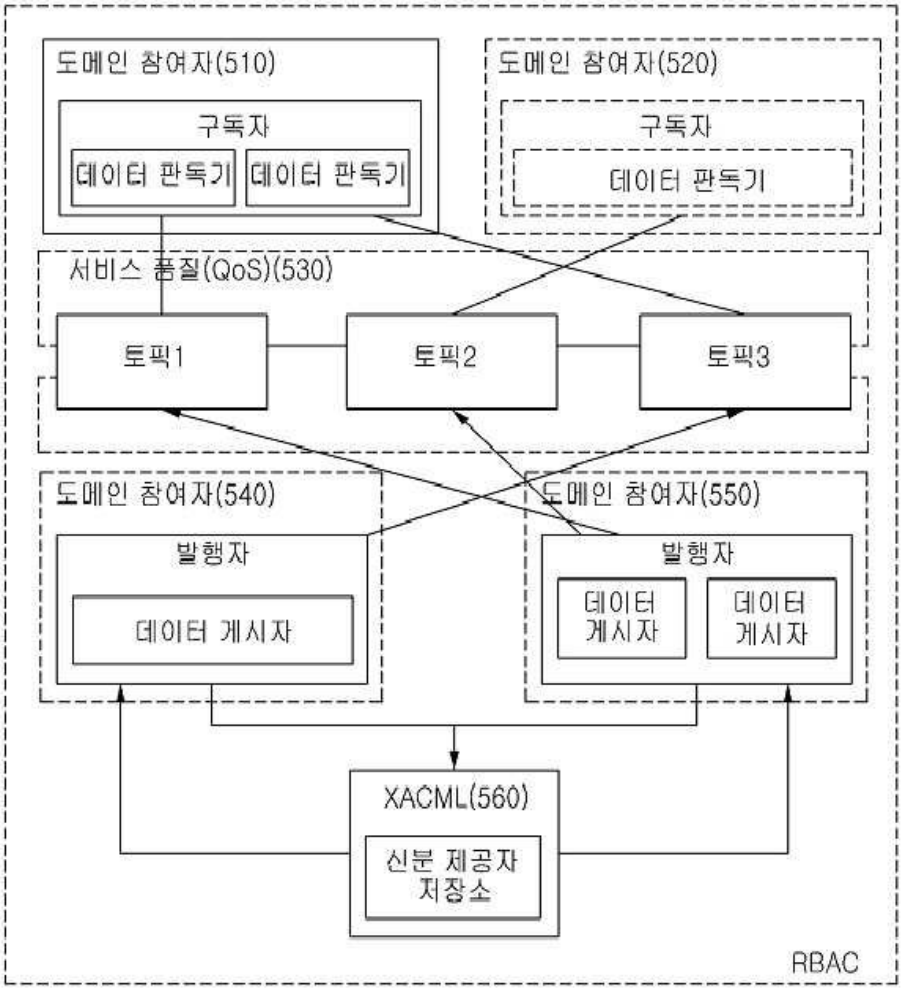
도면3


300
프로세서
310
PDP
311
PIP
312
PEP
313
360
361
330
350
320
구독자
네트워크
인터페이스
발행자
데이터베이스
362
메모리
340
운영 체제
341
스마트 그리드 통신 응용프로그램
수준의 보안 루틴
342

도면4


DDS(410)
구독자(411)
발행자(412)
토픽
HITPS
기반의
RESTful
(430)
XACML(420)
PDP(421)
PEP
(423)
PIP
(422)

도면5


도메인 참여자(510)
구독자
데이터 판독기
데이터 판독기
도메인 참여자(520)
구독자
데이터 판독기
서비스 품질(QoS)(530)
토픽1
토픽2
토픽3
도메인 참여자(540)
발행자
데이터 게시자
도메인 참여자(550)
발행자
데이터 게시자
데이터 게시자
XACML(560)
신분 제공자 저장소
RBAC