(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0065190
(43) 공개일자 2009년06월22일

(51) Int. Cl.
G06F 17/40 (2006.01)
(21) 출원번호 10-2007-0132659
(22) 출원일자 2007년12월17일
심사청구일자 2007년12월17일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
최진영
서울 성북구 안암동5가 고려대학교 아산이학관 201호
김일곤
서울 송파구 가락동 78번지 한국정보보호진흥원
(뒷면에 계속)
(74) 대리인
현종철

전체 청구항 수 : 총 15 항

(54) AXML 기반의 접근 통제 모델의 정형 명세 방법, 그장치 및 이를 기록한 기록 매체

(57) 요 약

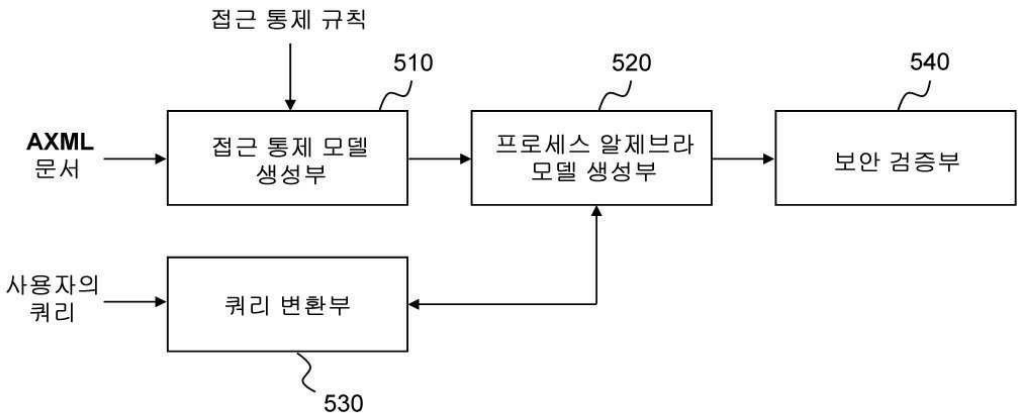
AXML 기반의 접근 통제 모델의 정형 명세 방법, 그 장치 및 이를 기록한 기록 매체가 개시된다.

본 발명에 따른 AXML 기반의 접근 통제 모델의 정형 명세 방법은,

계층적 트리 구조 형태로 구성된 AXML 문서에 대하여 상기 AXML 문서의 경로 지정 언어 및 미리 등록된 클라이언트별 퀴리에 따른 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성하는 단계; 상기 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 프로세스 알제브라 정형 모델을 생성하는 단계; 상기 AXML 문서에 대하여 클라이언트로부터 단순 객체 접근 프로토콜에 의한 쿼리가 발생하면, 상기 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구사항으로 명세하고, 상기 클라이언트에게 상기 프로세스 알제브라 정형 모델에 따라 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하는 단계; 및 상기 프로세스 알제브라 정형 모델을 FDR 모델 체킹 도구를 이용하여 상기 AXML 문서에 대한 보안 검증을 수행하는 단계를 포함한다.

본 발명에 의하면, 국제 공통 평가 기준에서 정의한 고등급의 보안 제품 개발을 위해서 필요한 정형 명세 및 정형 검증에 요구에 맞추어 웹 서비스 환경에서 AXML 문서의 비밀성을 보장하기 위해 사용되는 접근 통제 규칙을 계층적으로 정형 명세할 수 있고, 고등급의 AXML 기반의 접근 통제 보안제품의 보안성 향상 및 인허가 획득에 기여하고, 국가 보안 기술력 및 보안 제품의 국제 경쟁력을 향상시킬 수 있는 효과가 있다.

대 표 도 - 도5



(72) 발명자

김현석

서울 동대문구 제기동 한신아파트 103동 902호

이지연

경기 수원시 장안구 정자동 937 동남보건대학

특허청구의 범위

청구항 1

계층적 트리 구조 형태로 구성된 AXML 문서에 대하여 상기 AXML 문서의 경로 지정 언어 및 미리 등록된 클라이언트별 쿼리에 따른 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성하는 단계;

상기 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 프로세스 알제브라 정형 모델을 생성하는 단계;

상기 AXML 문서에 대하여 클라이언트로부터 단순 객체 접근 프로토콜에 의한 쿼리가 발생하면, 상기 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구사항인 필터링 쿼리를 생성하고, 상기 클라이언트에게 상기 프로세스 알제브라 정형 모델에 따라 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하는 단계; 및

상기 프로세스 알제브라 정형 모델을 FDR 모델 체킹 도구를 이용하여 상기 AXML 문서에 대한 보안 검증을 수행하는 단계를 포함하는 AXML 기반의 접근 통제 모델의 정형 명세 방법.

청구항 2

제 1 항에 있어서,

상기 경로 지정 언어는 XSquirrel 경로 지정 언어를 포함하는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 방법.

청구항 3

제 1 항에 있어서,

상기 프로세스 알제브라 정형 모델을 생성하는 단계는

상기 접근 통제 모델을 상기 경로 지정 언어를 이용하여 오토마타형 스키마 모델로 변환하는 단계; 및

상기 오토마타형 스키마 모델을 프로세스 알제브라 언어로 정형 명세하여 스키마 정형 모델을 생성하는 단계를 포함하는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 방법.

청구항 4

제 3 항에 있어서,

상기 오토마타형 스키마 모델은 트리구조를 가지는 상기 AXML 문서의 특정 노드의 속성 이름을 대수 표현으로 전환하여, 상기 대수 표현으로 전환된 속성값이 참일 경우에만 다음 하위 노드의 질의를 수행하도록 구성되는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 방법.

청구항 5

제 1 항에 있어서,

상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하는 단계는

상기 클라이언트로부터 상기 AXML 문서의 특정 서비스 호출에 따라 상기 클라이언트의 쿼리를 수신하는 단계; 및

상기 수신된 클라이언트의 쿼리를 상기 접근 통제 모델로부터 상기 클라이언트 쿼리와 관련된 접근 통제 규칙을 탐색하고, 상기 탐색된 복수의 접근 통제 규칙에 따라 쿼리 필터링을 수행하여 필터링 쿼리를 생성하는 단계를 포함하는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 방법.

청구항 6

제 5 항에 있어서,

상기 필터링 쿼리는 순수 동기화 연산자($|||$) 및 동기화 병렬 연산자($\circ$)에 의해 생성되는 것을 특징

으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 방법.

청구항 7

제 1 항에 있어서,

상기 클라이언트별 접근 통제 규칙은 상기 클라이언트에 대한 상기 AXML 문서의 특정 정보에 대하여 허용 또는 거부로 명시되는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 방법.

청구항 8

제 1 항 내지 제 7 항 중 어느 한 항의 방법을 컴퓨터에서 수행시킬 수 있도록 프로그램으로 기록된 기록매체.

청구항 9

계층적 트리 구조 형태로 구성된 AXML 문서에 대하여 상기 AXML 문서의 경로 지정 언어 및 미리 등록된 클라이언트별 쿼리에 따른 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성하는 접근 통제 모델 생성부;

상기 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 프로세스 알제브라 정형 모델을 생성하는 프로세스 알제브라 정형 모델 생성부;

상기 AXML 문서에 대하여 클라이언트의 쿼리가 발생하면, 상기 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구사항으로 명세하고, 상기 클라이언트에게 상기 프로세스 알제브라 정형 모델에 따라 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하는 쿼리 변환부; 및

상기 프로세스 알제브라 정형 모델을 FDR 모델 체킹 도구를 이용하여 상기 AXML 문서에 대한 보안 검증을 수행하는 보안 검증부를 포함하는 AXML 기반의 접근 통제 모델의 정형 명세 장치.

청구항 10

제 9 항에 있어서,

상기 경로 지정 언어는 XSquirrel 경로 지정 언어를 포함하는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 장치.

청구항 11

제 9 항에 있어서,

상기 프로세스 알제브라 정형 모델 생성부는

상기 접근 통제 모델을 상기 경로 지정 언어를 이용하여 오토마타형 스키마 모델로 변환하는 오토마타 스키마 모델 변환 모듈; 및

상기 오토마타형 스키마 모델을 프로세스 알제브라 언어로 정형 명세하여 스키마 정형 모델을 생성하는 스키마 정형 모델 생성 모듈을 포함하며,

상기 스키마 정형 모델에 프로세스 알제브라 언어를 적용하여 프로세스 알제브라 정형 모델을 생성하는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 장치.

청구항 12

제 11 항에 있어서,

상기 스키마 정형 모델은

트리구조를 가지는 상기 AXML 문서의 특정 노드의 속성 이름을 대수 표현으로 전환하여, 상기 대수 표현으로 전환된 속성값이 참일 경우에만 다음 하위 노드의 질의를 수행하도록 구성되는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 장치.

청구항 13

제 9 항에 있어서,

상기 쿼리 변환부는

상기 클라이언트로부터 상기 AXML 문서의 특정 서비스 호출에 따라 상기 클라이언트의 쿼리를 수신하고, 상기 수신된 클라이언트의 쿼리를 상기 접근 통제 모델로부터 상기 클라이언트 쿼리와 관련된 접근 통제 규칙을 탐색하고, 상기 탐색된 복수의 접근 통제 규칙에 따라 쿼리 필터링을 수행하여 필터링 쿼리를 생성하는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 장치.

청구항 14

제 9 항에 있어서,

상기 클라이언트별 접근 통제 규칙은 상기 클라이언트에 대한 상기 AXML 문서의 특정 정보에 대하여 허용 또는 거부로 명시되는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 장치.

청구항 15

제 9 항에 있어서,

상기 클라이언트별 접근 통제 규칙 중 특정 접근 통제 규칙에 있어서 충돌이 발생하는 경우, 허용 중복 또는 거부 중복 알고리즘에 따라 상기 클라이언트별 접근 통제 규칙이 결정되는 것을 특징으로 하는 AXML 기반의 접근 통제 모델의 정형 명세 장치.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 AXML 문서의 정보 보안에 관한 것으로서, 특히 AXML 문서의 자료 구조 형태를 정형 명세 모델로 명세하여, 주어진 쿼리에 대하여 접근 통제 모델이 의도한 바대로 AXML 문서에 대한 접근 통제를 정확히 수행할 수 있도록 AXML 기반의 접근 통제 모델을 정형 명세하는 AXML 기반의 접근 통제 모델의 정형 명세 방법, 그 장치 및 이를 기록한 기록 매체를 제공하는 것이다.

배 경 기 술

<2> 환자기록 정보와 같은 분산 비밀 정보에 대한 관리 및 접근통제에 대한 중요성이 점차 증대되고 있다. 하지만, 기존의 연구방법들은 중앙 집중형 데이터 접근통제에 대해 주로 다루었고, XML 문서의 접근통제에 대한 연구를 진행하였을 뿐이다.

<3> 확장성 표시 언어(eXtensible Markup Language:XML)는 하이퍼 텍스트 마크업 언어(Hyper Text Markup Language:HTML)와 일반화된 표준 마크업 언어(Standard Generalized Markup Language:SGML)의 단점을 개선하여 만들어진 차세대 인터넷 전자 문서 표준이다. XML은 플랫폼에 독립적이며, 문서 정보의 전송과 교환이 쉽고, 문서의 풍부한 의미를 그대로 나타낼 수 있다는 장점이 있다. 또한 XML은1998년 2월에 W3G에서 권고안으로 채택되어, 이후 XML로 이루어진 데이터를 저장하고, 이를 관리 검색하는 XML의 데이터 관리 시스템에 관한 연구가 있어 왔다.

<4> XML 기반의 웹 서비스 환경에서는 다양한 상품코드, 온도, 특정 문서 등과 같은 데이터들은 클라이언트 간에 송수신하게 된다.

<5> 이는, 특정 클라이언트가 서버에 쿼리(Query)를 전송한 후, 상기 쿼리에 매핑되는 중요한 XML 문서를 수신하는 형태로 이루어진다. 만약, 악의적인 사용자가 중요 XML 문서에 접근하는 것을 방지하기 위하여 서버에 위치하며, 문서 접근에 대한 규칙을 정한 접근통제모델을 통해 XML 문서의 중요 데이터 노드에 대한 접근을 통제하게 된다.

<6> 그러나, 복수의 접근통제규칙이 존재하는 경우, 접근통제규칙의 의미론 및 규칙의 복잡성으로 인하여, 예기치 않게 악의적인 공격자가 접근할 수 있는 오류가 발생할 수 있다.

<7> 실제로, XML 기반의 웹 서비스 분야의 활성화와 더불어, 정보를 요청한 사라용자가 XML 트리로 구성된 정보에서

허가받은 데이터 영역에만 접근하도록 하기 위한 보안 문제점이 대두되고 있어,트리의 데이터 노드들의 보안성, 예를 들어 읽기 허가, 읽기 거부 등을 표현하기 위해 데이터 베이스 영역에서는 경로 지정 언어가 새롭게 개발되었다.

<8> 그러나, XML 문서의 접근 통제 규칙을 명시하기 위한 지금까지의 연구 방향은 자연어 형태에 의존하여 왔기 때문에 명세 언어의 모호성으로 인하여 접근 통제 규칙의 명확성 및 데이터 비밀성 문제점을 분석하는데 비효율적인 문제점을 안고 있고, XML 문서에 대한 접근통제규칙의 복잡성과 오류로 인하여 허가받지 않은 사용자가 특정 중요 데이터 노드 영역에 접근할 수 있는 보안 문제점이 야기될 수 있다.

<9> 그러나, XML기반 웹서비스의 활성화와 더불어 효율적인 데이터 호출 및 통합을 위해, XML 문서 안에 웹서비스 호출 노드를 내장할 수 있는 액티브 확장성 표시 언어(Active eXtensible Markup Language:AXML)가 개발되었다.

<10> AXML 문서는 기존의 XML 문서와는 달리 문서안에 함수를 내장하여, 서비스를 호출할 수 있는 고유의 특징이 있다.

<11> AXML 문서는 계층적 자료 구조 형태를 취하고 있기 때문에 기존의 접근 통제 매커니즘과는 달리, 문서 안에 트리 노드에 대한 개별적인 보안뿐만 아니라, 전체 문서에 대한 보안성을 제공하고 있다.

<12> 실제로, AXML 문서가 가지는 내장형 서비스 호출, 쿼리 언어, 쿼리 필터링들의 고유 특징들로 인해, AXML 문서의 접근 통제 모델을 분석하는 것은 어려운 작업이다.

<13> 그러나, 최근의 AXML 문서의 접근 통제 모델의 관리는 주로 중앙 집중형 데이터 접근 통제에만 머무르고 있는 실정이다.

<14> 그 예로, Abiteboul et al은 일반적 사용자 프로파일(Generic User Profile)과 냅스터(Napster) 프로그램을 결합한 GUPster 기반의 접근 통제 매커니즘과 P2P 환경에서 AXML 문서를 병합하여 분산 테이블을 통합 관리하는 방법을 제안하였다.

<15> 그리고, Sahuguet et al은 GUPster 접근통제 모델을 개발하여, 컨버전스 네트워크 환경에서 분산 사용자 XML 프로파일의 통합 및 사용자 권한 및 데이터 소스를 표현하는 접근통제 메커니즘을 제시하여 데이터 베이스와 웹서비스 분야에서도 접근 통제 규칙을 검증하기 위한 연구를 진행하였고, Bryans는 XACML 접근 통제 표준 언어로 작성된 접근 통제 규칙을 분석하는 방법을 제안하였고, XACML의 의미론을 CSP 언어로 변환하고, FDR 모델체킹 도구를 이용하여 접근 통제 규칙을 분석하는 방법을 제안하였다.

<16> 이와 같이, 종래의 접근 통제 모델에 대한 정형 명세 방법은 XML 문서에 한정되어 상기 XML 문서를 비 계층적 데이터 형태로 명세하고 검증함으로써, AXML 문서의 접근 통제 규칙의 명확성 및 데이터 비밀성 문제점을 분석하는데 비효율적이며, 계층적 자료 구조 형태인 AXML 문서가 가지는 내장형 서비스 호출, 쿼리 언어, 쿼리 필터링들의 고유 특징들로 인해, AXML 문서의 접근 통제 모델을 분석하는 것이 실질적으로 불가능할 뿐더러, AXML 문서의 접근 통제 모델의 관리는 주로 중앙 집중형 데이터 접근 통제에만 머무르고 있는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<17> 본 발명이 해결하고자 하는 첫 번째 과제는,

<18> 계층적 트리 자료 구조 형태로 구성된 AXML 문서와 상기 문서의 특정 노드에 대한 경로 지정 언어로 표현된 쿼리 및 접근 통제 규칙을 정형 모델로 명세하고, 상기 명세된 정형 모델의 보안 속성을 검증할 수 있는 AXML 기반의 접근 통제 모델의 정형 명세 방법을 제공하는 것이다.

<19> 본 발명이 해결하고자 하는 두 번째 과제는,

<20> 상기 AXML 기반의 접근 통제 모델의 정형 명세 방법을 이용한 AXML 기반의 접근 통제 모델의 정형 명세 장치를 제공하는 것이다.

<21> 본 발명이 해결하고자 하는 세 번째 과제는

<22> 상기 AXML 기반의 접근 통제 모델의 정형 명세 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 기록매체를 제공하는 것이다.

과제 해결수단

<23> 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<24> 계층적 트리 구조 형태로 구성된 AXML 문서에 대하여 상기 AXML 문서의 경로 지정 언어 및 미리 등록된 클라이언트별 쿼리에 따른 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성하는 단계; 상기 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 프로세스 알제브라 정형 모델을 생성하는 단계; 상기 AXML 문서에 대하여 클라이언트의 쿼리가 발생하면, 상기 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구사항으로 명세하고, 상기 클라이언트에게 상기 프로세스 알제브라 정형 모델에 따라 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하는 단계; 및 상기 프로세스 알제브라 정형 모델을 FDR 모델 체킹 도구를 이용하여 상기 AXML 문서에 대한 보안 검증을 수행하는 단계를 포함하는 AXML 기반의 접근 통제 모델의 정형 명세 방법을 제공한다.

<25> 한편, 상기 경로 지정 언어는 XSquirrel 경로 지정 언어를 포함하는 것을 특징으로 한다.

<26> 아울러, 상기 프로세스 알제브라 정형 모델을 생성하는 단계는 상기 접근 통제 모델을 상기 경로 지정 언어를 이용하여 오토마타형 스키마 모델로 변환하는 단계; 및 상기 오토마타형 스키마 모델을 프로세스 알제브라 언어로 정형 명세하여 스키마 정형 모델을 생성하는 단계를 포함하는 것을 특징으로 한다.

<27> 그리고, 상기 오토마타형 스키마 모델은 트리구조를 가지는 상기 AXML 문서의 특정 노드의 속성 이름을 대수 표현으로 전환하여, 상기 대수 표현으로 전환된 속성값이 참일 경우에만 다음 하위 노드의 질의를 수행하도록 구성되는 것을 특징으로 한다.

<28> 또한, 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하는 단계는 상기 클라이언트로부터 상기 AXML 문서의 특정 서비스 호출에 따라 상기 클라이언트의 쿼리를 수신하는 단계; 및 상기 수신된 클라이언트의 쿼리를 상기 접근 통제 모델의 접근 통제 규칙에 따라 쿼리 필터링을 수행하여 필터링 쿼리를 생성하는 단계를 포함하는 것을 특징으로 한다.

<29> 여기서, 상기 필터링 쿼리는 순수 동기화 연산자(|||) 및 동기화 병렬 연산자(○)에 의해 생성되는 것을 특징으로 한다.

<30> 그리고, 상기 클라이언트별 접근 통제 규칙은 상기 클라이언트에 대한 상기 AXML 문서의 특정 정보에 대하여 허용 또는 거부로 명시되는 것을 특징으로 한다.

<31> 상기 두 번째 과제를 해결하기 위하여 본 발명은,

<32> 계층적 트리 구조 형태로 구성된 AXML 문서에 대하여 상기 AXML 문서의 경로 지정 언어 및 미리 등록된 클라이언트별 쿼리에 따른 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성하는 접근 통제 모델 생성부; 상기 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 프로세스 알제브라 정형 모델을 생성하는 프로세스 알제브라 정형 모델 생성부; 상기 AXML 문서에 대하여 클라이언트의 쿼리가 발생하면, 상기 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구사항으로 명세하고, 상기 클라이언트에게 상기 프로세스 알제브라 정형 모델에 따라 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하는 쿼리 변환부; 및 상기 프로세스 알제브라 정형 모델을 FDR 모델 체킹 도구를 이용하여 상기 AXML 문서에 대한 보안 검증을 수행하는 보안 검증부를 포함하는 AXML 기반의 접근 통제 모델의 정형 명세 장치를 제공한다.

<33> 여기서, 상기 경로 지정 언어는 XSquirrel 경로 지정 언어를 포함하는 것을 특징으로 한다.

<34> 그리고, 상기 프로세스 알제브라 정형 모델 생성부는 상기 접근 통제 모델을 상기 경로 지정 언어를 이용하여 오토마타형 스키마 모델로 변환하는 오토마타 스키마 모델 변환 모듈; 및 상기 오토마타형 스키마 모델을 프로세스 알제브라 언어로 정형 명세하여 스키마 정형 모델을 생성하는 스키마 정형 모델 생성 모듈을 포함하며, 상기 스키마 정형 모델에 프로세스 알제브라 언어를 적용하여 프로세스 알제브라 정형 모델을 생성하는 것을 특징으로 한다.

<35> 또한, 상기 스키마 정형 모델은 트리구조를 가지는 상기 AXML 문서의 특정 노드의 속성 이름을 대수 표현으로 전환하여, 상기 대수 표현으로 전환된 속성값이 참일 경우에만 다음 하위 노드의 질의를 수행하도록 구성되는 것을 특징으로 한다.

<36> 그리고, 상기 쿼리 변환부는 상기 클라이언트로부터 상기 AXML 문서의 특정 서비스 호출에 따라 상기 클라이언트의 쿼리를 수신하고, 상기 수신된 클라이언트의 쿼리를 상기 접근 통제 모델의 접근 통제 규칙에 따라 쿼리 필터링을 수행하여 필터링 쿼리를 생성하는 것을 특징으로 한다.

<37> 여기서, 상기 클라이언트별 접근 통제 규칙은 상기 클라이언트에 대한 상기 AXML 문서의 특정 정보에 대하여 허용 또는 거부로 명시되는 것을 특징으로 한다.

<38> 아울러, 상기 클라이언트별 접근 통제 규칙 중 특정 접근 통제 규칙에 있어서 충돌이 발생하는 경우, 허용 중복 또는 거부 중복 알고리즘에 따라 상기 클라이언트별 접근 통제 규칙이 결정되는 것을 특징으로 한다.

<39> 상기 세 번째 과제를 해결하기 위하여 본 발명은

<40> 상기 AXML 기반의 접근 통제 모델의 정형 명세 방법을 컴퓨터에서 수행시킬 수 있도록 프로그램으로 기록된 기록매체를 제공한다.

효 과

<41> 본 발명에 의하면, 웹 서비스 환경에서 AXML 문서의 비밀성을 보장하기 위해 사용되는 접근 통제 규칙의 보안성을 계층적으로 정형 검증할 수 있도록 AXML 문서를 정형 명세할 수 있고, 고등급의 AXML 기반의 접근 통제 보안 제품의 보안성 향상 및 인허가 획득에 기여하고, 국가 보안 기술력 및 보안 제품의 국제 경쟁력을 향상시킬 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<42> 본 발명은, 계층적 트리 자료 구조 형태로 구성된 AXML 문서와 상기 문서의 특정 노드에 대한 경로 지정 언어로 표현된 쿼리 및 접근 통제 규칙을 프로세스 알제브라 언어 형태의 정형 모델로 명세하고, 상기 명세된 정형 모델의 보안 속성을 FDR 도구를 이용하여 검증하고 분석하는 기술로 구성된다.

<43> 즉, 중요 정보 데이터를 포함하고 있는 AXML 문서가 존재할 경우, 클라이언트의 쿼리에 대한 접근통제모델의 보안 정책 규칙의 실행을 통해 생성된 보안 문서의 보안성이 정확하게 보장되고 있는지를 검증하는 기술이다.

<44> 이를 위하여, 첫 번째로 내장형 서비스 호출 기능을 내포한 계층형 구조의 AXML 문서, 경로 지정 언어로 표현된 쿼리 및 접근 통제 규칙을 CSP 프로세스 알제브라 언어로 명세한다.

<45> 두 번째로, CSP 언어가 가지고 있는 데이터 통신 프로토콜과 같은 동시성 시스템 (concurrent system)의 동시성 의미론을 이용하여 쿼리 표현식, 접근 통제규칙, AXML 문서에 대한 CSP 프로세스들을 생성한다.

<46> 세 번째로, 접근 통제 규칙과 필터링 서비스에 의해 재작성된 질의(rewritten query)를 모델링한다.

<47> 그런 다음, 마지막으로, AXML 접근 통제 시스템과 속성 모델의 예제에 따라 모델 체킹 도구를 이용하여 AXML 문서의 쿼리에 대한 접근 통제 규칙을 검증한다.

<48> 즉, 본 발명은 계층적 트리 자료 구조를 가지는 AXML 문서, 클라이언트의 쿼리, 경로 지정 언어, 접근 통제 규칙을 오토마타 이론을 기반으로 프로세스 알제브라 언어로 정형명세하고, 모델체킹 알고리즘을 이용하여 AXML 문서에 주어진 쿼리가 접근 통제 보안 규칙을 만족하는지를 검증하는 기법을 제공한다.

<49> 도 1은 본 발명에 적용되는 AXML 문서의 내장형 시스템 호출 및 필터링 서비스의 일 예를 도시한 것이다.

<50> 도 1은 스키마 레벨의 접근 통제 정책에 따라 쿼리를 필터링하여 AXML 비밀 데이터를 보호하는 질의 필터링 서비스의 개념을 도시하고 있다.

<51> 도 1에서 클라이언트(110)인 Dr. Kim은 'Suzzane'이라는 이름의 환자를 진찰하기 전에 그녀의 환자 기록 카드를 열람한다고 가정한다.

<52> Dr. Kim은 이미 서버 1(120)인 Paris 병원에 등록되어 있어서, 병원간의 네트워크에는 이미 인증을 받은 상태이다.

<53> 또한, Dr. Kim은 환자의 ID가 '123'이고, 환자의 기록 정보가 Rennes 병원에 저장되어 있다는 사실을 알고 있다고 가정한다.

<54> 그러면, 우선, 클라이언트(110)인 Dr. Kim은 Paris 병원의 인트라넷 사이트에 로그인한 후, AXML 문서의 내장형

함수 'getPatientRecord'에 따라 'getPatientRecord@reneshospital.fr' 서비스 호출을 이용하여 쿼리 q 를 Paris 병원에 전송한다.

<55> 이 서비스 호출은 'filterACL@parishopital'이라는 다른 서비스 호출 기능을 통하여 Dr. Kim과 연관된 접근 통제 규칙을 실행하여 쿼리 q 를 필터링 하게 된다.

<56> 그러면, Paris 병원은 병원의 인트라넷 사이트의 AXML 문서의 'filterACL@parishospital' 서비스 호출 후, 관련 접근 통제 규칙들을 실행하여 쿼리 필터링 서비스를 수행하게 되며, 상기 쿼리 필터링 서비스에 의하여 쿼리 q 는 필터링 쿼리 q' 로 변경된다.

<57> 그런 다음, 필터링 쿼리 q' 는 Paris 병원의 개인키를 이용하여 서명된 후, Dr. Kim의 AXML 문서에 반환된다.

<58> 그러면, 마지막으로, Dr. Kim은 서비스 호출을 통해 Rennes 변원에 필터링된 쿼리 q' 을 반환하며, q' 에 대한 해당 데이터가 Dr. Kim의 AXML 문서에 반환되게 된다.

<59> 한편, XSquirrel은 접근 통제 모델에 사용되는 간단한 형태의 AXML 경로 지정 표현 언어 이다.

<60> 상기 경로 지정 언어를 이용하여 스키마 문서와 원격 지정에 위치한 소스 데이터 간의 매핑, 클라이언트가 접근할 수 있는 데이터에 대한 접근 통제 규칙, 그리고 문서에 대한 쿼리를 표현할 수 있다.

<61> 이 언어는 XML 에서의 경로 지정 언어인 XPath와 유사한 표현식을 사용하고 있지만, #(union)과 같은 결합 연산자를 사용하여 AXML 문서상에서 하나 이상의 경로를 명시할 수 있다.

<62> AXML 문서 D 에 XSquirrel 언어로 작성된 $l_1/l_2/(l_3 \# l_4)$ 형태의 경로 지정 표현식의 쿼리 q 가 주어졌을 때, 이 표현식은 경로 구분자 '/'와 '#' 연산자로 구분된다.

<63> 한편, 문서 D 에 대한 $q(D)$ 는 쿼리 q 에 대한 반환값 집합이며, 이는 문서의 부분집합으로 구성된다.

<64> 그리고, $Eval(q[D])$ 기호는 쿼리 q 에 해당하는 노드를 클라이언트에게 반환한다.

<65> 예를 들어, 하기의 수학식 1과 같은 XSquirrel 쿼리 q 가 문서 D 에 대해 주어졌다고 가정한다.

수학식 1

<66> /PatientRecord/Patient/Medical/(VisitDate # Physid)

<67> 그러면, 상기 쿼리 q 에 해당되는 반환값 $q(D)$ 는 하기의 수학식 2와 같이 표현될 수 있다.

수학식 2

<68> /PatientRecord/Patient/Medical/VisitDate U
/PatientRecord/Patient/Medical/Physid

<69> 상기 수학식 2에서 볼 수 있는 바와 같이 상기 쿼리 q 에 해당되는 반환값 $q(D)$ 는 환자 기록 카드 문서에 대하여 두 가지 경로를 포함하고 있으며, XPath 표현식의 결과값과는 달리 여전히 문서의 본래 구조를 유지하고 있다.

<70> 그러나, $Eval(q[D])$ 의 결과값은 하기의 수학식 3에서 볼 수 있는 바와 같이, VisitDate와 Physid 두 노

드와 노드 값들을 반환하게 된다.

수학식 3

<VisitDate> March 11, 2000 </VisitDate>
<Physid> Dr.Smith 301 </Physid>

<71>

<72> 한편, 경로 지정에 대한 표현식은 조건 표현식을 지원한다. 예를 들면, 경로 지정의 표현식이 /PatientRecord/Patient[ID="123"]일 경우, 이에 대하여 환자의 ID가 123인 문서의 부분 문서가 반환되게 된다.

<73> AXML 문서와 접근 통제 모델을 이용한 통합 프레임워크 환경에서 사용되는 쿼리 전이(query transformation) 접근 통제 규칙을 실행하여, 개인 비밀 정보를 비인가 요청자로부터 보호하고, 필터링된 쿼리를 제공하여 요청된 자원을 소유한 제3의 호스트에 접근할 수 있다.

<74> 상기 도 1에 도시된 스키마 레벨의 접근 통제 정책에 따라 쿼리를 필터링하여 AXML 비밀 데이터를 보호하는 질의 필터링 서비스의 시스템을 보면, Dr. Kim이 Paris 병원에 저장된 의료 정보를 열람하기 위해 쿼리 q를 전송하게 되면, filterACL 서비스 호출을 통하여 Paris 병원에 저장된 스키마 s에 기술된 접근 통제 규칙을 실행하여, 쿼리 q는 필터링 쿼리 q'로 변경되게 된다.

<75> 따라서, $q'(D)$는 클라이언트가 접근하여 열람할 수 있는 제한된 데이터 정보만을 보여주며, 본 발명에서는 이를 인증 창(authorized view)이라고 일컫는다.

<76> 그런 다음, Paris 병원은 Dr. Kim에게 필터링된 쿼리를 반환하게 되고, Dr. Kim은 Rennes 병원으로부터 그가 열람할 수 있는 권한의 범위내에서 환자기록 카드 정보를 전송받게 된다.

<77> 환자기록 카드 스키마에 대한 일 예는 도 2에 도시된 바와 같다.

<78> 도 2를 참조하면 환자기록카드에 대한 AXML 문서 스키마는 트리 구조의 형태로 각각의 경로를 가진 데이터 노드로 구성되어 있음을 알 수 있다.

<79> 한편, 도 3은 각 정보에 대한 데이터 매핑 및 접근 통제 규칙을 XSquirrel로 표현한 것이다. 본 발명은 도 3과 같이 경로 지정 언어인 XSquirrel로 각 정보에 대한 데이터 매핑 및 접근 통제 규칙이 표현된다고 가정한다.

<80> 도 4는 본 발명에 따른 AXML 기반의 접근 통제 모델의 정형 명세 방법의 흐름도이다.

<81> 도 4를 참조하면 우선, 계층적 트리 구조 형태로 구성된 AXML 문서에 대하여 상기 AXML 문서의 경로 지정 언어 및 미리 등록된 클라이언트별 쿼리에 따른 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성한다(410 과정).

<82> 접근 통제 규칙은 단일 AXML 문서상에서 혹은 스키마 레벨에서 명시할 수 있다. 스키마 레벨의 접근 통제 규칙의 경우에는 스키마에 일맥 상통하는 모든 AXML 문서에 접근 통제 규칙을 적용할 수 있기 때문에 객체에 대한 접근 권한을 명시하는데 매우 효율적인 방법이므로, 본 발명에서는 스키마 레벨에서 접근 통제 규칙을 규정하는 방법을 적용한다.

<83> AXML 문서의 계층적 특징으로 인하여, 규칙의 적용 범위는 웹서비스 기반의 접근 통제 시스템을 구축하는데 매우 중요한 요인이 된다.

<84> 그 다음, 상기 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 프로세스 알제브라 정형 모델을 생성한다(420 과정).

<85> 여기서, 프로세스 알제브라 정형 모델을 생성하는 과정은 상기 접근 통제 모델을 상기 경로 지정 언어를 이용하여 오토마타형 스키마 모델로 변환하고, 상기 오토마타형 스키마 모델을 프로세스 알제브라 언어로 정형 명세하여 스키마 정형 모델을 생성할 수 있다.

<86> 여기서, 기존의 오토마타와의 구별점은 AXML 문서의 속성 이름을 대수 표현으로 전환하여 속성값이 참일 경우에만 다음 하위 노드의 질의를 수행할 수 있도록 구성할 수 있다.

<87> 한편, 여기서 경로 지정 언어는 XSquirrel 경로 지정 언어를 포함할 수 있다.

<88> 그 다음, 상기 AXML 문서에 대하여 클라이언트로부터 단순 객체 접근 프로토콜에 의한 쿼리가 발생하면, 상기 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구사항으로 명세하고, 상기 클라이언트에게 프로세스 알제브라 정형 모델에 따라 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송한다(430 과정).

<89> 여기서, AXML 문서에 대한 쿼리에 대응되는 정보를 전송하기 위하여, 상기 클라이언트로부터 AXML 문서의 특정 서비스 호출에 따라 상기 쿼리를 수신하고, 상기 수신된 클라이언트의 쿼리를 상기 접근 통제 모델의 접근 통제 규칙에 따라 쿼리 필터링을 수행하여 필터링 쿼리를 생성한다.

<90> 클라이언트의 쿼리 q로부터 접근 통제 규칙에 의하여 필터링 쿼리 q'로 변환 및 생성되는 과정은 하기와 같다.

<91> 우선, 접근 통제 모델은 클라이언트에 의해 요청된 쿼리 q에 대한 모든 관련 접근 통제 규칙 $\cup_i ACR_i$를 찾아낸다. 여기서, '$\cup$'는 합집합 기호를 나타내며, 'i'는 인덱스로 $\cup_i ACR_i$는 모든 관련 접근 통제 규칙을 의미하게 된다.

<92> 그 다음, 관련 접근 통제 규칙을 적용하여 쿼리 q는 필터링 쿼리 q'로 변환된다. 상기 쿼리 q로부터 접근 통제 규칙 $\cup_i ACR_i$를 통해 필터링 쿼리 q'를 생성하는 과정은 하기와 같이 수학식 4로 표현 가능하다. 하기의 수학식 4에서 '$\circ$'는 교집합 연산자를 의미한다.

수학식 4

<93> $$q' = q \circ \cup_i ACR_i$$

<94> 그 다음, 관련 접근 통제 규칙을 적용하여 쿼리 q를 필터링 쿼리 q'로 변환한 다음, 쿼리 요청 관련 데이터를 보관하고 있는 원격 저장소에 매핑되는 문서를 AXML 문서에 통합시킨다.

<95> 예를 들어, 상기 도 1을 참조하여, Dr. Kim이 호출한 쿼리 q가 하기의 수학식 5와 같다고 가정한다.

수학식 5

<96> $$/PatientRecord/Patient/Medical/(VisitDate \# Physid \# Diagnosis)$$

<97> 그러면, Dr. Kim과 연관된 모든 관련 접근 통제 규칙 Rule 1과 Rule 2는 허용 중복(grant overwrites) 알고리즘을 통해 병합된다.

<98> 그런 다음, 통합된 규칙은 쿼리 q와 병합되게 되며, 필터링 쿼리 q'는 상기 수학식 4에 따라 쿼리 q와 관련된 접근 통제 규칙의 교집합으로 연산될 수 있으며, 연산된 필터링 쿼리는 하기의 수학식 6과 같이 표현된다.

수학식 6

<99> $$q' = /PatientRecord/Patient/Medical$$
$$/(VisitDate \# Physid \# Diagnosis/(Disease \# Prescription))$$

<100> 그러면, 마지막으로, 상기 프로세스 알제브라 정형 모델을 FDR 모델 체킹 도구를 이용하여 상기 AXML 문서에 대한 보안 검증을 수행한다.

<101> 이는 AXML 문서에 대하여 생성된 프로세스 알제브라 정형 모델의 보안 적합성을 평가하기 위하여, FDR 모델 체킹 도구를 이용하여 AXML 문서에 대한 보안 검증을 수행한다.

<102> 이는 하기에 자세하게 상술하기로 한다.

<103> 본 발명은 오토마타 이론을 기반으로 스키마, 쿼리, 접근 통제 규칙 및 필터링 쿼리에 대하여 트리구조 형태의 접근 통제 모델을 구성한다.

<104> 접근 통제 모델을 구축할 경우, 상기 접근 통제 모델은 경로 지정 언어인 XSquirrel 조건 표현을 항상 만족하고 있다고 가정한다.

<105> 예를 들어, /PatientRecord/Patient[ID="123"]에 대하여 접근 통제 모델에 포함되는 경로 지정식은 /PatientRecord/Patient로 간략히 표현된다.

<106> 이와 같이, 상기 도 2에 대하여 접근 통제 모델을 구성하면 하기의 수학식 7과 같이 간략히 표현된다.

수학식 7

<107>
$$S = patientrecord \rightarrow PR$$
$$PR = patient \rightarrow P$$
$$P = personal \rightarrow PERS\ [\ ]\ medical \rightarrow MD$$
$$PERS = name \rightarrow N\ [\ ]\ address \rightarrow ADDR\ [\ ]\ birth \rightarrow BIRTH$$
$$MD = visit \rightarrow VISIT\ [\ ]\ physid \rightarrow PHYSID\ [\ ]\ (diagnosis \rightarrow DIAG\ [\ ]\ getdiagnosis \rightarrow GD)$$
$$GD = (xray \rightarrow XRAY\ [\ ]\ getxray \rightarrow GX)\ [\ ]\ (disease \rightarrow DIS\ [\ ]\ (prescription \rightarrow PRES\ [\ ]\ getprescription \rightarrow GPRES)$$

<108> 한편, XSquirrel 언어로 표현된 쿼리 q가 주어졌을 때, 이 쿼리는 경로지정 표현을 해석한 후, 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구 사항으로 명세할 수 있다.

<109> 예를 들어, 도 3에서 볼 수 있는 바와 같이 하기의 수학식 8과 같은 쿼리 q가 있다고 가정한다.

수학식 8

<110>
$$q=/PatientRecord/Patient/Medical/(VisitDate\ \#\ Physid\ \#\ Diagnosis)$$

<111> 그러면, 상기 수학식 8과 같은 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하면 하기의 수학식 9와 같은 질문 셋(answer set)인 $q(D)$가 생성되게 된다.

수학식 9

$$q[D] = \text{patientrecord} \rightarrow \text{patient} \rightarrow \text{medical} \rightarrow (\text{visit} \rightarrow \text{SKIP} [] \text{physid} \rightarrow \text{SKIP} [] \text{diagnosis} \rightarrow (\text{xray} \rightarrow \text{SKIP} [] \text{disease} \rightarrow \text{SKIP} [] \text{prescription} \rightarrow \text{SKIP}))$$

<112>

<113> 한편, 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 생성된 프로세스 알제브라 정형 모델은 접근 통제 규칙의 합집합으로 구성되어 있다.

<114> 프로세스 알제브라 정형 모델은 <Requester, Resource, Action>의 3개의 튜플로 구성되어 있으며, 프로세스 알제브라 언어에서는 상기 3개의 튜플은 채널 타입으로 표현될 수 있다.

<115> 이 경우, read를 채널 이름으로 정의하고, Requester를 채널 타입으로 선언하며, Action은 상기 read의 읽기 행위를 의미하며, 프로세스 알제브라 정형 모델을 Resource의 개념으로 트리 구조 형태를 가지고, read 이벤트 발생 후 Resource에 접근할 수 있도록 모델링한다. 이의 표현은 하기의 수학식 10과 같다.

수학식 10

$$\text{PEER} = 1 \ldots N$$

$$\text{channel read: PEER}$$

$$\text{PEER}_1 = \text{read} \rightarrow \text{ACP}$$

<116>

<117> 상기 수학식 10에서 $\text{PEER}_1, \text{PEER}_2, \cdots \text{PEER}_n$은 상기 Requester의 원소로, PEER은 read 채널 상에서 read.p_1의 이벤트 형태를 가지게 된다.

<118> 이는 전술한 바와 같이, 문서에 대한 모든 관련 접근 통제 규칙인 $\bigcup_i ACR_i$을 실행한 후, 클라이언트에게 필터링하여 보여지게 된다.

<119> 따라서, 접근 통제 규칙에서 허용 중복 의미론을 반영하기 위해서 경로 지정 언어의 인터리빙 오퍼레이터(interleveaving operator)인 '|||' 기호를 사용하여 접근 통제 규칙을 포함하는 프로세스 알제브라 정형 모델을 구축할 수 있다.

<120> 예를 들어, 도 1과 관련한 Dr. Kim의 접근 통제 정책 ACP 모델은 하기와 같이 프로세스 알제브라 정형 모델인 CSP 정형 모델로 표현될 수 있다.

수학식 11

$$\text{ACP} = \text{ACR}_1 ||| \text{ACR}_2$$

$$\text{ACR}_1 = \text{patientrecord} \rightarrow \text{patient} \rightarrow \text{medical} \rightarrow \text{visit} \rightarrow \text{STOP}$$

$$\text{ACR}_2 = \text{patientrecord} \rightarrow \text{patient} \rightarrow \text{medical} \rightarrow (\text{visit} \rightarrow \text{STOP} [] \text{physid} \rightarrow \text{STOP} [] \text{diagnosis} \rightarrow (\text{disease} \rightarrow \text{STOP} [] \text{prescription} \rightarrow \text{STOP}))$$

<121>

<122> 상기 수학식 1에서 ACR_1과 ACR_2는 도 2의 필터링 쿼리에 있어서 Rule 1과 Rule 2 각각에 대한 프로세스

알제브라 언어의 프로세스들을 나타낸다.

<123> 한편, 전술한 바와 같이, '$\cup$' 연산자는 프로세스 알제브라 언어의 '$|||$' 기호와 매핑된다. 그리고, '$\circ$' 연산자는 프로세스 알제브라 언어의 동기 병렬 연산자(synchronized parallel operator)인 $[|A|]$기호로 그 의미론을 반영한다.

<124> 이는 전술한 필터링 쿼리 q'는 프로세스 알제브라 정형 모델에서 Q'로 하기의 수학식 12와 같이 표현된다.

수학식 12

<125> $$Q' = Q|[A|](S[|A|](ACR_1 ||| ACR_2)$$

<126> 여기서, A는 이벤트의 집합으로 하기의 수학식 13과 같이 표현된다.

수학식 13

<127> $$A = \alpha(Q) \cup \alpha(S) \cup \alpha(ACR_1) \cup \alpha(ACR_1)$$

<128> 여기서, 스키마 프로세스 S, ACR_1, ACR_2의 병렬 구성(parallel composition)은 AXML 문서에 대한 스키마 레벨의 접근 통제 모델을 나타낸다.

<129> 한편, 상기와 같은 접근 통제 규칙에 대한 검증은 쿼리 Q프로세스의 추적 이벤트(trace event)의 집합이 스키마 프로세스 S와 ACP 프로세스의 추적 이벤트(trace event)의 부분집합이 되면, 접근 통제 규칙에 대한 요청자의 쿼리 q는 항상 허용(always grant)이 된다.

<130> 이는 하기의 수학식 14으로 표현할 수 있다.

수학식 14

<131> $$assert\ S\ |[A]|\ ACP \sqsubseteq_T Q$$

<132> 여기서, A는 전술한 바와 같이, S 프로세스와 ACP 프로세스의 합집합이며, $assert$는 접근 통제 규칙에 대한 정형검증도구인 FDR 도구에서 등가 체킹(equivalence checking) 예약어로 사용된다.

<133> $S\ |[A]|\ ACP$ 병렬 프로세스는 AXML 문서에 대한 스키마 레벨 접근통제모델을 나타낸다.

<134> 예를 들어, Dr. Kim으로부터 온 쿼리 q가 /PatientRecord/Patient/Medical/VisitDate 이라고 가정하기로 한다.

<135> 그러면, FDR 도구를 이용하여 시스템 모델이 상기 수학식 14의 속성을 만족하는지의 여부를 확인할 수 있다.

<136> 그러나,, 만약 쿼리 q가 /PatientRecord/Patient/Medical 이라면, CSP 모델 Q는 전술한 바와 같이 하기의 수학식 15에 따른 프로세스 모델로 변환되게 된다.

수학식 15

$$Q = patientrecord \rightarrow patient \rightarrow medical \rightarrow (visit \rightarrow STOP\ [\,]\ physid \rightarrow STOP\ [\,]\ diagnosis \rightarrow (xray \rightarrow STOP\ [\,]\ disease \rightarrow STOP\ [\,]\ prescription \rightarrow STOP))$$

<137>

<138> 이 경우, FDR 모델 체킹 도구는 CSP 모델 Q에서 <patientrecord, patient, medical, diagnosis, xray>에 대한 반례를 보여준다.

<139> 이 결과는 쿼리 q에 대해 Xray 노드에 대한 접근이 허용되지 않음을 의미한다.

<140> 그 결과로 접근 통제 규칙은 모든 관련 규칙들을 실행하여 비밀정보 Xray 데이터를 보호하기 위하여 쿼리 q를 q' 로 변환한다. 필터링된 쿼리 q는 하기의 수학식 16와 같다.

수학식 16

$$q' = /PatientRecord/Patient/Medical/(Diagnosis/(Disease\ \#\ Prescription) \#\ VisitDate\ \#\ Physid))$$

<141>

<142> 본 발명에서는 트리 구조의 쿼리, 스키마 및 접근 통제 규칙을 CSP 언어로 모델링하여, AXML 문서에 대한 쿼리 접근을 제한하기 위한 접근 통제 모델을 분석하기 위한 검증 방법을 제시하고 있다.

<143> 또한, 본 발명에 따른 접근 통제 규칙 및 쿼리 필터링 서비스에 의한 쿼리 재생성의 의미론을 CSP 언어로 변환하는 방법을 기술한다.

<144> 따라서, AXML 문서에 대한 쿼리, 접근 통제 규칙 및 스키마에 대한 CSP 모델이 주어졌을 때, 본 논문에서 제시한 정적 검증 방법은 요청 쿼리가 스키마 레벨 접근 통제 규칙에서 허용되는지 뿐만 아니라, 허용 및 거부되는 트리 구조의 계층형 정보를 보여줄 수 있다.

<145> 도 5는 본 발명에 따른 AXML 기반의 접근 통제 모델의 정형 명세 장치의 블록도를 도시한 것이다.

<146> 도 5를 참조하면, 본 발명에 따른 AXML 기반의 접근 통제 모델의 정형 명세 장치는 접근 통제 모델 생성부(510), 프로세스 알제브라 정형 모델 생성부(520), 쿼리 변환부(530) 및 보안 검증부(540)로 이루어질 수 있다.

<147> 접근 통제 모델 생성부(510)는 계층적 트리 구조 형태로 구성된 AXML 문서에 대하여 상기 AXML 문서의 스키마 및 경로 지정 언어에 따른 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성한다.

<148> 접근 통제 규칙은 단일 AXML 문서상에서 혹은 스키마 레벨에서 명시할 수 있다. 스키마 레벨의 접근 통제 규칙의 경우에는 스키마에 일맥 상통하는 모든 AXML 문서에 접근 통제 규칙을 적용할 수 있기 때문에, 객체에 대한 접근권한을 명시하는데 매우 효율적인 방법이므로, 본 발명에서는 상술한 바와 같이 스키마 레벨에서 접근 통제 규칙을 규정하는 방법을 적용한다.

<149> 본 발명은 오토마타 이론을 기반으로 스키마, 쿼리, 접근 통제 규칙 및 필터링 쿼리에 대하여 트리구조 형태의 접근 통제 모델을 구성한다.

<150> 접근 통제 모델을 구축할 경우, 상기 접근 통제 모델은 경로 지정 언어인 XSquirrel 조건 표현을 항상 만족하고 있다고 가정한다.

<151> 한편, 접근 통제 모델은 상기의 상술한 바와 동일하므로 중복된 상술은 가급적 생략하기로 한다.

<152> 프로세스 알제브라 정형 모델 생성부(520)는 상술한 AXML 문서에 대하여 생성된 접근 통제 모델을 프로세스 알

제브라 언어인 CSP 언어로 정형 명세하여 프로세스 알제브라 정형 모델을 생성한다.

<153> 이를 위해 본 발명에서는, 오토마타 스키마 모델 변환 모듈을 이용하여 AXML 문서에 대한 접근통제규칙을 명시한 경로 지정 언어인 XSquirrel 표현식에 따라 상기 접근 통제 모델을 오토마타(Automata) 형 스키마 모델로 변환한다.

<154> 그리고, 스키마 정형 모델 생성 모듈은 오토마타형 스키마 모델을 CSP 프로세스 알제브라 언어로 정형명세하여 스키마 정형 모델을 생성한다.

<155> 이와 같이 생성된 스키마 정형 모델은 CSP 프로세스 알제브라 문법에 맞게 변환되어 프로세스 알제브라 정형 모델이 생성된다.

<156> 그리고, 기존의 오토마타와의 구별점은 트리구조를 가지는 AXML 문서의 특정 노드의 속성 이름을 대수 표현으로 전환하여, 상기 대수 표현으로 전환된 속성값이 참일 경우에만 다음 하위 노드로의 질의를 수행할 수 있도록 구성하였다는 점에 있다.

<157> 한편, 쿼리 변환부(530)는 상기 AXML 문서에 대하여 클라이언트의 쿼리가 발생하면, 상기 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 접근 통제 모델에 대한 요구사항으로 명세하고, 상기 클라이언트에게 상기 프로세스 알제브라 정형 모델 생성부(520)에서 생성된 프로세스 알제브라 정형 모델에 따라 상기 AXML 문서에 대한 쿼리에 대응되는 정보를 전송한다.

<158> 이는 상술한 바와 같이, 접근 통제 모델 생성부(510)에서 클라이언트별 접근 통제 규칙을 이용하여 접근 통제 모델을 생성하고, 프로세스 알제브라 정형 모델 생성부(520)에서 접근 통제 모델을 프로세스 알제브라 언어로 변환하여 프로세스 알제부라 모델을 생성한 후, 상기 AXML 문서에 대하여 클라이언트의 쿼리가 발생하면, 클라이언트의 쿼리를 프로세스 알제브라 언어로 변환하여 상기 생성된 접근 통제 모델에 대한 요구사항으로 명세하고, 상기 프로세스 알제브라 정형 모델에 따라 클라이언트에게 AXML 문서에 대한 쿼리에 대응되는 정보를 전송하게 된다.

<159> 여기서 클라이언트별 접근 통제 규칙은 상기 클라이언트에 대한 상기 AXML 문서의 특정 정보에 대하여 허용 또는 거부로 명시되는 것을 특징으로 할 수 있다.

<160> 그리고, 상기 클라이언트별 접근 통제 규칙은 전술한 바와 같이 특정 규칙에 있어서 충돌이 발생하는 경우, 허용 중복 또는 거부 중복 알고리즘에 따라 클라이언트별 접근 통제 규칙이 결정될 수 있다.

<161> 또한, 쿼리 변환부(530)는 상기 클라이언트로부터 상기 AXML 문서의 특정 서비스 호출에 따라 상기 클라이언트의 쿼리를 수신하고, 상기 수신된 클라이언트의 쿼리를 상기 접근 통제 모델의 접근 통제 규칙에 따라 쿼리 필터링을 수행하여 필터링 쿼리를 생성한다.

<162> 필터링 쿼리에 생성하는 것에 대한 설명은 상기에 상술한 바와 동일하다.

<163> 마지막으로, 보안 검증부(540)는 상기 프로세스 알제브라 정형 모델을 FDR 모델 체킹 도구를 이용하여 상기 AXML 문서에 대한 보안 검증을 수행한다.

<164> 이는, 생성된 프로세스 알제브라 정형 모델의 보안 적합성을 평가하는 것으로 전술한 바와 동일하므로 중복된 상술은 생략하기로 한다.

<165> 한편, 본 발명은 AXML 기반의 접근 통제 모델의 정형 명세 방법은 소프트웨어를 통해 실행될 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

<166> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 테이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<167> 본 발명은 도면에 도시된 일 실시예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시예의 변형이 가능하다는 점을 이해할 것이다. 그러나,

이와 같은 변형은 본 발명의 기술적 보호범위내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

도면의 간단한 설명

<168> 도 1은 본 발명에 적용되는 AXML 문서의 내장형 시스템 호출 및 필터링 서비스의 일 예를 도시한 것이다.

<169> 도 2는 본 발명에 적용되는 트리 구조의 형태로 각각의 경로를 가진 데이터 노드로 구성된 AXML 문서 스키마를 도시한 것이다.

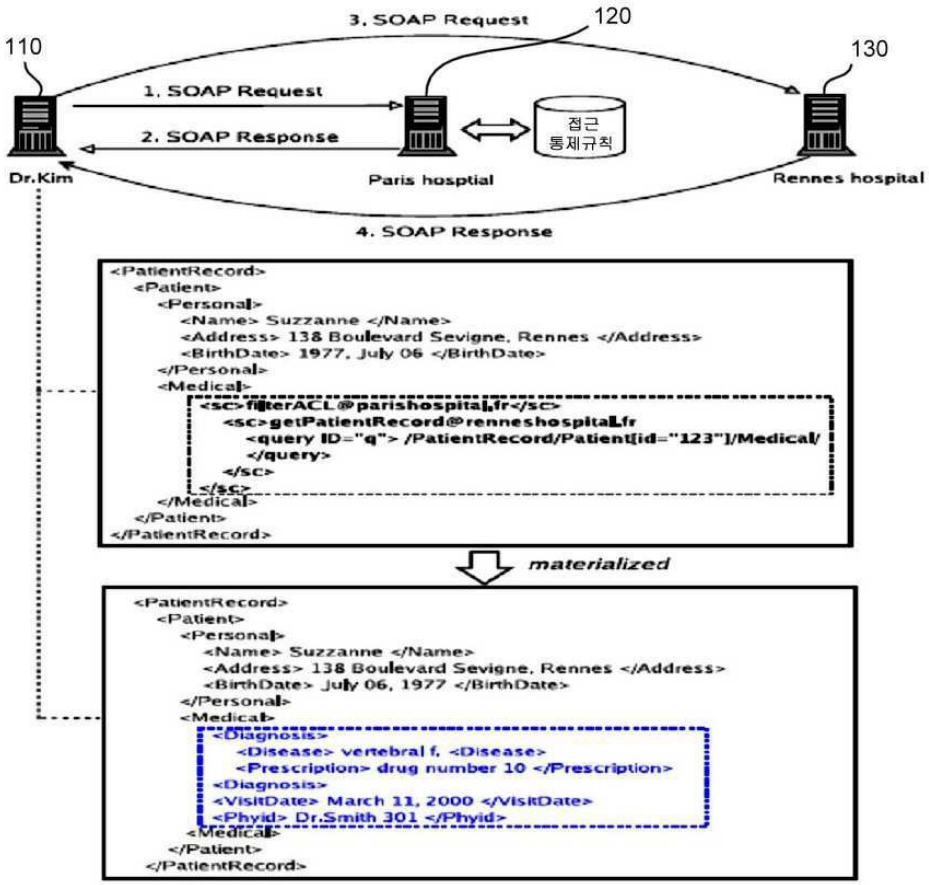
<170> 도 3은 각 정보에 대한 데이터 매핑 및 접근 통제 규칙을 XSquirrel로 표현한 것이다.

<171> 도 4는 본 발명에 따른 AXML 기반의 접근 통제 모델의 정형 명세 방법의 흐름도이다.

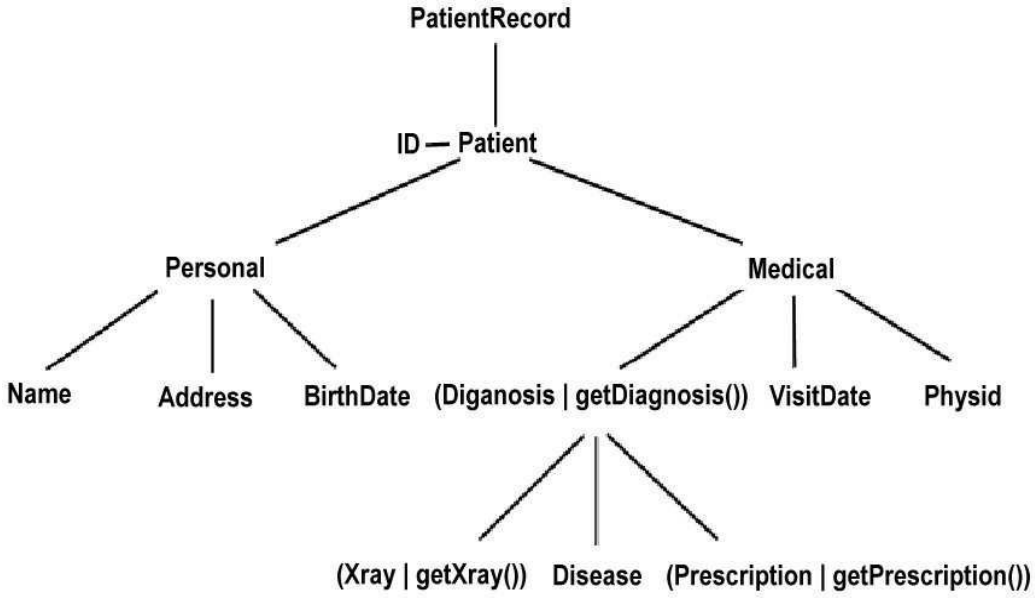
<172> 도 5는 본 발명에 따른 AXML 기반의 접근 통제 모델의 정형 명세 장치의 블록도이다.

도면

도면1



도면2



도면3

Mapping Rule	Sub-document	Resource Location
1	/PatientRecord/Patient[ID="1234"]/	www.renneshospital.com

(a) Data mappings between the sub-document for patient records and remote source location

Rule	Requester	Action	Resource
1	Kim	read	/PatientRecord/Patient/Medical/VisitDate
2	Kim	read	/PatientRecord/Patient/Medical/(VisitDate # Physid # Diagnosis/(Disease # Prescription))
3	Lee	read	/PatientRecord/Patient/Medical/VisitDate

(b) Access control rules

Query q from Dr. Kim : /PatientRecord/Patient/Medical/(VisitDate # Physid # Diagnosis)

⇩ *query rewriting*

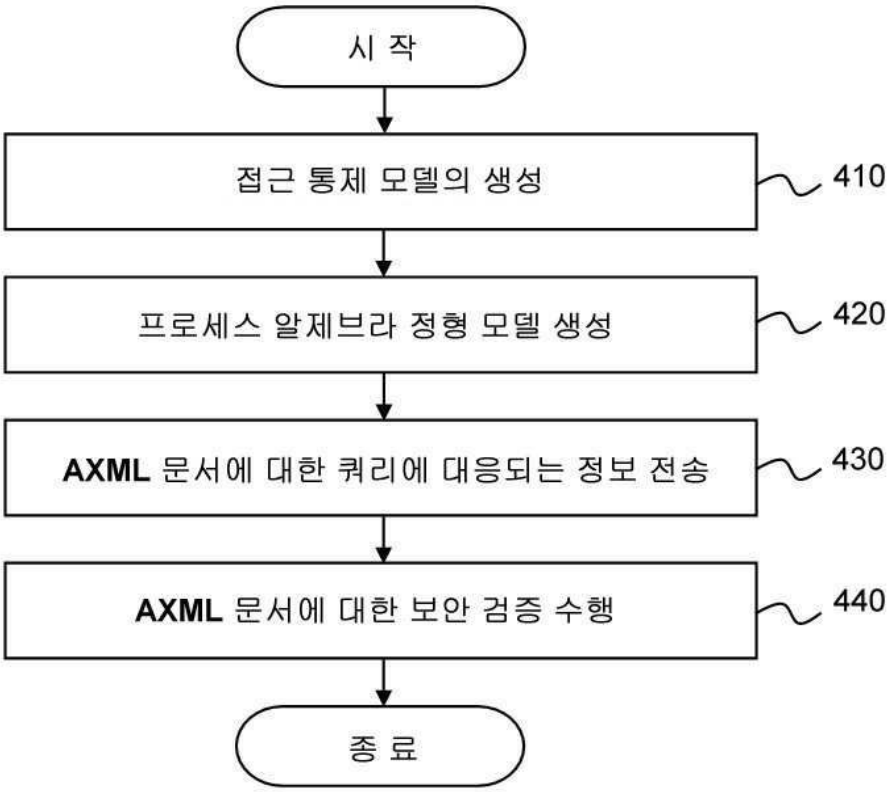
Rule1 = /PatientRecord/Patient/Medical/VisitDate
Rule2 = /PatientRecord/Medical/(VisitDate # Physid # Diagnosis(Disease # Prescription))

q' = q ∘ (Rule1 U Rule2)

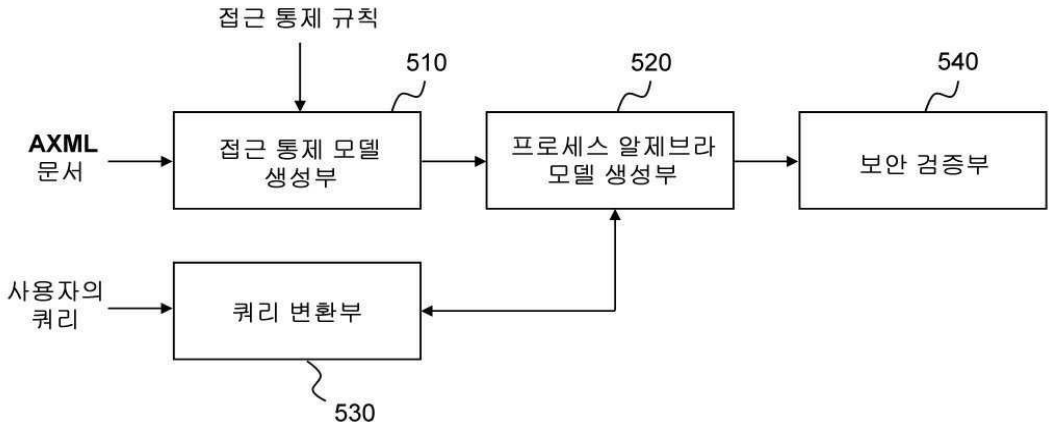
Filtered query q' : /PatientRecord/Patient/Medical/(VisitDate # Physid # Diagnosis/(Disease # Prescription))

(c) Query filtering

도면4


시 작
접근 통제 모델의 생성
410
프로세스 알제브라 정형 모델 생성
420
AXML 문서에 대한 쿼리에 대응되는 정보 전송
430
AXML 문서에 대한 보안 검증 수행
440
종 료

도면5


접근 통제 규칙
510
520
540
AXML 문서
접근 통제 모델 생성부
프로세스 알제브라 모델 생성부
보안 검증부
사용자의 쿼리
쿼리 변환부
530