



**(19) 대한민국특허청(KR)**  
**(12) 공개특허공보(A)**

(11) 공개번호 10-2013-0100242  
 (43) 공개일자 2013년09월10일

(51) 국제특허분류(Int. Cl.)  
 H04L 12/22 (2006.01) H04L 29/06 (2006.01)  
 (21) 출원번호 10-2012-7032899  
 (22) 출원일자(국제) 2011년07월11일  
 심사청구일자 없음  
 (85) 번역문제출일자 2012년12월17일  
 (86) 국제출원번호 PCT/KR2011/005070  
 (87) 국제공개번호 WO 2012/008721  
 국제공개일자 2012년01월19일  
 (30) 우선권주장  
 1966/CHE/2010 2010년07월10일 인도(IN)

(71) 출원인  
**삼성전자주식회사**  
 경기도 수원시 영통구 삼성로 129 (매탄동)  
 (72) 발명자  
**베둘라, 키란 바라드와즈**  
 인도, 방갈로 560093, 비라잔드라, C V 라만 나가르, 바그마네 테크 파크, 넘버 66/1, ब्लॉक 'B', 바그마네 레이크뷰  
**이종효**  
 인도, 방갈로 560093, 비라잔드라, C V 라만 나가르, 바그마네 테크 파크, 넘버 66/1, ब्लॉक 'B', 바그마네 레이크뷰  
 (74) 대리인  
**이건주**

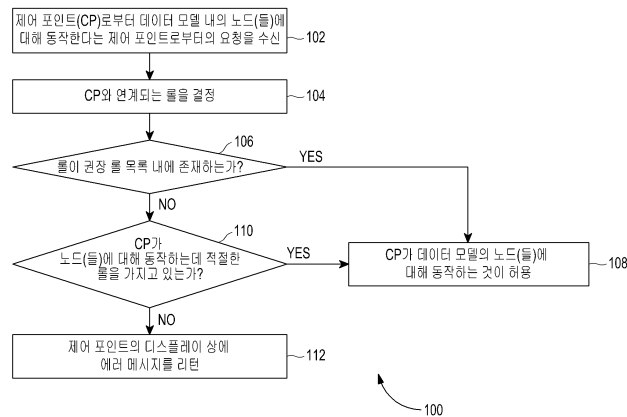
전체 청구항 수 : 총 31 항

(54) 발명의 명칭 **범용 플러그 앤 플레이 데이터 모델들에 저장된 구성 정보로의 액세스를 보안하기 위한 방법 및 시스템**

**(57) 요약**

본 발명은 범용 플러그 앤 플레이 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법 및 시스템을 제공한다. 하나의 실시예에서, 제어 포인트(CP)로부터 데이터 모델의 노드(들)에 대하여 동작한다는 요청이 수신된다. 데이터 모델은 복수의 노드들을 포함하고 복수의 노드들 각각은 구성 정보를 나타낸다. CP와 연계되는 룰이 결정된다. CP가 권장 룰 목록 내에 있는지가 결정된다. 룰이 존재하면, CP는 노드(들)에 대해 동작하는 것이 허용된다. 룰이 존재하지 않으면, CP는 노드(들)와 연계되는 ACL 데이터에 기초하여 노드(들)에 대해 동작하는 적절한 노드를 가지고 있는지가 결정된다. 따라서, CP는 노드(들)에 대해 동작하는 것이 허용되거나 에러 메시지가 CP의 디스플레이 상에 리턴된다.

**대표도 - 도1**



## 특허청구의 범위

### 청구항 1

하나 이상의 제어 포인트들 및 하나 이상의 제어 디바이스들을 지니는 홈 네트워크 환경에서 데이터 모델들에 저장된 구성 정보로의 액세스를 보안하기 위한 컴퓨터 구현 방법에 있어서,

제어 포인트로부터 데이터 모델의 하나 이상의 노드들에 대해 동작한다는 요청을 수신하는 단계를 포함하며, 상기 데이터 모델은 복수의 노드들을 포함하고, 상기 복수의 노드들의 각각은 구성 정보를 나타내며;

상기 수신된 요청에 기초하여 상기 제어 포인트와 연계되는 룰(role)을 결정하는 단계와;

상기 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있는지를 결정하는 단계와;

권장 룰 목록 내에 있다고 결정하는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계와;

권장 룰 목록 내에 있지 않다고 결정하는 경우, 상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(access control list; ACL) 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있는지를 결정하는 단계와;

적합한 룰을 가지고 있는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계; 및

적합한 룰을 가지고 있지 않은 경우, 상기 제어 포인트의 디스플레이 상에 에러 메시지를 리턴(return)시키는 단계를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

### 청구항 2

제 1 항에 있어서, 상기 데이터 모델에 대한 요청은 상기 데이터 모델에 대한 액세스 동작, 수정 동작, 및 관독 동작 중 하나를 실행한다는 요청을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

### 청구항 3

제 1 항에 있어서, 상기 하나 이상의 노드들은 리프(leaf) 노드들, 단일 인스턴스(instance) 노드들, 다중-인스턴스 노드들 및 인스턴스 노드들을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

### 청구항 4

제 1 항에 있어서, 상기 제어 포인트와 연계되는 룰은 기본 룰, 공중 룰, 어드민(admin) 룰, 및 판매자 규정 룰들 중 하나를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

### 청구항 5

제 1 항에 있어서, 상기 하나 이상의 노드들의 각각과 연계되는 ACL 데이터는 액세스 요소, 관독 요소, 및 수정 요소로 연계되는 노드 식별자를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

### 청구항 6

제 2 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계는, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 저장된 구성 정보에 액세스하는 것을 인에이블(enable)하는 단계를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

### 청구항 7

제 2 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계는, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들과 연계되는 적어도 하나의 노드들을 판독하는 것을 인에이블하는 단계를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

**청구항 8**

제 2 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계는, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들과 연계되는 적어도 하나의 노드를 수정하는 것을 인에이블하는 단계를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

**청구항 9**

제 1 항에 있어서, 상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 ACL 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있는지를 결정하는 단계는,

상기 수신된 요청 내의 데이터 모델의 노드와 연계되는 노드 식별자를 결정하는 단계와, 상기 노드 식별자에 기초하여 상기 데이터 모델의 노드와 연계되는 ACL 데이터를 검색하는 단계와, 상기 제어 포인트와 연계되는 룰이 상기 ACL 데이터 내의 노드에 대한 요청된 동작을 실행하는 권한을 부여받은 룰과 정합하는지를 결정하는 단계와, 상기 제어 포인트와 연계되는 룰이 상기 ACL 데이터 내의 노드에 대한 요청된 동작을 실행하는 권한을 부여받은 룰과 정합하는 경우, 상기 수신된 요청에 남겨진 임의의 다른 노드가 존재하는지를 결정하는 단계와, 상기 수신된 요청에 남겨진 임의의 다른 노드가 존재하는 경우, 모든 노드들이 프로세싱될 때까지 상기 단계들을 반복하는 단계와, 상기 수신된 요청에 남겨진 임의의 다른 노드가 존재하지 않는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

**청구항 10**

제 9 항에 있어서, 상기 제어 포인트와 연계되는 룰이 상기 ACL 데이터 내의 노드에 대한 요청된 동작을 실행하는 권한을 부여받은 룰과 정합하는지를 결정하는 단계는, 상기 제어 포인트와 연계되는 룰이 상기 ACL 데이터 내의 노드에 대한 요청된 동작을 실행하는 권한을 부여받은 룰과 정합하지 않는 경우, 에러 메시지를 상기 제어 포인트의 디스플레이 상에 리턴시키는 단계를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 방법.

**청구항 11**

프로세서; 및

상기 프로세서와 결합되는 메모리를 포함하고, 상기 메모리는,

제어 포인트로부터 데이터 모델의 하나 이상의 노드들에 대해 동작한다는 요청을 수신하는 단계를 포함하며, 상기 데이터 모델은 복수의 노드들을 포함하고, 상기 복수의 노드들의 각각은 구성 정보를 나타내며;

상기 수신된 요청에 기초하여 상기 제어 포인트와 연계되는 룰을 결정하고;

상기 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있는지를 결정하고;

상기 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있다고 결정하는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하고;

상기 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있지 않다고 결정하는 경우, 상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL) 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있는지를 결정하고;

상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL) 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하고;

상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL) 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있지 않은 경우, 상기 제어 포인트의 디스플레이 상에 에러 메시지를 리턴시키는 구성 관리 서비스(configuration management service; CMS) 모듈을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 12**

제 11 항에 있어서, 상기 데이터 모델에 대한 요청은, 상기 데이터 모델에 대한 액세스 동작, 수정 동작, 및 판독 동작 중 하나를 실행한다는 요청을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 13**

제 11 항에 있어서, 상기 하나 이상의 노드들은, 리프 노드들, 단일 인스턴스 노드들, 다중-인스턴스 노드들 및 인스턴스 노드들을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 14**

제 11 항에 있어서, 상기 제어 포인트와 연계되는 룰은 기본 룰, 공중 룰, 어드민 룰, 및 판매자 규정 룰들 중 하나를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 15**

제 11 항에 있어서, 상기 하나 이상의 노드들의 각각과 연계되는 ACL 데이터는 액세스 요소, 판독 요소, 및 수정 요소로 연계되는 노드 식별자를 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 16**

제 12 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는데 있어서, 상기 CMS 모듈은, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 저장된 구성 정보에 액세스하는 것을 인에이블하는 것을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 17**

제 12 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는데 있어서, 상기 CMS 모듈은, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들과 연계되는 적어도 하나의 노드들을 판독하는 것을 인에이블하는 것을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 18**

제 12 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는데 있어서, 상기 CMS 모듈은, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들과 연계되는 적어도 하나의 노드를 수정하는 것을 인에이블하는 것을 포함함을 특징으로 하는 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하기 위한 장치.

**청구항 19**

내부에 저장된 명령들을 가지는 비밀시적 컴퓨터 판독 가능 저장 매체로서,

상기 명령들은, 홈 네트워크 환경의 제어 디바이스에 의해 실행될 때, 상기 제어 디바이스로 하여금 제어 포인트로부터 데이터 모델의 하나 이상의 노드들에 대해 동작한다는 요청을 수신하는 단계를 포함하며, 상기 데이터 모델은 복수의 노드들을 포함하고, 상기 복수의 노드들의 각각은 구성 정보를 나타내며; 상기 수신된 요청에 기초하여 상기 제어 포인트와 연계되는 룰을 결정하는 단계와; 상기 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있는지를 결정하는 단계와; 상기 제어 포인트와 연계되는 룰이 상기 수신된

요청과 연계되는 권장 롤 목록 내에 있다고 결정하는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계와; 상기 제어 포인트와 연계되는 롤이 상기 수신된 요청과 연계되는 권장 롤 목록 내에 있지 않다고 결정하는 경우, 상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL) 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 롤을 가지고 있는지를 결정하는 단계와; 상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL) 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 롤을 가지고 있는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 단계; 및 상기 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL) 데이터에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 롤을 가지고 있지 않은 경우, 상기 제어 포인트의 디스플레이 상에 에러 메시지를 리턴시키는 단계를 포함하는 방법을 실행하도록 함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

**청구항 20**

제 19 항에 있어서, 상기 데이터 모델에 대한 요청은 상기 데이터 모델에 대한 액세스 동작, 수정 동작, 및 판독 동작 중 하나를 실행한다는 요청을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

**청구항 21**

제 19 항에 있어서, 상기 하나 이상의 노드들은 리프 노드들, 단일 인스턴스 노드들, 다중-인스턴스 노드들 및 인스턴스 노드들을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

**청구항 22**

제 19 항에 있어서, 상기 제어 포인트와 연계되는 롤은 기본 롤, 공중 롤, 어드민 롤, 및 판매자 규정 롤들 중 하나를 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

**청구항 23**

제 19 항에 있어서, 상기 하나 이상의 노드들의 각각과 연계되는 ACL 데이터는 액세스 요소, 판독 요소, 및 수정 요소로 연계되는 노드 식별자를 포함함을 특징으로 하는 컴퓨터-판독 가능 저장 매체.

**청구항 24**

제 20 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 명령들은, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 저장된 구성 정보에 액세스하는 것을 인에이블하는 것을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

**청구항 25**

제 20 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 명령들은, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들과 연계되는 적어도 하나의 노드들을 판독하는 것을 인에이블하는 것을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

**청구항 26**

제 20 항에 있어서, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하는 명령들은, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들과 연계되는 적어도 하나의 노드를 수정하는 것을 인에이블하는 것을 포함함을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

**청구항 27**

데이터 모델의 하나 이상의 노드들에 대해 동작한다는 요청을 인보킹하기 위한 적어도 하나의 제어 포인트를 포함하며, 상기 데이터 모델은 복수의 노드들을 포함하고, 상기 복수의 노드들의 각각은 구성 정보를 나타내며;

상기 적어도 하나의 제어 포인트에 통신 가능하게 접속되는 적어도 하나의 제어 디바이스들을 포함하고, 상기 적어도 하나의 제어 디바이스는:

상기 수신된 요청에 기초하여 상기 적어도 하나의 제어 포인트와 연계되는 롤을 결정하고;

상기 적어도 하나의 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있는지를 결정하고;

상기 적어도 하나의 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있다고 결정하는 경우, 상기 적어도 하나의 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하고;

상기 적어도 하나의 제어 포인트와 연계되는 룰이 상기 수신된 요청과 연계되는 권장 룰 목록 내에 있지 않다고 결정하는 경우, 상기 하나 이상의 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL)에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있는지를 결정하고;

상기 하나 이상의 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL)에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있는 경우, 상기 제어 포인트가 상기 데이터 모델의 하나 이상의 노드들에 대해 동작하는 것을 허용하고;

상기 하나 이상의 제어 포인트가 상기 하나 이상의 노드들의 각각과 연계되는 액세스 제어 목록(ACL)에 기초하여 상기 데이터 목록의 하나 이상의 노드들에 대해 동작하는데 적합한 룰을 가지고 있지 않은 경우, 상기 제어 포인트의 디스플레이 상에 예러 메시지를 리턴시키는 것을 포함함을 특징으로 하는 홈 네트워크 시스템.

**청구항 28**

제 27 항에 있어서, 상기 데이터 모델에 대한 요청은 상기 데이터 모델에 대한 액세스 동작, 수정 동작, 및 판독 동작 중 하나를 실행한다는 요청을 포함함을 특징으로 하는 홈 네트워크 시스템.

**청구항 29**

제 27 항에 있어서, 상기 하나 이상의 노드들은 리프 노드들, 단일 인스턴스 노드들, 다중-인스턴스 노드들 및 인스턴스 노드들을 포함함을 특징으로 하는 홈 네트워크 시스템.

**청구항 30**

제 27 항에 있어서, 상기 제어 포인트와 연계되는 룰은 기본 룰, 공중 룰, 어드민 룰, 및 판매자 규정 룰들 중 하나를 포함함을 특징으로 하는 홈 네트워크 시스템.

**청구항 31**

제 27 항에 있어서, 상기 하나 이상의 노드들의 각각과 연계되는 ACL 데이터는 액세스 요소, 판독 요소, 및 수정 요소로 연계되는 노드 식별자를 포함함을 특징으로 하는 홈 네트워크 시스템.

**명세서**

**기술분야**

[0001] 본 발명은 범용 플러그 앤 플레이(universal plug and play; UPnP) 홈 네트워크 시스템 분야에 관한 것으로, 더욱 상세하게는, UPnP 디바이스 관리 모델들의 액세스(accessing)에 관한 것이다.

**배경기술**

[0002] 범용 플러그 앤 플레이(UPnP)는 UPnP 포럼에 의해 공표된 컴퓨터 네트워크 프로토콜들의 세트이다. UPnP의 목적들은 액세스가 단절 없이 접속하고 홈 (예를 들어 데이터 공유, 통신들, 및 엔터테인먼트) 및 기업 환경들에서 네트워크들의 구현을 간소화하는 것을 가능하게 하는 것이다. 이 목적들은 개방형, 인터넷-기반 통신 표준들에 기반한 UPnP 디바이스 제어 프로토콜들을 규정하고 공표함으로써 달성된다.

[0003] UPnP 기술은 홈 네트워크에서 광범위한 디바이스들에 제공될 수 있다. UPnP는 발견, 제어, 및 이벤팅(eventing) 메커니즘들을 제공한다. 발견은 SSDP 프로토콜을 이용하여 가능하다. 이벤팅은 GENA 프로토콜을 따른다. 이 기술들을 이용함으로써, UPnP는 UPnP 디바이스가 UPnP 홈 네트워크 내의 다른 디바이스들에 즉각적으로 이용 가능하게 하거나 이용 가능하지 않게 만든다.

- [0004] UPnP 아키텍처로 인해 개인용 컴퓨터들(PC들), 네트워크형 기기들, 및 무선 디바이스들의 피어-투-피어(peer-to-peer) 네트워크가 가능하다. 이는 TCP/IP, UDP, HTTP 및 XML과 같이 설정된 표준들에 기초하는 분산형, 개방 아키텍처이다. UPnP 아키텍처는 제로 구성 네트워킹(zero configuration networking)을 지원한다. 예를 들어, 다른 판매자로부터의 UPnP 호환 디바이스는 네트워크에 동적으로 참여하고, IP 어드레스를 획득하고, 이의 명칭을 공표하고, 요청 시에 자신의 케이퍼빌리티(capability)들을 전달하고, 다른 디바이스들에 대한 존재 및 케이퍼빌리티들을 습득할 수 있다. 한편, UPnP 디바이스들은 어떠한 원치 않는 상태 정보를 남기지 않고도 UPnP 홈 네트워크를 자동으로 떠날 수 있다.
- [0005] UPnP 네트워킹을 위한 기반은 IP 어드레싱이다. 각각의 UPnP 디바이스는 UPnP 디바이스가 처음 UPnP 네트워크에 접속될 때 동적 호스트 구성 프로토콜(dynamic host configuration protocol: DHCP) 서버를 탐색하는 DHCP 클라이언트를 포함한다. DHCP 서버가 이용 가능하지 않은 경우, UPnP 디바이스는 자신에게 어드레스를 할당한다. DHCP 트랜잭션(transaction) 중에, UPnP 디바이스가 예를 들어 DNS 서버를 통해 또는 DNS 포워딩(DNS forwarding)을 통해, 도메인 이름을 획득하는 경우, UPnP 디바이스는 후속 네트워크 동작들에서 그 이름을 이용하거나; 그렇지 않으면 UPnP 디바이스는 자체의 IP 어드레스를 이용한다.
- [0006] UPnP는 디바이스 보호 서비스를 UPnP에서 규정되는 모든 서비스들에 의해 이용될 수 있는 범용 보안 솔루션으로 규정한다. 디바이스 보호 서비스는 룰(role)들의 개념을 규정한다. 모든 제어 포인트들 또는 제어 디바이스들에는 UPnP 액션(action)들을 실행하기 위해 상이한 룰들, 즉 상이한 공중, 기본 및 어드민(admin)이 할당된다. 상이한 DCP들 및 판매자들은 자유로이 이 룰들의 세트를 확장한다.
- [0007] UPnP 디바이스 관리 서비스는 데이터 모델들의 개념을 규정한다. 데이터 모델은 다양한 디바이스들 및 서비스 구성 관련 정보의 트리 표현(tree representation)이다. 데이터 모델은 리프 노드(leaf node)들, 단일 인스턴스 노드(single instance node)들, 다중 인스턴스 노드들 및 인스턴스 노드들과 같은 다양한 종류의 노드들을 구성한다. 데이터 모델들은 보호될 필요가 있는 민감 정보(sensitive information)를 포함할 수 있다. 또한, 데이터 모델들에 포함되는 구성 정보의 일부는 홈 네트워크 환경 내의 일부의 제어 포인트들 또는 이용자와는 무관할 수 있다. 현재의 데이터 보호 서비스는 요청 시에 데이터 모델들에 저장되어 있는 전체의 구성 정보를 제어 포인트에 제공한다. 결과적으로, 제어 포인트는 전체 구성 정보 내에 제공되는 민감 정보 및 관련 없는 정보에 액세스하게 된다.

**발명의 내용**

**해결하려는 과제**

- [0008] 그러므로, UPnP 디바이스 관리 데이터 모델들에 저장되는 구성 정보를 수정할 뿐만 아니라 뷰잉, 관독하기 위한 액세스 제어를 제공함으로써, 데이터 모델들에 저장된 구성 정보에 대한 보호를 제공할 필요가 있다.

**과제의 해결 수단**

- [0009] 본 발명은 범용 플러그 앤 플레이(UPnP) 데이터 모델들에 저장되는 구성 정보로의 액세스를 보안하는 방법 및 시스템을 제공한다. 본 발명의 실시예들의 다음의 상세한 설명에서, 본 발명의 일부를 형성하고 본 발명이 실행될 수 있는 예시의 특정한 실시예들을 통하여 도시되는 첨부 도면들이 참조된다. 이 실시예들은 당업자가 본 발명을 실행할 수 있도록 충분히 자세하게 기술되고, 다른 실시예들이 이용될 수 있고 본 발명의 범위를 벗어나지 않고 변형들이 행해질 수 있음이 이해될 것이다. 그러므로, 다음의 상세한 설명은 제한하는 의미로 취해지는 것은 아니며, 본 발명은 첨부된 청구항들에 의해서만 규정된다.

- [0010] 용어들 "UPnP 데이터 모델" 및 "데이터 모델" 문서 전체에 걸쳐 상호 교환하여 이용된다.

**발명의 효과**

- [0011] 상술한 바와 같이, 본 발명에 따르면, UPnP 디바이스 관리 데이터 모델들에 저장되는 구성 정보를 수정할 뿐만 아니라 뷰잉, 관독하기 위한 액세스 제어를 제공함으로써, 데이터 모델들에 저장된 구성 정보에 대한 보호를 제공하는 것이 가능하다.

**도면의 간단한 설명**

- [0012] 도 1은 본 발명의 일 실시예에 따른, 범용 플러그 앤 플레이(UPnP) 데이터 모델들에 저장된 구성 정보로의 보안

액세스를 제공하는 예시적인 방법을 도시하는 프로세스 흐름도

도 2는 본 발명의 상황에서, 다수의 노드들을 가지는 예시적인 UPnP 데이터 모델들의 개략적인 도면

도 3은 본 발명의 일 실시예에 따른, 데이터 모델의 구성 정보로의 액세스를 보안하는 예시적인 방법의 흐름도

도 4는 본 발명의 일 실시예에 따른, 제어 포인트에 의해 데이터 모델의 다중-인스턴스 노드를 수정하고 다른 제어 포인트로부터 수정된 다중-인스턴스 노드를 보안하는 예시적인 방법의 흐름도

도 5는 본 발명의 일 실시예에 따른, UPnP 데이터 모델에 저장된 구성 정보로의 액세스를 보안하기 위한 홈 네트워크 시스템을 도시하는 블록도

도 6은 본 발명의 실시예들을 구현하기 위해 도 5에 도시된 홈 네트워크 시스템과 같은 홈 네트워크 시스템의 제어 디바이스의 다양한 구성요소들을 도시하는 블록도

본원에 기술되는 도면들은 단지 설명을 위한 것이고 어떠한 식으로도 본 발명의 범위를 제한하는 것으로 의도되지 않는다.

**발명을 실시하기 위한 구체적인 내용**

- [0013] 도 1은 본 발명의 일 실시예에 따른, UPnP 데이터 모델들에 저장된 구성 정보로의 보안 액세스를 제공하는 예시적인 방법을 도시하는 프로세스 흐름도(100)이다. 102 단계에서, 홈 네트워크 환경 내의 제어 포인트로부터 데이터 모델의 노드(들)에 대해 동작한다는 요청이 수신된다. 데이터 모델은 리프 노드들, 단일 인스턴스 노드들, 다중 인스턴스 노드들 및 인스턴스 노드들과 같은 다양한 노드들을 포함한다. 복수의 노드들 각각은 홈 네트워크 환경 내의 제어 포인트들과 연계되는 구성 정보를 저장한다. 구성 정보는 서비스 구성 정보 및 디바이스 구성 정보일 수 있다. 도 2를 참조하면, 데이터 모델(200)이 도시되고 이 데이터 모델(200)은 구성 정보를 저장하기 위해 노드(/A/B), 노드(/A/E), 노드(/A/F), 노드(/A/B/C), 및 노드(/A/B/G)를 포함한다. 제어 포인트는 데이터 모델의 노드들 중 임의의 노드에 대하여 작동한다고 요청할 수 있다.
- [0014] 104 단계에서, 제어 포인트와 연계되는 롤(role)은 상기 요청에 기초하여 결정된다. 홈 네트워크 환경 내의 제어 포인트들의 각각은 연계된 구성 정보에 따라 동작하는 롤을 할당 받는다. 예를 들어, 상기 요청과 연계되는 제어 포인트에는 공중 롤, 기본 롤, 또는 어드민 롤(admin role)이 할당될 수 있다. 제어 포인트에 판매자 지정 롤들과 같은 다른 유형의 롤들이 할당될 수 있음이 언급될 수 있다.
- [0015] 106 단계에서, 제어 포인트에 할당된 롤이 상기 요청에서 지정된 동작(예를 들어 액세스, 판독 또는 수정)과 연계되는 권장 롤 목록 내에 있는지가 결정된다. 권장 롤 목록은 데이터 모델의 노드들 상에서 액세스, 판독, 및 수정 동작을 실행하도록 권장되는 홈 네트워크 환경 내의 제어 포인트들과 연계되는 롤들의 목록을 포함한다. 롤이 권장 롤 목록 내에 있다면, 108 단계에서, 제어 포인트가 데이터 모델의 노드(들)에 대해 동작하는 것이 허용된다.
- [0016] 예를 들어, 102 단계에서, 제어 포인트가 데이터 모델(200)의 노드(/A/B/C)에 액세스한다고 요청했다면, 제어 디바이스는 제어 포인트가 권장 롤 목록에 기초하여 노드(/A/B/C)에 액세스하는 것을 허용한다. 상기 요청이 판독 동작과 연계되면, 제어 디바이스는 데이터 모델(200)의 노드(/A/B/C)에 저장된 구성 정보를 판독하는 것을 허용한다. 대안으로, 제어 포인트가 수정 동작을 요청하면, 제어 디바이스는 제어 포인트가 노드(/A/B/C)를 수정(예를 들어, 다른 노드를 추가, 노드를 제거)하는 것을 허용한다. 일부 실시예들에서, 데이터 모델의 연계된 노드(들)만이 제어 포인트의 디스플레이 상에 디스플레이된다. 이 실시예들에서, 데이터 모델의 나머지 노드들(요청된 것을 제외한)은 제어 포인트의 디스플레이 상에 디스플레이되지 않는다.
- [0017] 롤이 권장 롤 목록 내에 있다면, 단계 110에서, 제어 포인트가 데이터 모델의 노드(들)에 대해 동작하는 적절한 롤을 가지고 있는지가 결정된다. 하나의 실시예에서, 데이터 모델의 요청된 노드(들)와 연계되는 액세스 제어 목록(access control list; ACL) 데이터를 이용하여 결정이 행해진다. ACL 데이터는 노드 특성임이 언급될 수 있다. 노드와 연계되는 ACL 데이터는 액세스 요소, 판독 요소, 및/또는 수정 요소와 연계되어 있는 노드 식별자를 포함한다. 액세스 요소, 판독 요소 및 수정 요소는, 대응하는 노드 식별자와 연계되는 노드에 대해 액세스, 판독 및 수정 동작들의 각각을 실행하도록 권한이 부여된 롤 유형을 나타낸다. 각각의 노드의 예시적인 ACL 데이터는 대응하는 노드 식별자와 함께 아래 표 1에 기술되어 있다.

표 1

NODE IDENTIFIER	ACL DATA
/A/B/C	ACCESS=PUBLIC,ADMIN; READ=BASIC; MODIFY="
/A/B	ACCESS=BASIC,READ=ADMIN; NIDIFY=ADMIN
/A/B/D	ACCESS=PUBLIC,READ=BASIC; MODIFY=ADMIN

[0018]

[0019]

도 2 및 표 1을 참조하면, 공중 롤을 가지는 제어 포인트가 노드 식별자(NODE IDENTIFIER)(/A/B/C)를 가지는 노드로 액세스하는 것이 허용되고, 반면에 기본 롤을 가지는 제어 포인트가 노드 식별자(/A/B/C)를 가지는 노드를 관독하는 것이 허용된다. 그러나, 어떠한 롤도 노드 식별자(/A/B/C)를 가지는 노드를 수정하기 위한 권한을 부여 받지 않는다. 기본 롤을 가지는 제어 포인트가 노드 식별자(/A/B)를 가지는 노드로 액세스하는 것이 허용되고, 어드민 롤을 가지는 제어 포인트가 노드 식별자(/A/B)를 가지는 노드를 관독 및/또는 수정하는 것이 허용된다. 유사하게, 공중 롤을 가지는 제어 포인트가 노드 식별자(/A/B/D)를 가지는 노드에 액세스하는 것이 허용되고, 기본 롤을 가지는 제어 포인트가 노드 식별자(/A/B/D)를 가지는 노드를 관독하는 것이 허용되고, 어드민 롤을 가지는 제어 포인트가 노드 식별자(/A/B/D)를 가지는 노드를 수정하는 것이 허용된다. 노드 식별자들(/A/B/C, /A/B, 및 /A/B/D)에 대한 ACL 데이터들의 예시적인 XML 방식들은 각각 부록 A, B, 및 C에서 제공된다.

[0020]

도 1을 다시 참조하면, 노드(들)의 ACL 데이터에 기초하여 제어 포인트가 노드(들)에 대하여 동작하도록 허용되는지에 대한 결정은 다음과 같이 실행된다. 처음에, 요청에 표시된 노드와 연계되는 노드 식별자가 결정된다. 그리고 나서, 동작이 요청된 노드와 연계되는 ACL 데이터가 검색된다. 게다가, 제어 포인트와 연계되는 롤이 ACL 데이터 내의 노드에 대해 요청된 동작을 실행하도록 권한 부여된 롤과 정합하는지가 결정된다. 정합이 발견되면, 동작한다는 요청이 행해진 임의의 다른 노드가 존재하는지가 결정된다. 남겨져 있는 임의의 노드가 존재하면, 모든 모드들이 프로세싱될 때까지 상기 단계들이 반복된다. 프로세싱하도록 남겨진 노드가 없고 요청된 모든 노드(들)에 대해 정합이 발견되면, 108 단계가 실행된다. 요청된 하나 이상의 노드(들)에서 정합이 발견되지 않으면, 112 단계에서, 에러 메시지가 제어 포인트의 디스플레이 상으로 리턴된다.

[0021]

예를 들어, 제어 포인트가 노드(/A/B/D)에 대하여 관독 동작을 요청했고 제어 포인트와 연계되는 롤이 공중 롤이라고 고려하자. 표 1에서와 같이, 노드(/A/B/D)와 연계되는 ACL 데이터는 "Access=Public, Read=Basic, 및 Modify=Admin"을 표시한다. 그러므로, 노드(/A/B/D)에 대한 관독 동작을 거부하고 에러 메시지가 리턴된다. 그러나, 제어 포인트가 노드(/A/B/D)에 대한 액세스 동작을 요청하면, 표 1에서 액세스 요소가 노드(/A/B/D)에 대한 공중 롤을 표시할 때, 제어 포인트가 노드(/A/B/D)에 대한 액세스 동작을 실행하는 것이 허용된다.

[0022]

도 3은 본 발명의 일 실시예에 따른, 데이터 모델의 구성 정보로의 액세스를 보안하는 예시적인 방법의 흐름도(300)이다. 302 단계에서, 디바이스 보호(device protection; DP) 엔티티(entity)는 디바이스 보호(DP) 서비스와 연계되는 ACL 데이터를 구성 관리 서비스(configuration management service; CMS) 엔티티에 제공한다. 304 단계에서, CMS 엔티티는 대역의 채널을 통하여 CMS ACL 데이터로 로딩된다. 306 단계에서, CMS 엔티티 및 CP1은 상호 인증된다. 308 단계에서, CP1은 데이터 모델에 액세스한다는 요청을 CMS 엔티티에 송신한다.

[0023]

310 단계에서, CMS 엔티티는 DP 엔티티와 함께 CP1이 데이터 모델로 액세스할 권리를 가지고 있는지를 검사한다. DP 엔티티는 CP1이 권장 롤 목록 내에 존재하는지를 결정한다. DP 엔티티는 CP1이 데이터 모델에 액세스할 권리를 가지고 있지 않음을 발견한다. 312 단계에서, DP 엔티티는 CP1이 데이터 모델에 액세스할 권리를 가지고 있지 않음을 확인한다. 314 단계에서, CMS 엔티티는 CP1이 데이터 모델의 요청된 노드(들)에 액세스하는데 적절한 롤을 가지고 있는지를 결정하고 CP1이 이 노드(들)에 액세스하는 권한을 가지고 있음을 발견한다. 따라서, 316 단계에서, CMS 엔티티는 CP1에 요청된 노드(들)만을 가지는 데이터 모델을 리턴시키고 반면에 나머지 노드들을 CP1에게 감춘다.

[0024]

도 4는 본 발명의 일 실시예에 따른, 제어 포인트에 의해 데이터 모델의 다중-인스턴스 노드를 수정하고 다른 제어 포인트로부터 수정된 다중-인스턴스 노드를 보안하는 예시적인 방법의 흐름도(400)이다. 402 단계에서, 디바이스 보호(DP) 엔티티는 디바이스 보호(DP) 서비스와 연계되는 ACL 데이터를 구성 관리 서비스(CMS) 엔티티에 제공한다. 404 단계에서, CMS 엔티티는 대역의 채널을 통하여 CMS ACL 데이터로 로딩된다. 406 단계에서, CMS

엔티티 및 CP1은 상호 인증된다. 408 단계에서, CP1은 데이터 모델의 다중-인스턴스 노드를 수정한다는 요청을 CMS 엔티티에 송신한다.

[0025] 410 단계에서, CMS 엔티티는 DP 엔티티와 함께 CP1이 데이터 모델의 다중-인스턴트 노드를 수정할 액세스 권리를 가지고 있는지를 검사한다. DP 엔티티는 CP1이 권장 롤 목록 내에 존재하는지를 결정한다. DP 엔티티는 CP1이 데이터 모델의 다중-인스턴스 노드를 수정할 권리를 가지지 않음을 발견한다. 412 단계에서, DP 엔티티는 CP1이 데이터 모델의 다중-인스턴스 노드를 수정할 권리를 가지지 않음을 확인한다. 414 단계에서, CMS 엔티티는 CP1이 CMS ACL 데이터에 기초하여 데이터 모델의 다중-인스턴스 노드를 수정할 적절한 롤을 가지고 있는지를 결정하고 CP1이 다중-인스턴스 노드를 수정할 적절한 롤을 가지고 있음을 발견한다. 따라서, 416 단계에서, CMS 엔티티는 다중-인스턴스 노드가 성공적으로 수정됨을 CP1에 통지한다.

[0026] 418 단계에서, CP1은 CMS에게 데이터 모델의 수정된 다중-인스턴스 노드를 뷰잉할 것을 요청한다. 420 단계에서, CMS 엔티티는 데이터 모델의 수정된 다중-인스턴스 노드를 CP1에 디스플레이한다. 이제, 다른 제어 포인트(CP2)가 422 단계에서, 데이터 모델의 수정된 다중-인스턴스 노드에 액세스하는 시도를 행하고 CMS 엔티티에 요청을 송신한다. 424 단계에서, CMS 엔티티는, CP2가 수정된 다중-인스턴스 노드에서의 구성 정보를 판독하기 위한 정합 롤을 가지지 않을 때, 에러 메시지를 CP2로 리턴시킨다. 예를 들어, CMS 엔티티는 "/UPnP/DM/DeviceInfo/PhysicalDevice/NetworkInterface/#/"로 칭해지는 다중-인스턴스 노드를 규정하고 네트워크 인터페이스(1)를 생성하기 위해 CP1이 다중-인스턴스 노드에 대한 수정 명령을 인보킹(invoking)하는 것이 허용된다. 그러나, CP2가 다중-인스턴스 노드의 ACL 데이터에 기초하여 새로 생성된 네트워크 인터페이스에 관련된 구성 정보를 판독하는 것은 허용되지 않는다.

[0027] 도 5는 본 발명의 일 실시예에 따른, UPnP 데이터 모델(200)에 저장된 구성 정보로의 액세스를 보안하기 위한 홈 네트워크 시스템(500)을 도시하는 블록도이다. 도 5에서, 홈 네트워크 시스템(500)은 제어 디바이스(502) 및 제어 포인트(506)를 포함한다. 본 발명에 따르면, 제어 디바이스(502)는 데이터 모델(200)을 가지는 구성 관리 서비스(CMS) 모듈(504)을 포함한다.

[0028] 예시적인 동작에서, 제어 포인트(506)는 구성 관리 서비스와 연계되는 데이터 모델(200)의 노드(들)에 대하여 동작하기 위한 요청을 인보킹한다. CMS 모듈(504)은 이 요청에 기초하여 제어 포인트(506)와 연계되는 롤을 결정한다. CMS 모듈(504)은 제어 포인트(506)와 연계되는 롤이 권장 롤 목록 내에 있는지를 결정한다. 상기 롤이 권장 롤 목록 내에 있다면, CMS 모듈(504)은 제어 포인트(506)가 데이터 모델(200)의 노드(2)에 액세스하고/판독하고/수정하는 것을 허용한다. 상기 롤이 권장 롤 목록 내에 존재하지 않으면, CMS 모듈(504)은 노드(들)의 ACL 데이터에 기초하여 데이터 모델(200)의 노드(들)에 대해 동작하는 적절한 롤을 가지고 있는지를 결정한다. 이 결정에 기초하여, CMS 모듈(504)은 제어 포인트가 데이터 모델(200)의 노드(들)에 액세스하고/판독/수정하는 것을 허용하거나 또는 제어 포인트(506)에 에러 메시지를 리턴시킨다. CMS 모듈(504)이 도 1 내지 도 4에 도시된 하나 이상의 실시예들에 따라 UPnP 데이터 모델에 저장된 구성 정보로의 액세스를 보안한다고 이해된다.

[0029] 도 6은 본 발명의 실시예들을 구현하기 위해 도 5에 도시된 홈 네트워크 시스템(500)과 같은 홈 네트워크 시스템(502)의 제어 디바이스(502)의 다양한 구성요소들을 도시하는 블록도이다. 도 6에서, 제어 디바이스(502)는 프로세서(602), 메모리(604), 판독 전용 메모리(ROM)(606), 송수신기(608), 버스(610), 통신 인터페이스(612), 디스플레이(614), 입력 디바이스(616), 및 커서 제어기(618)를 포함한다.

[0030] 프로세서(602)는, 본원에서 이용되는 바와 같이, 마이크로프로세서, 마이크로컨트롤러, 복잡 명령 세트 컴퓨팅 마이크로프로세서, 감소 명령 세트 컴퓨팅 마이크로프로세서, 초장 명령어 마이크로프로세서(very long instruction word microprocessor), 명시적 병렬 명령 컴퓨팅 마이크로프로세서, 그래픽 프로세서, 디지털 신호 프로세서와 같은 임의의 유형의 계산 회로, 또는 임의의 다른 유형의 프로세싱 회로를 의미하지만, 이로 한정되지 않는다. 프로세서(602)는 또한 일반 또는 프로그램 가능 논리 디바이스들 또는 어레이들, 주문형 반도체들, 단일-칩 컴퓨터들, 스마트 카드들 등과 같은 임베디드 컨트롤러들을 포함할 수 있다.

[0031] 메모리(604) 및 ROM(606)은 휘발성 메모리 및 비휘발성 메모리일 수 있다. 메모리(604)는 도 1 내지 도 5에 기술된 하나 이상의 실시예들에 따라, UPnP 데이터 모델에 저장된 구성 정보로의 액세스를 보안하기 위해 CMS 모듈(504)을 포함한다. 다양한 컴퓨터-판독 가능 저장 매체는 메모리 소자들에 저장되거나 메모리 소자들로부터 액세스될 수 있다. 메모리 소자들은 데이터 및 기계-판독 명령들을 저장하기 위한 임의의 적절한 메모리 디바이스(들), 예를 들어 판독 전용 메모리, 랜덤 액세스 메모리, 소거 가능 프로그램 가능 판독 전용메모리(erasable programmable read only memory), 전기적 소거 가능 프로그램 가능 판독 전용 메모리, 하드 드라이브

브, 콤팩트 디스크들, 디지털 비디오 디스크들, 디스켓들, 자기 테이프 카트리지들, 메모리 카드들, 메모리 스틱들(TM)을 처리하기 위한 제거 가능 매체 드라이브 등을 포함한다.

[0032] 본 주제의 실시예들은 임무들을 실행하거나 추상적인 데이터 유형들 또는 저-레벨 하드웨어 컨텍스트들을 규정하기 위하여, 함수들, 절차들, 데이터 구조들, 및 응용 프로그램들을 포함하는 모듈들과 함께 구현될 수 있다. 상술한 저장 매체 중 임의의 매체에 저장된 기계-판독 가능 명령들은 프로세서(602)에 의해 수행될 수 있다. 예를 들어, 컴퓨터 프로그램은 본 주제의 내용들 및 본원에 기술된 실시예들에 따라, UPnP 데이터 모델에 저장된 구성 정보로의 액세스를 보안할 수 있는 기계-판독 가능 명령들을 포함할 수 있다. 하나의 실시예에서, 프로그램은 콤팩트 디스크-판독 전용 메모리(CD-ROM) 상에 포함되고 CD-ROM으로부터 비-휘발성 메모리 상태인 하드 드라이브로 로딩될 수 있다. 기계-판독 가능 명령들은 제어 디바이스(502)로 하여금 본 주제의 다양한 실시예들에 따라 인코딩하도록 할 수 있다.

[0033] 송수신기(608)는 데이터 모델의 노드(들)에 대해 동작하기 위한 요청을 수신하고 제어 포인트(506)들에게 노드(들)의 ACS 데이터 및 제어 포인트(506)의 룰에 기초하여 데이터 모델의 노드(들)에 대하여 동작하는 권한을 부여할 수 있다. 버스(610)는 제어 디바이스(502)의 다양한 구성요소들 사이를 상호 연결하는 역할을 한다. 통신 인터페이스들(612), 디스플레이(614), 입력 디바이스(616), 및 커서 제어기(618)와 같은 구성요소들은 당업자에게 널리 공지되어 있으므로 이의 설명은 생략된다.

[0034] 본 실시예들은 특정한 예시 실시예들을 참조하여 설명되었고, 다양한 실시예들의 보다 광의의 정신 및 범위를 벗어나지 않고 이 실시예들에 다양한 수정들 및 변형들이 행해질 수 있음이 명백할 것이다. 더욱이, 본원에서 기술되는 다양한 장치들, 모듈들, 선택기들, 추정기들 등은 하드웨어 회로소자, 예를 들어 상보성 금속 산화막 반도체 기반 논리 회로 소자, 펌웨어, 소프트웨어, 및/또는 기계 판독 가능 매체 내에 내장된 하드웨어, 펌웨어, 및/또는 소프트웨어의 임의의 조합을 이용하여 가능하거나 동작될 수 있다. 예를 들어, 트랜지스터들, 논리 게이트들, 및 주문형 반도체와 같은 전기 회로들을 이용하여 다양한 전기 구조 및 방법들이 구현될 수 있다.

[0035] **부록 'A'**

[0036] <ACLData>

[0037] <NodeIdentifier> /A/B/C </NodeIdentifier>

[0038] <Access> Public </Access>

[0039] <Read> Basic </Read>

[0040] <Modify> None </Modify>

[0041] <ACLData>

[0042] **부록 'B'**

[0043] <ACLData>

[0044] <NodeIdentifier> /A/B </NodeIdentifier>

[0045] <Access> Public </Access>

[0046] <Read> Admin </Read>

[0047] <Modify> Admin </Modify>

[0048] <ACLData>

[0049] **부록 'C'**

[0050] <ACLData>

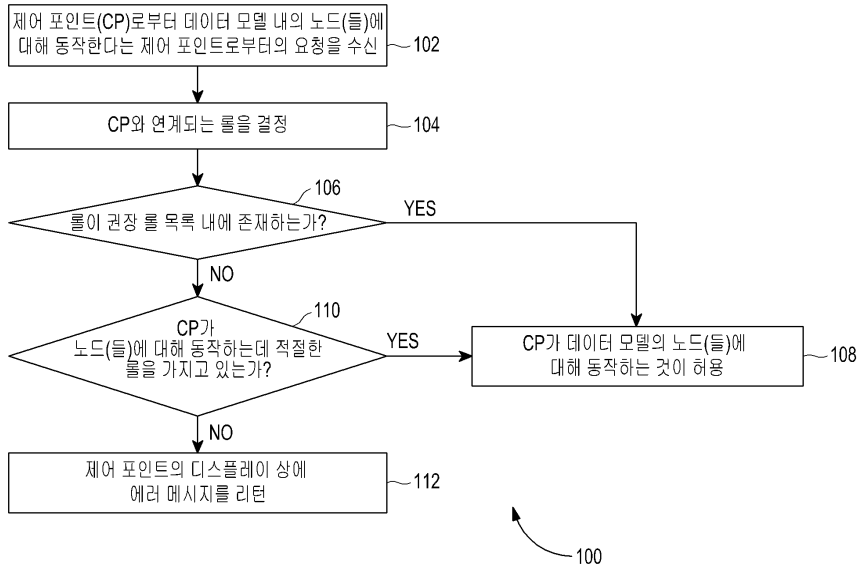
[0051] <NodeIdentifier> /A/B/D </NodeIdentifier>

[0052] <Access> Public </Access>

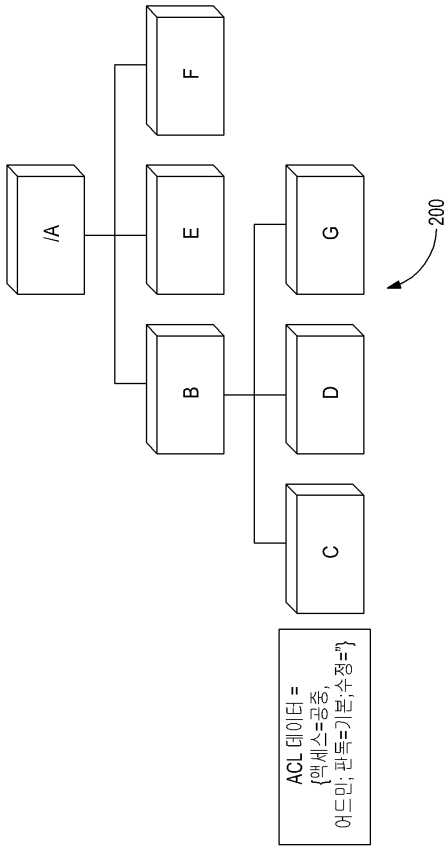
- [0053] <Read> Basic </Read>
- [0054] <Modify> Admin </Modify>
- [0055] <ACLData>

도면

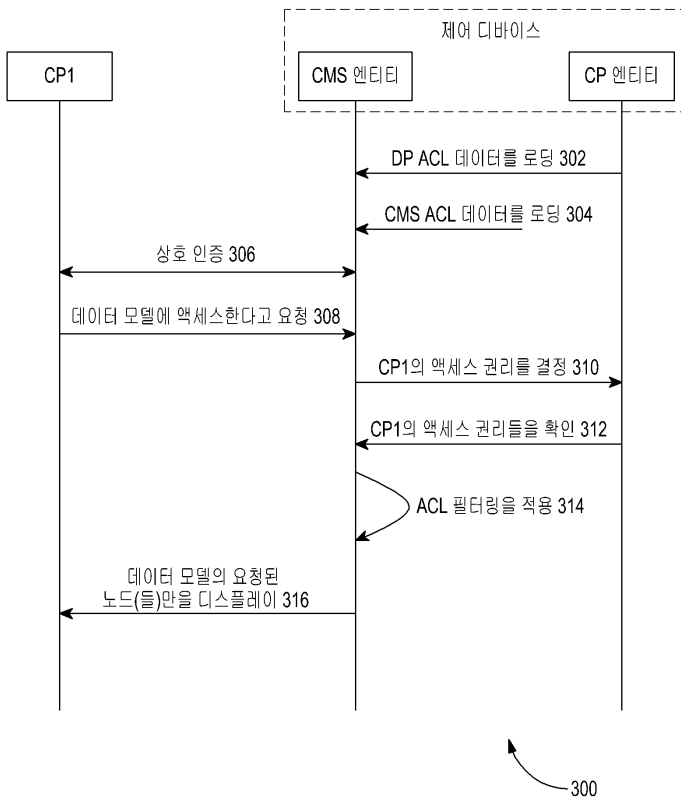
도면1



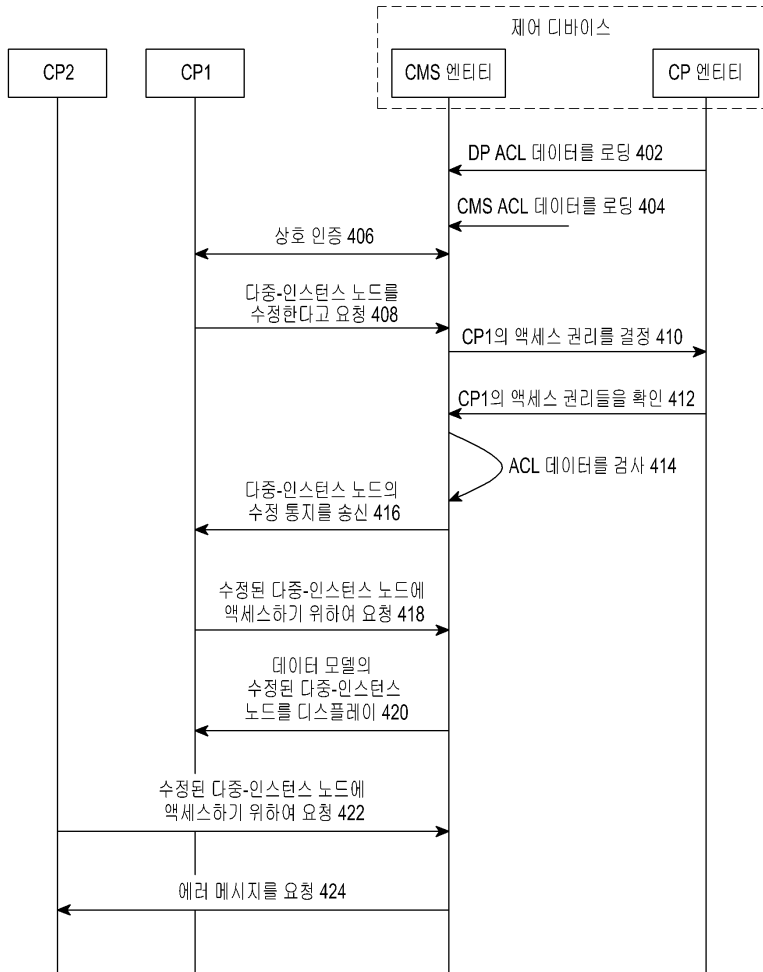
도면2



도면3

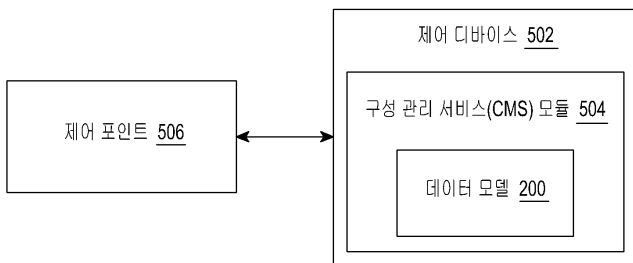


도면4



400

도면5



500

도면6

