(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년06월26일
(11) 등록번호 10-1751088
(24) 등록일자 2017년06월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/44* (2013.01)
(21) 출원번호 10-2012-7012954
(22) 출원일자(국제) 2010년10월29일
심사청구일자 2015년09월24일
(85) 번역문제출일자 2012년05월18일
(65) 공개번호 10-2012-0117018
(43) 공개일자 2012년10월23일
(86) 국제출원번호 PCT/US2010/054722
(87) 국제공개번호 WO 2011/062743
국제공개일자 2011년05월26일
(30) 우선권주장
12/622,441 2009년11월20일 미국(US)
(56) 선행기술조사문헌
US20070156694 A1
US20080155687 A1
JP2007293630 A

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
벤-지비 니르
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
페루말 라자 파자니벨
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인

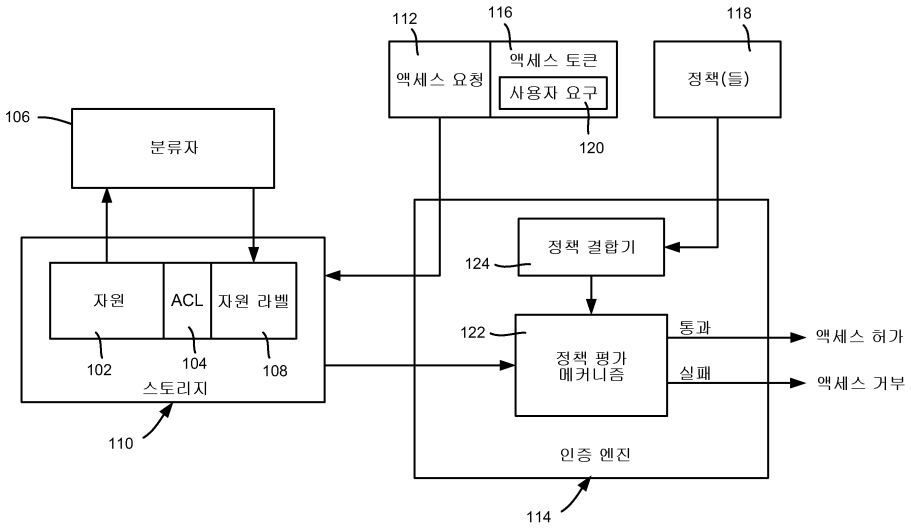
전체 청구항 수 : 총 20 항 심사관 : 홍경아

(54) 발명의 명칭 **자원 속성에 기초한 자원 액세스의 제어**

(57) 요 약

자원으로부터 분리된 정책에 따라 액세스 요청의 사용자 요구에 대해 자원의 자원 레벨을 평가함에 의해 자원에 대한 액세스가 판단되는 기술이 설명된다. 자원은 파일일 수 있으며, 자원 라벨은 파일을 분류 속성으로 분류함으로써 얻어질 수 있어서, 파일의 변경은 그 자원 라벨을 변경할 수 있으며, 그에 의해 어떤 사용자가 파일에 액세스할 수 있는 지를 변경한다. 자원 라벨 기반 액세스 평가는 자원에 대한 액세스를 허가하거나 거부할 것인지를 판단하기 위해 종래의 ACL 기반 액세스 평가와 논리적으로 결합될 수 있다.

대 표 도



(72) 발명자

사무엘슨 앤더스

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

햄블린 제프리 비

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

칼라흐 란

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

리 지쿠안

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

울링크 마티아스 에이치

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

로 클라이드

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

올틴 폴 아드리안

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

명 세 서

청구범위

청구항 1

컴퓨팅 환경에서 수행되는 방법으로서,

적어도 하나의 처리 장치에 의해, 자원(resource)으로부터 분리된 정책에 기초하여 상기 자원에 대한 액세스를 결정하는 단계- 상기 결정하는 단계는 상기 자원과 연관된 자원 라벨(resource label)이 캐싱되어 있는지 여부를 판정하고, 상기 자원 라벨이 캐싱되어 있지 않은 경우 상기 자원을 분류하여 상기 자원 라벨을 캐싱하고, 상기 자원 라벨이 캐싱되어 있는 경우 상기 자원 라벨이 유효한지 또는 재분류가 필요한지 여부를 평가하고, 액세스 요청과 연관된 사용자 요구(user claim)에 대해 상기 자원과 연관된 상기 자원 라벨을 평가함으로써 수행되고, 상기 자원 라벨은 상기 자원에 대한 액세스를 결정하는 데 사용되는 상기 자원과 연관된 분류 속성(classification property)을 포함하고, 상기 액세스 요청은 상기 사용자 요구에 의해 요청되는 상기 자원을 식별함 -와,

상기 자원 라벨이 유효하지 않다는 판정에 응답하여, 유효한 자원 라벨을 획득하기 위해 상기 자원의 재분류를 요구하는 단계와,

상기 자원 라벨의 평가와 상기 사용자 요구에 근거하여 상기 정책이 상기 자원에 대한 액세스를 허가한다는 판정에 응답하여, 상기 자원에 대한 액세스를 허용하는 단계와,

상기 자원 라벨의 평가와 상기 사용자 요구에 근거하여 상기 정책이 상기 자원에 대한 액세스를 허가하지 않는다는 판정에 응답하여, 상기 자원에 대한 액세스를 거부하는 단계

를 포함하는 방법.

청구항 2

제 1 항에 있어서,

액세스를 허가할 때 액세스 제어 리스트 검증과 자원 라벨 검증 모두가 요구되는지 또는 상기 액세스 제어 리스트 검증 및 상기 자원 라벨 검증 중 하나의 검증만으로도 상기 자원에 대한 액세스에 충분한지 여부를 판정하는 단계를 더 포함하는 방법.

청구항 3

제 2 항에 있어서,

상기 자원을 분류하기 위한 분류 규칙은 특정 자원 라벨을 특정 파일에 할당하는 선언형 명령어를 포함하는 방법.

청구항 4

제 1 항에 있어서,

상기 자원은 파일이며,

상기 파일의 콘텐츠의 변경, 상기 파일의 하나 이상의 라벨의 변경, 상기 파일의 다른 속성의 변경, 상기 파일의 위치의 변경, 분류 규칙의 변경 및 하나 이상의 분류 규칙의 상태 변경 중 적어도 하나의 변경에 기초해서 상기 자원 라벨을 업데이트하기 위한 상기 자원의 재분류를 수행하는 단계를 더 포함하는 방법.

청구항 5

제 1 항에 있어서,

상기 자원에 연결된 액세스 제어 리스트에 기초해서 상기 액세스를 결정하는 단계를 더 포함하는 방법.

청구항 6

제 1 항에 있어서,

상기 액세스 요청과 연관된 상기 사용자 요구에 대해 상기 자원과 연관된 상기 자원 라벨을 평가하는 단계는 복합적인 조건을 평가하는 단계를 포함하는 방법.

청구항 7

제 1 항에 있어서,

상기 액세스 요청에 대응하는 하나 이상의 액세스 관련 동작을 평가하고 상기 자원 라벨 및 액세스 제어 리스트 중 적어도 하나에 기초하여 상기 하나 이상의 액세스 관련 동작 각각이 허용되는지 여부를 판정하는 단계를 더 포함하는 방법.

청구항 8

제 1 항에 있어서,

상기 액세스 요청과 연관된 상기 사용자 요구에 대해 상기 자원 라벨을 평가하는 단계는 상기 사용자 요구에서의 데이터에 대응하는 사용자 승인 레벨 값(user clearance level value)이 상기 자원 라벨에서의 데이터에 대응하는 자원 민감성 레벨 값(resource sensitivity level value)을 달성하는지를 판단하는 단계를 포함하는 방법.

청구항 9

컴퓨팅 환경에서의 시스템으로서,

하나 이상의 프로세서와,

인증 엔진을 포함하되,

상기 인증 엔진은 상기 하나 이상의 프로세서에 의해 실행되어 정책에 기초하여 자원에 대한 액세스를 결정하도록 구성되고, 상기 인증 엔진은 상기 정책 내의 정보를 이용하여 액세스 요청과 연관된 사용자 요구에 대해 상기 자원과 연관된 자원 라벨을 평가하되, 상기 자원 라벨이 유효한지 또는 업데이트된 자원 라벨을 얻기 위한 재분류가 필요한지 여부도 결정하도록 구성되고, 상기 자원 라벨은 상기 자원에 대한 액세스를 결정하는 데 사용되는 상기 자원과 연관된 분류 속성을 포함하고, 상기 액세스 요청은 상기 사용자 요구에 의해 요청되는 상기 자원을 식별하는

시스템.

청구항 10

제 9 항에 있어서,

상기 인증 엔진은 운영 체제의 보안 모델에 통합되는

시스템.

청구항 11

제 9 항에 있어서,

상기 정책은 정책 구성요소들의 조합에 기초하는

시스템.

청구항 12

제 9 항에 있어서,

상기 정책은 상기 자원에 독립적으로 유지되며, 복수의 자원에 적용되는

시스템.

청구항 13

제 9 항에 있어서,

파일을 포함하는 상기 자원에 대한 하나 이상의 자원 라벨을 제공하도록 구성된 분류자를 더 포함하되, 상기 분류자는 또한 상기 파일의 콘텐츠와 연관된 민감성 레벨을 포함하여, 상기 파일의 콘텐츠를 분류함으로써 상기 하나 이상의 자원 라벨을 제공하도록 구성되는

시스템.

청구항 14

제 9 항에 있어서,

상기 자원은 액세스 제어 리스트와 연관되고, 상기 인증 엔진은 상기 사용자 요구에 대해 상기 자원 라벨을 평가하도록 구성되고 또한 상기 자원에 대한 액세스를 결정하기 위해 액세스 토큰에 대해 상기 액세스 제어 리스트를 평가하도록 구성된

시스템.

청구항 15

제 9 항에 있어서,

상기 자원은 파일을 포함하며, 상기 자원 라벨은 상기 파일의 대체 데이터 스트림에 캐싱되는

시스템.

청구항 16

컴퓨터 실행가능 명령어가 저장된 하나 이상의 컴퓨터 저장 장치로서,

상기 컴퓨터 실행가능 명령어는 컴퓨터에 의해 실행되는 경우 상기 컴퓨터로 하여금,

액세스 요청을 처리하여 자원에 대한 액세스를 허가 또는 거부하는 단계- 이 단계는 상기 액세스 요청에 대응하는 하나 이상의 액세스 관련 동작을 평가하는 단계와, 상기 자원으로부터 분리된 정책을 획득하는 단계와, 상기 정책을 사용하여 또한 상기 액세스 요청과 연관된 사용자 요구에 대해 상기 자원과 연관된 자원 라벨을 평가함으로써 상기 하나 이상의 액세스 관련 동작 각각을 허가 또는 거부할지를 결정하는 단계를 포함하고, 상기 자원 라벨은 상기 자원에 대한 액세스를 결정하는 데 사용되는 상기 자원과 연관된 분류 속성을 포함하고, 상기 액세스 요청은 상기 사용자 요구에 의해 요청되는 상기 자원을 식별함 -

를 수행하게 하는

컴퓨터 저장 장치.

청구항 17

제 16 항에 있어서,

상기 자원은 파일이고, 상기 컴퓨터 실행가능 명령어는 또한 상기 컴퓨터로 하여금 상기 자원 라벨에 대응하는 분류 속성을 포함하는 분류 속성으로 상기 파일을 분류하게 하는

컴퓨터 저장 장치.

청구항 18

제 16 항에 있어서,

상기 자원은 파일이고, 상기 자원 라벨은 상기 파일과 연계하여 캐싱되며,

상기 컴퓨터 실행가능 명령어는 또한 상기 컴퓨터로 하여금

상기 자원 라벨이 유효하며 최신인지를 판정하는 단계와,

상기 자원 라벨이 유효하지 않고 최신이지 않다는 판정에 응답하여, 유효하며 최신인 자원 라벨을 획득하는 단

계와,

상기 유효하며 최신인 자원 라벨을 상기 파일과 연계하여 캐싱하는 단계

를 수행하게 하는

컴퓨터 저장 장치.

청구항 19

제 16 항에 있어서,

복수의 정책이 적용가능하며, 상기 정책을 사용하여 상기 액세스 관련 동작을 허가 또는 거부할 것인지를 판정하는 단계는 사용자 요구에 대해 상기 자원과 연관된 자원 라벨을 평가한 결과를 적어도 하나의 다른 정책 평가의 결과와 논리적으로 결합하는 단계를 더 포함하는

컴퓨터 저장 장치.

청구항 20

제 19 항에 있어서,

적어도 하나의 다른 정책 평가의 결과는 액세스 제어 리스트 기반 평가 결과를 포함하는

컴퓨터 저장 장치.

발명의 설명

배 경 기 술

[0001] 통상의 기업 환경에서, 유지되며 처리되는 데이터의 양은 엄청나며 빠르게 증가하고 있다. 정보 기술(IT) 부서는 수십 개의 포맷으로 수백만 또는 심지어 수십억 개의 파일을 처리해야 한다. 더욱이, 기존의 수는 상당한(예를 들어, 두 자리 수의 연간 성장) 비율로 증가하는 경향이 있다.

[0002] 그러한 데이터 사이즈 및 성장에 따라, 다수의 복합 시나리오가 규정 준수, 보안, 및 저장에 관련하여 IT 부서에 의해 고려될 필요가 있다. 이 시나리오들은 구조화되지 않은 데이터(예를 들어, 파일), 반구조화된 데이터(예를 들어, 속성 저장소를 갖는 파일), 및 구조화된 데이터(예를 들어, 데이터베이스)와 관련이 있다. 흔히 이들 데이터는 능동적으로 관리되지 않으며, 파일 공유 디렉토리(file shares)에서 구조화되지 않은 형태로 유지된다.

[0003] 파일과 같은 자원(객체)에 대한 액세스를 관리하기 위해, 현재의 보안 모델은 인증되지 않은 사용자의 액세스를 제한하면서 정당한 사용자가 액세스하는 것을 허용하는 객체에 대한 액세스 제어 정책을 구비하는 것에 기초한다. 그러나, 데이터를 포함하는 자원에 대한 액세스 제어 리스트(ACL)를 통해 사업 정책에 기초한 액세스를 보안 유지하는 것에 더하여, 기업은 또한 콘텐츠 민감성에 기초해서 데이터에 대한 보안을 유지하기를 바란다.

[0004] 예로서, 보안 그룹에 있는 수백 명의 사용자에게 판독 액세스를 허가하는 보안 정책을 갖는 파일을 고려하자. 언젠가 파일이 고객 기록 데이터를 노출시도록 파일 콘텐츠가 우연히 업데이트되면, 회사는 전체 보안 그룹에 그러한 액세스를 제공하는 것을 더 이상 원하지 않을 수 있다. 그러나, 콘텐츠 변경을 검출한 다음 보안 정책을 수정하는 자동적인 메커니즘이 존재하지 않는다.

[0005] 파일의 변경된 콘텐츠는 회사가 데이터를 어떻게 처리되기를 원하는지에 대한 다른 함의를 가질 수 있다. 예를 들어, 회사는 데이터를 포함하는 파일이 이메일에 첨부되거나 휴대용 스토리지 장치(예를 들어, USB 장치)에 클리어 텍스트로 복사되는 것을 방지하기 위한 것과 같은 목적으로 데이터가 어떻게 분배될 수 있는지를 변경하기 위해 민감 데이터를 추가하는 콘텐츠의 변경을 원할 수 있다.

[0006] 변경된 콘텐츠의 결과로서 액세스 및/또는 분산을 방지하는 것은 기존 보안 모델로는 가능하지 않다. 이것은 의도되지 않은 정보 누설 및 데이터의 내부자 침범을 가져오며, 규제 산업 및 공공 부문에서의 경우를 포함해서 다수의 기업 등과 직면해있는 중요한 이슈이다.

발명의 내용

과제의 해결 수단

[0007] 본 요약은 이하 상세한 설명에 더 설명되는 대표적인 개념의 선택을 간략화된 형태로 소개하기 위해 제공된다. 본 요약은 청구된 발명 대상의 중요 특징 또는 본질적 특징을 식별하도록 의도되지 않으며, 청구된 발명 대상의 범위를 제한하는 어느 방식으로 사용되도록 의도되지 않는다.

[0008] 간단히 말해서, 여기에 기재된 발명 대상의 각종 양상은 자원의 액세스 요청과 관련된 사용자 요구에 대해 자원과 관련된 자원 라벨을 평가하기 위한 정책에 기초해서 자원에 대한 액세스가 결정되는 기술에 관한 것이다. 일 구현예에서, 정책은 자원으로부터 분리되며, 자원으로부터 개별적으로/독립적으로 유지되어, 동일한 정책에 다수의 자원을 적용하는 방법을 제공한다.

[0009] 자원은 파일일 수 있으며, 자원 라벨은 파일을 분류 속성으로 분류함으로써 획득될 수 있다. 이와 같이, 예를 들어 파일의 콘텐츠 변경은 그 자원 라벨을 변경할 수 있는 재분류를 초래함으로써, 어떤 사용자가 각각의 사용자 요구 또는 요구들에 따라 파일에 액세스하는 지를 변경한다.

[0010] 액세스는 정책으로부터 결정될 수 있으며, 정책은 자원 라벨 대 사용자 요구 평가에만 기초해서, 또는 하나 이상의 다른 평가 결과와 조합해서 액세스를 지정할 수 있다. 예를 들어, 액세스 제어 리스트 대 사용자 토큰 평가는 액세스를 허가하거나 거부하는지를 판단할 시에 더 사용될 수 있다. 따라서, 예를 들어 정책은 액세스를 획득하기 위해 사용자가 사용자 그룹(ACL 기반 평가)의 회원 모두인 것 그리고 충분한 승인 레벨 대 자원 민감성 레벨(자원 라벨 기반 평가)을 가지는 것을 지정할 수 있다. 다른 예에서, 정책은 액세스를 획득하기 위해 사용자가 사용자 그룹(ACL 기반 평가)의 어느 한쪽의 회원인 것 또는 특정 프로젝트(자원 라벨 기반 평가)의 회원으로서 식별되는 것을 지정할 수 있다.

[0011] 다른 장점들은 도면과 연계하여 살펴볼 때 이하의 상세한 설명으로부터 명백해질 수 있다.

도면의 간단한 설명

[0012] 본 발명은 예로서 도시되며 동일 참조 숫자가 동일 요소를 지시하는 첨부 도면에 한정되지 않는다.

도 1은 자원 라벨 대 사용자 요구에 기초해서 자원 액세스를 제어하기 위한 컴퓨팅 환경에서 예시적 구성요소를 나타내는 블록도이다.

도 2는 자원에 대한 액세스를 허가할 때 보안 기관에 의해 취해질 수 있는 단계를 나타내는 순서도이다.

도 3은 본 발명의 각종 양상이 통합될 수 있는 컴퓨팅 환경의 예시적인 예를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 여기에 설명된 기술의 각종 양상은 일반적으로 자원을 분류함으로써 획득되는 분류 속성 세트(하나 이상의 분류 속성)에 기초해서 자원에 액세스 정책을 적용하는 것에 관한 것이다. 이것은 자원의 현재 콘텐츠를 처리함으로써 분류 속성 세트의 적어도 일부를 획득하는 것에 기초하고 있다.

[0014] 자원에 대한 액세스를 결정하기 위해 사용되는 자원과 관련된 분류 속성은 자원 라벨로 지칭된다. 이하에 기재된 바와 같이, 자원에 액세스를 요청하는 개체(entity)는 액세스 관련 동작을 허가하거나 거부할 것인지를 판단하기 위해 자원 라벨(또는 라벨들)에 대해서 평가되는 하나 이상의 사용자 요구를 제공한다. 따라서, 예를 들어 파일의 콘텐츠가 변경되면, 그 파일이 재분류되며, 그것에 의해 그 자원이 라벨 변경될 수 있으며, 그에 의해 그 변경된 자원 라벨에 대해 적절한 사용자 요구 또는 요구들을 갖지 않는 사용자에 대한 액세스를 방지한다. 보다 상세한 예로서, 파일이 이제 민감 데이터를 포함하도록 변경되면, 파일이 재분류되어, 사용자 요구를 갖지 않는 사용자에 대한 액세스를 방지하는 수정된 자원 라벨을 생성해서, 그들이 그러한 민감 데이터에 액세스하는 것을 허가한다.

[0015] 여기의 예 중 어느 것도 비제한적이라는 것이 이해되어야 한다. 실제로, 여기서는 설명을 위해 파일의 형태인 자원에 대한 액세스가 통상 설명되지만, 파일은 단지 자원의 한 타입이며, 다른 자원은 컴퓨터 및 주변 장치와 같은 물리적 개체, 및/또는 응용 역할과 같은 가상 개체뿐만 아니라, 파일, 데이터베이스 행 및/또는 열의 일부

와 같은 특정 데이터 세트 등을 포함할 수 있다. 이와 같이, 본 발명은 여기에 기재된 어느 특정 실시예, 양상, 개념, 구조, 기능 또는 예에 한정되지 않는다. 오히려, 여기에 기재된 실시예, 양상, 개념, 구조, 기능 또는 예의 어느 것도 비제한적이며, 본 발명은 통상 컴퓨팅 및 자원 액세스에 이익 및 장점을 제공하는 각종 방법에 사용될 수 있다.

[0016] 도 1은 액세스 제어 리스트(ACL)(104)와 현재 관련된 자원(102)이 적어도 하나의 자원 라벨(108)을 포함하는 분류 속성 세트를 획득하도록 분류자(106)에 의해 분류되는 예시적 컴퓨팅 환경을 도시한다. 분류는 자원과 관련된 다수의 분류 속성을 포함하는 속성 세트를 얻는 것이 될 수 있고, 속성 세트는 하나 이상의 자원 라벨을 포함할 수 있지만, 간결/설명을 위해 1개의 자원 라벨만이 도 1에 도시되어 있는 것에 주목하라. 파일 자원에 대해서는, 자원 및 ACL이 스토리지(110)에 유지되며, 그것은 자원 라벨(108)을 포함하는 분류 속성을 캐싱하기 위해 사용될 수도 있다.

[0017] 데이터 항목의 콘텐츠를 처리하는 것을 포함할 수 있는 분류는 여기에 참조로 통합된 미국 특허출원 제12/427,755호에 더 설명되어 있다. 이 기술은 분류 속성을 파일에 규정 및 할당하며 이 속성에 기초해서 파일에 적용되는 액션을 파일 서버 상에 지정하기 위한 파일 분류 인프라스트럭처(FCI)로서 마이크로소프트 코포레이션의 Windows® Server 2008 R2에 구현되며, 파일 서버 자원 관리자(FSM) 서버 역할의 일부로서 이용 가능하다.

[0018] 자원 라벨(108)은 발명의 명칭이 "파일 분류를 위한 대안적 데이터 스트림 캐시(Alternate Data Stream Cache for File Classification)"이며 여기에 참조로 통합된 미국 특허출원 제12/605,451호에 기재된 바와 같이 특정 방식, 예컨대 자원 라벨을 특정 규칙에 따라 문서에 자동적으로 할당하는 선언적 분류 규칙에 의해, 분류 속성의 캐시에 대한 참조 포인터에 의해, 및/또는 자원 라벨을 파일 자원의 교체 데이터 스트림에 저장함에 의해 자원과 관련된다. 자원 라벨이 분류 규칙으로부터 추정될 수 있으며, 반드시 저장될 필요가 없는 것에 주목하라.

[0019] 통상, 자원 라벨(108)은 정책을 적용하기 위해 사용자 요구와 함께 사용될 수 있는 정보를 포함한다. 그러나, 캐싱된 자원 라벨은 기간이 경과되거나 그렇지 않으면 무효가 될 수 있다. 예를 들어, 파일이 수정되거나 이동되는(그것에 의해 속성이 기간이 경과되게 하는) 경우를 포함하여 캐싱된 자원 라벨이 기간이 경과될 수 있는 다수의 방식이 존재하며, 이것은 콘텐츠 변경, 및/또는 파일이 재명명되거나 파일 시스템 내의 다른 위치(새로운 위치에 기초해서 분류 변경으로 될 수 있는)로 이동되는 경우를 포함한다. 캐싱된 자원 라벨이 무효가 되는 다른 방식은 이전 분류에 사용된 분류 규칙(미국 특허 출원 일련번호 제12/427,755호에 기재된)이 그 후 수정된 경우, 및/또는 분류를 결정하는 모듈의 내부 상태 또는 구성이 수정되는 경우이다. 예를 들어, 분류 규칙이 변경되지 않을지라도, 2개 이상의 분류 규칙을 조합하는 순서 및/또는 방법이 변경될 수 있고, 그러한 상태 변경은 다른 파일 속성 분류 결과 및 그것에 의해 캐싱된 자원 라벨이 될 수 있다.

[0020] 따라서, 사용자 요구에 대해 자원 라벨을 평가하기 전에, 캐시 자원 라벨의 유효성 및 최신의 상태는 재분류가 요구되는지를 판단하기 위해 검사된다. 재분류가 요구되면, 재분류는 상술한 미국 특허 출원에 기재된 바와 같이 수행된다. 캐싱된 속성 세트의 일부 또는 모두가 유효성에 대해 검사되며 그리고/또는 자원의 일부 또는 모두가 캐싱된 속성 세트를 업데이트하기 위해 재분류될 수 있는 것에 주목하라.

[0021] 자원 라벨 인식 보안 모델에 의한 정책 적용을 살펴보면, 자원(102)에 대한 액세스 요청(112)이 보안 인증 엔진(114)(예를 들어, 운영 체제로 내장되는)에 의해 수신될 때, 인증 엔진(114)은 액세스 요청(112)에서 식별되는 액세스 관련 동작이 허용되는지를 확인하기 위해 요청을 처리한다. 일 구현예에서, 액세스 요청(112)은 정책 또는 정책들(118)에 따라 자원의 ACL(104)에 대해 평가될 수 있는 종래의 액세스 토큰(116)과 관련된다.

[0022] 알려진 바와 같이, 종래의 ACL 기반 보안은 자원의 ACL과 토큰(116)을 비교한다. 그러나, ACL 기반 정책은 기본적으로 정적이고, 문서에서 콘텐츠(예를 들어, 데이터의 민감성)에 따라 변경되지 않는다. 외부 에이전트가 콘텐츠 변경을 감시하고 ACL을 적절히 변경하게 하는 것이 가능하지만, 이것은 상당한 관리 복잡성을 수반하므로 비현실적이다. 예를 들어, 그러한 에이전트는 특정 정책 변경의 경우 수백/수천 파일에 대한 정책을 감시하며 변경가능해야 한다.

[0023] 대조적으로, 여기에 기재된 바와 같이, 자원 라벨(108) 대 사용자 요구(120) 평가는 문서의 상태(예를 들어, 그 민감성, 파일이 속하는 프로젝트 등)와 이 라벨을 처리하는 정책(118) 사이에 분리를 제공한다. 정책 변경은 파일 상에 라벨을 유지하면서 중앙에서 수행될 수 있다.

[0024] 따라서, 여기에 기재된 바와 같이, 정책(또는 정책들)(118)에 따라, 사용자 요구(120)가 자원 라벨(108)에 대해 평가될 수 있는데, 이것은 액세스 관련 동작이 허용되는지를 판단하기 위해 자원의 현재 상태에 기초하고 있다.

도 1에 나타낸 바와 같이, 인증 엔진(114)의 정책 평가 메커니즘(122)(도 2를 참조하여 이하에 예시되는)은 보안 검사를 수행하며, 그것은 사용자 요구(120)를 포함하는 액세스 토큰(116)에 대한 ACL(104) 및/또는 자원 라벨(108)을 평가하는 것을 포함할 수 있다. 정책 평가 메커니즘(122)은 이 예에서 액세스를 허가 또는 거부한다.

[0025] 정책 결합기(124)가 도 1에 완결성을 위해 도시되어 있다. 통상, 조직에 걸쳐 및/또는 경영자에 의해 정의되는 바와 같이, 글로벌 정책, 도메인 특정 정책, 국부 정책, 디렉토리 정책 등과 같은 자원 액세스를 위한 다수의 정책 구성요소가 존재할 수 있다. 정책 적용에 통상 알려진 바와 같이, 계승, 무효, 블로킹 등과 같은 개념은 결합된 자원 정책을 설정하기 위해 사용될 수 있다. 그럼에도 불구하고, 정책이 이와 같이 원하는 만큼 복합적일 수 있지만, 작은 개개의 간단한 정책은 예를 들어 자원 라벨 및 ACL이 액세스 토큰/사용자 요구에 의해 만족되면 액세스를 허가하기 위해 여기에 설명된 기술과 함께 사용될 수 있다. 동시에, 그러한 정책은 이 정책이 개별 자원으로부터 분리되므로 변경하기 쉽다.

[0026] 일 구현예에서, 인증 엔진(114)은 마이크로소프트 코포레이션의 Windows® 7 강화 인증 런타임에 기초하고 있다. Windows® 7 런타임은 요구 기반(명칭 값 쌍 기반) 식별을 사용하여 복합 정책을 지정하기 위해 조건부 표현 언어를 지원한다.

[0027] 예로서, 이하의 정책(보안 기술자 정의 언어, 또는 SDDL로 재기록될 수 있는)은 XYZ 회사의 상근자가 10000(달러)보다 적은 승인 금액을 인가할 수 있다는 것을 진술한다:

[0028] (XA;;APPROVE;;;WD;(member_of{SG_XYZ,SG_FTE} AND

[0029] ApprovalAmount < 10000)).

[0030] 정책이 여기에 기재된 바와 같이 라벨 및 사용자 요구를 통해 어떻게 적용되는지의 예로서, 파일을 호스트하는 업무별과 같은 특정 환경에서 민감 고객 데이터에 액세스하기 위해 허가된 직원(보안 그룹에서 회원 자격으로 표시되는)에 의해 민감 고객 데이터를 지닌 문서에 대한 판독 액세스를 허용하고자 하는 회사를 고려하자. 이 타입의 정책은 그 목적이 환경에서 모든 민감 고객 데이터에 대한 허가된 직원 액세스를 허용하지 않도록 되어 있기 때문에 '필수'이지만 '충족'이 아닌 것을 평가하며, 오히려 액세스는 그렇게 하는 업무 요구가 존재할 때에만 허용된다. 이 충족 정책은 문서의 업무 요구에 따라 설정되는 ACL에 의해 명령된다.

[0031] 이 종류의 제한은 금융 정보, 고객 데이터 및 주요 업무 데이터의 누설을 방지하기 위해 금융, 건강 관리, 공공부문 등과 같은 규제 산업에서 정부 규제가 요구되거나 필요해진다. 상술한 바와 같이, 현재의 ACL 모델을 사용하는 정책 집행은 실용적이지 못하다. 여기에서의 기술은 정책을 자원에 물리적으로 첨부하지 않고서도 정책을 집행함으로써, 그것이 매우 탄력있고, 집행가능하며, 업무 민감 데이터를 지닌 컴퓨터의 하나 이상의 수집에 분산되게 한다.

[0032] 자원 라벨에 기초해서 특정 사용자 그룹에 액세스를 집행하고자 하는 회사의 예를 계속 살펴보면, 그룹 "SG ClearedPrnl"의 회원만이 "customerData" 요구를 지닌 파일을 판독할 수 있지만, 그 이외는 누구든지(자원의 ACL에 대한 다르게 적당한 토근을 갖는) 그러한 데이터를 갖지 않고서도 파일을 판독할 수 있는 것을 지정하기 위해, 하기의 것이 정책으로서 설정될 수 있다:

[0033] (XA;; GR;;; WD;(resource.Exists(customerData) AND

[0034] member_of{SG_ClearedPrnl} OR NOT(resource.Exists(customerData)))

[0035] 알 수 있듯이, 파일이 고객 데이터를 포함하면, 판독 액세스는 SG ClearedPrnl 그룹의 회원인 사용자에게만 허가된다. 파일이 고객 데이터를 이전에 포함하지 않았지만, 이 때 그것을 포함하는 것으로 수정되었다면, 파일이 재분류될 것이며(콘텐츠 변경으로 인해), 그 고객 데이터를 나타내는 그 파일과 관련된 자원 라벨이 그 파일에 존재한다. 따라서, 액세스는 고객 데이터가 파일에 존재하는지 여부에 기초해서 변경된다.

[0036] 다른 예로서, 자원 라벨 및 사용자 요구는 레벨을 할당받을 수 있으며, 그것은 이때 그 분류된 레벨에 기초해서 자원에 액세스를 허가하거나 허가하지 않는 비교 방법에 사용될 수 있다:

[0037] (XA;;GR;;;WD;(user.clearanceLevel >= resource.sensitivityLevel)

[0038] 자원이 먼저 분류될 때, 분류는 자원 라벨에 민감성 레벨을 설정한다. 자원의 민감성 레벨(자원 라벨에서 데이터에 대응하는 값 등)은 민감성 레벨이 달성되는지(그것에 의해 액세스가 허가되는지)를 판단하기 위해 사용자의 승인 레벨(사용자 요구에서 데이터에 대응하는 값 등)과 비교된다. 자원이 특정 방법으로 변경된 후 재분류

되면, 자원 라벨의 민감성 레벨이 변경됨으로써, 파일에 액세스하기 위해 요구되는 승인 레벨을 증가 또는 감소시킬 수 있다.

[0039] 다른 예는 그 사용자가 파일에 액세스할 수 있는 보안 그룹의 일부가 아닐지라도 사용자 프로젝트의 파일에 액세스를 허용한다. 예를 들어 컨설턴트와 같은 비직원은 이하의 정책(적절한 언어로 재기록될 수 있는)에 의해 직원만이 액세스할 수 있는 파일에 액세스를 할 수 있다:

[0040] (XA;;GR;;;WD;(user.projects OVERLAP resource.projects))

[0041] 상술한 것은 늦은 바인딩 결정을 허용하는 사용자 요구 및 자원 라벨를 포함하는 복합 조건의 평가를 제공하는 것에 주목하라. 일례는 "User.Projects any_ofresource.Projects" 등이다.

[0042] 도 2는 ACL 및/또는 자원 라벨 대 사용자 요구에 기초해서 자원에 대한 액세스를 결정하기 위해 정책이 어떻게 사용될 수 있는지의 간략화된 예를 도시한다. 도 2에는, ACL 및 자원 라벨을 사용하기 위해 예시된 2개의 가능한 정책, 즉 ACL 및 자원 라벨 둘 다가 액세스를 위해 요구되는지(즉, 충분한 승인을 받은 사용자 그룹 AND에서 회원이 되는 것과 같은 AND 논리 조합), 또는 어느 하나가 액세스를 허가하는지(즉, 프로젝트와 관련된 것으로 식별되는 사용자 그룹 OR에서 회원이 되는 것과 같은 OR 논리 조합)가 존재한다. 정책은 논리가 소정의 자원에 어떻게 적용되는지를 설정하며, 쉽게 인식될 수 있는 바와 같이, 더 복잡한 논리 조합(NOT, XOR 등)이 실행될 수 있다. 예를 들어, 자원 라벨은 액세스를 얻기 위해 다수의 그룹(컴파운드 프린시펄(compound principal))에서 사용자 회원 자격을 필요로 할 수 있다. 다른 예는 자원이 특정 양(특정 곳에 로그되는)으로 하루의 특정 시간에 적절한 사용자에게만 액세스 가능하게 하는 것과 같은 조건 등을 포함한다.

[0043] 단계 202는 소정의 자원에 대해서 자원 라벨이 캐시되는지, 즉 분류가 이전에 수행되었는지를 판단하는 것을 나타낸다. 그렇다면, 단계 204는 상술한 "파일 분류를 위한 대안적 데이터 스트림 캐시(Alternate Data Stream Cache for File Classification)" 특허 출원에 전체적으로 기재된 바와 같이 자원 라벨이 유효하고 최신인지 또는 재분류가 요구되는지를 평가한다. 초기 분류(단계 202) 또는 재분류(단계 204)가 요구되면, 단계 206은 자원을 분류/재분류하기 위해 실행된다. 단계 208은 후속 사용을 위해 자원 라벨 또는 라벨들을 포함한 분류 속성을 캐싱하는 것을 나타낸다.

[0044] 단계 210은 사용자의 액세스 토큰 대 자원의 ACL을 평가하는 것, 즉 종래의 액세스 체크를 수행하는 것을 나타낸다. 액세스가 허가되면, 단계 212는 그것이 이러한 간략화된 예에서 단독으로 충분한지(정책은 ACL이 OR 자원 라벨 액세스에 액세스하는 것을 지정하는지)를 평가하며, 그렇다면 액세스는 단계 220에 의해 표현된 바와 같이 허가된다. 이것은 "프로젝트" 예에 대응하며, 예를 들어, 사용자는 프로젝트 사용자 요구(대 자원 라벨)를 갖는 사용자 그룹 요구(대 ACL) OR에 의해 액세스를 허가할 수 있다.

[0045] "프로젝트" 예에서 액세스를 획득하는 다른 방법은 ACL이 단계 210에서 액세스를 허가하는 것이 아니라, 정책이 단계 214에서 "OR 자원 라벨"인 경우이다. 그렇다면, 단계 216은 단계 216에서 사용자 요구 대 자원 라벨을 통해 사용자 액세스를 평가한다. 자원 라벨이 액세스를 허용하면, 단계 216은 액세스를 허용하기 위해 단계 220으로 분기되며, 그 밖의 액세스는 단계 218을 통해 거부된다.

[0046] 앞서 설명된 바와 같이, 도 2의 논리는 민감 데이터에 대한 승인을 받은 보안 그룹 AND가 되도록 요구되는 것과 같은 "AND" 조합을 또한 취급한다. 단계 212 및/또는 214의 "AND" 분기를 수행함으로써 쉽게 인식될 수 있는 바와 같이 액세스는 ACL 검사가 통과되며 자원 라벨이 통과되는 것을 둘 다 필요로 한다. 단계 216이 자동적으로 통과되도록(후에 다르게 재분류되지 않으면) 분류는 파일에 대해 자원 라벨을 설정할 수 있으며, 예를 들어 민감성 레벨은 누구든지 다르게 재분류되지 않을 때까지 승인을 받도록 제로인 것에 주목하라.

[0047] 자원에 대한 요청된 액세스 관련 동작은 간단한 판독 또는 기록(또는 실행) 액세스보다 많을 수 있는 것에 주목하라. 상술한 예 중 하나를 사용하면, 사용자는 클리어 텍스트의 파일을 휴대용 스토리지 장치로(예를 들어, 직접 또는 클립보드를 통해) 복사하기 위해 파일 액세스를 요청할 수 있다. 판독 액세스가 액세스 정책의 경계 내에(예를 들어, 도메인 머신 상에) 있을 때 허용될 수 있을지라도, 클리어 텍스트의 복사는 자원 라벨 대 요청자의 사용자 요구에 반영되는 바와 같이 파일 콘텐츠에 따라 허용될 수 있거나 허용되지 않을 수 있다. 다른 예에서, 다른 요청된 액세스 관련 동작이 하나의 데이터를 이메일 메시지에 첨부할 수 있으며, 그것은 자원 라벨 대 요청자의 사용자 요구에도 의존할 것이다. 그러한 정책은 특정될 수 있으며, 적절히 구비된 인증 엔진/운영 체제에서 구현될 수 있다.

[0048] 더욱이, 액세스 정책은 파일의 교체 데이터 스트림과 같은 파일과 함께 이동될 수 있다. 예를 들어, 파일의 콘텐츠의 성질에 기초해서, 파일이 액세스 정책의 경계를 넘어 이동될 때 액세스 정책을 파일과 함께 패키지하는

것이 바람직할 수 있으며, 따라서 파일이 액세스 정책을 방해하지 않는 장치로 원래대로 복사되면 그 정책이 적용된다. 이 동작을 집행하기 위해 파일은 액세스 정책의 경계를 넘을 때 보호된다(예를 들어, 암호화된다).

[0049] 자원 속성에 기초해서 액세스하는 다른 시나리오는 저장소에 걸쳐 액세스 정책을 유지하는 것을 포함한다. 파일이 다른 머신과 저장소 사이에서 이동될(예를 들어, 파일 서버로부터 SharePoint®로 이동될) 때, 파일이 그 라벨을 유지하는 한, 그리고 파일은 분류 라벨이 동일한 액세스 정책에 참조되는 동일한 정책 도메인에 체류하는 한, 액세스 정책이 유지된다.

[0050] 이상과 같이, 파일의 분류 속성에 기초해서 파일에 액세스 정책을 적용하는 것을 포함하여 사용자 요구 대 자원 라벨에 기초하는 액세스 정책을 집행하기 위한 능력이 제공된다. 사용자 요구 및 자원 라벨은 승인/민감성 레벨과 같은 복잡한 조건 세트, 및/또는 다른 논리 조합에 사용될 수 있다. 이것은 컴파운드 프린시펄 및 다른 조건을 위해 포함해서 유연성 복합 정책을 쉽게 하며, 그것은 알려진 시스템에 현재 이용 가능하지 않다.

[0051] *전형적인 동작 환경*

[0052] 도 3은 도 1 및 2의 예가 구현될 수 있는 적절한 컴퓨팅 및 네트워킹 환경(300)의 예를 도시한다. 컴퓨팅 시스템 환경(300)은 단지 적절한 컴퓨팅 환경의 일례이며, 본 발명의 사용 또는 기능의 범위에 대해 특정 제한을 제시하도록 의도되지 않는다. 컴퓨팅 환경(300)은 예시적 운영 환경(300)에 도시된 구성요소 중 어느 하나 또는 조합에 관한 특정 종속성 또는 요구 사항을 갖는 것으로 해석되지 않아야 한다.

[0053] 본 발명은 다수의 다른 범용 또는 특수 목적 컴퓨팅 시스템 환경 또는 구성으로 동작한다. 본 발명에 사용하기 위해 적당할 수 있는 잘 알려진 컴퓨팅 시스템, 환경, 및/또는 구성의 예는 개인용 컴퓨터, 서버 컴퓨터, 핸드헬드 랩톱 장치, 태블릿 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 시스템, 셋톱 박스, 프로그램가능 가전, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 상기 시스템 또는 장치 중 어느 하나를 포함하는 분산 컴퓨팅 환경 등을 포함하지만, 이들에 한정되지 않는다.

[0054] 본 발명은 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터 실행 가능 명령어의 전체적인 컨텍스트에 기재될 수 있다. 통상, 프로그램 모듈은 루틴, 프로그램, 객체, 구성요소, 데이터 구조 등을 포함하며, 그것은 특정 태스크를 수행하거나 특정 추상 데이터 타입을 구현한다. 또한, 본 발명은 태스크가 통신 네트워크를 통해 링크되는 원격 처리 장치에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 메모리 스토리지 장치를 포함하는 국부 및/또는 원격 컴퓨터 저장 매체에 위치될 수 있다.

[0055] 도 3을 참조하면, 본 발명의 각종 양상을 구현하는 예시적 시스템은 컴퓨터(310)의 형태인 범용 컴퓨팅 장치를 포함할 수 있다. 컴퓨터(310)의 구성요소는 처리 유닛(320), 시스템 메모리(330), 및 시스템 메모리를 포함하는 각종 시스템 구성요소를 처리 유닛(320)에 연결하는 시스템 버스(321)를 포함할 수 있지만 이들에 한정되지 않는다. 시스템 버스(321)는 각종 버스 아키텍처 중 어느 하나를 사용하는 메모리 버스 또는 메모리 제어기, 주변 장치 버스, 및 로컬 버스를 포함하는 수 개의 타입의 버스 구조 중 어느 하나일 수 있다. 예지만 제한이 아닌 것으로서, 그러한 아키텍처는 업계 표준 아키텍처(ISA) 버스, 마이크로 채널 아키텍처(MCA) 버스, 향상된 ISA(EISA) 버스, 비디오 전자 공학 표준 위원회(VESA) 로컬 버스, 및 메자닌 버스(Mezzanine bus)로도 알려진 주변 장치 상호 연결(PCI) 버스를 포함한다.

[0056] 컴퓨터(310)는 통상 각종 컴퓨터 판독 가능 매체를 포함한다. 컴퓨터 판독 가능 매체는 컴퓨터(310)에 의해 액세스될 수 있으며 휘발성과 비휘발성 매체, 및 제거 가능과 제거 불가능 매체를 포함하는 특정 이용 가능 매체일 수 있다. 예지만 제한이 아닌 것으로서, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터와 같은 정보를 저장하기 위해 특정 방법 또는 기술로 구현되는 휘발성과 비휘발성, 제거 가능과 제거 불가능 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, 디지털 다용도 디스크(DVD) 또는 다른 광 디스크 스토리지, 자기 카세트, 자기 테이프, 자기 디스크 스토리지 또는 다른 자기 스토리지 장치, 또는 원하는 정보를 저장하기 위해 사용될 수 있으며 컴퓨터(310)에 의해 액세스될 수 있는 특정 다른 매체를 포함하지만, 이들에 한정되지 않는다. 통신 매체는 통상 반송파 또는 다른 전송 메커니즘과 같은 변조된 데이터 신호에 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터를 구체화하고 특정 정보 전달 매체를 포함한다. 용어 "변조된 데이터 신호"는 그 특징 중 하나 이상을 갖고 신호에서 정보를 인코드하는 그러한 방식으로 변경되는 신호를 의미한다. 예지만 제한이 아닌 것으로서, 통신 매체는 유선 네트워크 또는 직접 유선 접속과 같은 유선 매체, 및 음향, RF, 적외선 및 다른 무선 매체와 같은 무선 매체를 포함한다. 상술한 것 중 어느 하나의 조합은 컴퓨터 판독 가능 매체의 범위 내에 포함될 수 있다.

[0057] 시스템 메모리(330)는 읽기 전용 메모리(ROM)(331) 및 랜덤 액세스 메모리(RAM)(332)와 같은 휘발성 및/또는 비휘발성 메모리의 형태인 컴퓨터 저장 매체를 포함한다. 시동 동안과 같이 컴퓨터(310) 내의 요소들 사이에서 정보를 전송하는데 원조하는 기본 루틴을 포함하는 기본 입/출력 시스템(333)(BIOS)은 통상 ROM(331)에 저장된다. RAM(332)은 통상 처리 유닛(320)에 즉시 액세스 가능하며 그리고/또는 이 처리 유닛에 의해 현재 운영되고 있는 데이터 및/또는 프로그램 모듈을 포함한다. 예지만 제한이 아닌 것으로서, 도 3은 운영 체제(334), 응용 프로그램(335), 다른 프로그램 모듈(336) 및 프로그램 데이터(337)를 도시한다.

[0058] 또한, 컴퓨터(310)는 다른 제거 가능/제거 불가능, 휘발성/비휘발성 컴퓨터 저장 매체를 포함할 수 있다. 단지 한 예로서, 도 3은 제거 불가능, 비휘발성 자기 매체로부터 판독되거나 이 매체에 기록되는 하드 디스크 드라이브(341), 제거 가능, 비휘발성 자기 디스크(352)로부터 판독되거나 이 디스크에 기록되는 자기 디스크 드라이브(351), 및 CD ROM 또는 다른 광 매체와 같은 제거 가능, 비휘발성 광 디스크(356)로부터 판독되거나 이 디스크에 기록되는 광 디스크 드라이브(355)를 도시한다. 예시적 운영 환경에 사용될 수 있는 다른 제거 가능/제거 불가능, 휘발성/비휘발성 컴퓨터 저장 매체는 자기 테이프 카세트, 플래시 메모리 카드, 디지털 다용도 디스크, 디지털 비디오 테이프, 고체 상태 RAM, 고체 상태 ROM 등을 포함하지만, 이들에 한정되지 않는다. 하드 디스크 드라이브(341)는 통상 인터페이스(340)와 같은 제거 불가능 메모리 인터페이스를 통해 시스템 버스(321)에 접속되며, 자기 디스크 드라이브(351) 및 광 디스크 드라이브(355)는 통상 인터페이스(350)와 같은 제거 가능 메모리 인터페이스에 의해 시스템 버스(321)에 접속된다.

[0059] 앞서 기재되고 도 3에 도시된 드라이브 및 그 관련 컴퓨터 저장 매체는 컴퓨터(310)를 위한 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 다른 데이터의 스토리지를 제공한다. 도 3에서 예를 들어 하드 디스크 드라이브(341)는 운영 체제(344), 응용 프로그램(345), 다른 프로그램 모듈(346) 및 프로그램 데이터(347)를 저장하는 것으로 도시되어 있다. 이들 구성요소는 운영 체제(334), 응용 프로그램(335), 다른 프로그램 모듈(336), 및 프로그램 데이터(337)와 동일하거나 이들과 다를 수 있는 것에 주목하라. 운영 체제(344), 응용 프로그램(345), 다른 프로그램 모듈(346), 및 프로그램 데이터(347)는 적어도 다른 복사인 것을 예시하기 위해 다른 숫자로 제공된다. 사용자는 명령 및 정보를 마우스, 트랙볼 또는 터치 패드로 통상 지칭되는 태블릿, 또는 전자 디지타이저(364), 마이크로폰(363), 키보드(362) 및 포인팅 장치(361)와 같은 입력 장치를 통해 컴퓨터(310)로 입력할 수 있다. 도 3에 도시되지 않은 다른 입력 장치는 조이스틱, 게임 패드, 위성 접시형 안테나, 스캐너 등을 포함할 수 있다. 이들 및 다른 입력 장치는 시스템 버스에 연결되는 사용자 입력 인터페이스(360)를 통해 처리 유닛(320)에 흔히 접속되지만, 병렬 포트, 게임 포트 또는 범용 직렬 버스(USB)와 같은 다른 인터페이스 및 버스에 의해 접속될 수 있다. 모니터(391) 또는 다른 타입의 표시 장치는 비디오 인터페이스(390)와 같은 인터페이스를 통해 시스템 버스(321)에도 접속된다. 또한, 모니터(391)는 터치 스크린 패널 등과 통합될 수 있다. 모니터 및/또는 터치 스크린 패널은 컴퓨팅 장치(310)가 태블릿 타입 개인용 컴퓨터에서와 같이 통합되는 하우징에 물리적으로 연결될 수 있다. 게다가, 컴퓨팅 장치(310)와 같은 컴퓨터는 스피커(395) 및 프린터(396)와 같은 다른 주변 출력 장치를 포함할 수도 있으며, 그것은 출력 주변 인터페이스(394) 등을 통해 접속될 수 있다.

[0060] 컴퓨터(310)는 원격 컴퓨터(380)와 같은 하나 이상의 원격 컴퓨터에 논리적 접속을 사용하는 네크워크 환경에서 동작할 수 있다. 원격 컴퓨터(380)는 개인용 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 다른 공통 네트워크 노드일 수 있으며, 메모리 스토리지 장치(381)만이 도 3에 도시되었을지라도 컴퓨터(310)에 대하여 상술한 요소 중 다수 또는 모두를 통상 포함한다. 도 3에 도시된 논리적 접속은 하나 이상의 근거리 통신망(LAN)(371) 및 하나 이상의 광역 통신망(WAN)(373)을 포함하지만, 다른 네트워크를 포함할 수도 있다. 그러한 네트워킹 환경은 오피스, 전사적 컴퓨터 네트워크, 인트라넷 및 인터넷에서 평범하다.

[0061] LAN 네트워킹 환경에 사용될 때, 컴퓨터(310)는 네트워크 인터페이스 또는 어댑터(370)를 통해 LAN(371)에 접속된다. WAN 네트워킹 환경에 사용될 때, 컴퓨터(310)는 통상 인터넷과 같은 WAN(373)에 걸쳐 통신을 설정하기 위한 모뎀(372) 또는 다른 수단을 포함한다. 내부 또는 외부일 수 있는 모뎀(372)은 사용자 입력 인터페이스(360) 또는 다른 적절한 메커니즘을 통해 시스템 버스(321)에 접속될 수 있다. 예컨대 인터페이스 및 안테나를 포함하는 무선 네트워킹 구성요소는 액세스 포인트 또는 피어 컴퓨터와 같은 적당한 장치를 통해 WAN 또는 LAN에 연결될 수 있다. 네트워크 환경에서, 컴퓨터(310)에 관하여 도시된 프로그램 모듈, 또는 그 일부는 원격 메모리 스토리지 장치에 저장될 수 있다. 예지만 제한이 아닌 것으로서, 도 3은 메모리 장치(381) 상에 존재할 때의 원격 응용 프로그램(385)을 도시한다. 도시된 네트워크 접속은 예시적이고 컴퓨터들 사이에서 통신 링크를 설정하는 다른 통신이 사용될 수 있는 것이 인식될 수 있다.

[0062] 보조 서브시스템(399)(예를 들어, 콘텐츠의 보조 표시를 위한)은 컴퓨터 시스템의 주요부가 저전력 상태에 있을

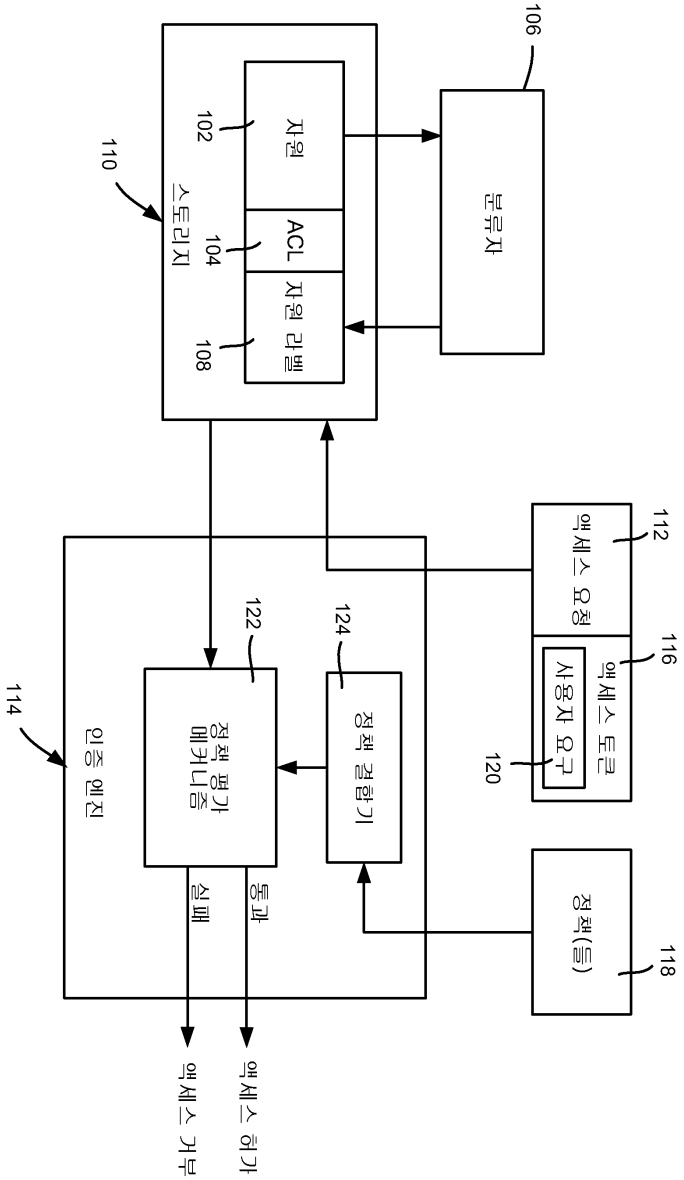
지라도 프로그램 콘텐츠, 시스템 상태 및 이벤트 통지와 같은 데이터가 사용자에게 제공되게 하기 위해 사용자 인터페이스(360)를 통해서 접속될 수 있다. 보조 서브시스템(399)은 주처리 유닛(320)이 저전력 상태에 있는 동안 이들 시스템들 사이에서 통신을 허용하기 위해 모뎀(372) 및/또는 네트워크 인터페이스(370)에 접속될 수 있다.

[0063] *결론*

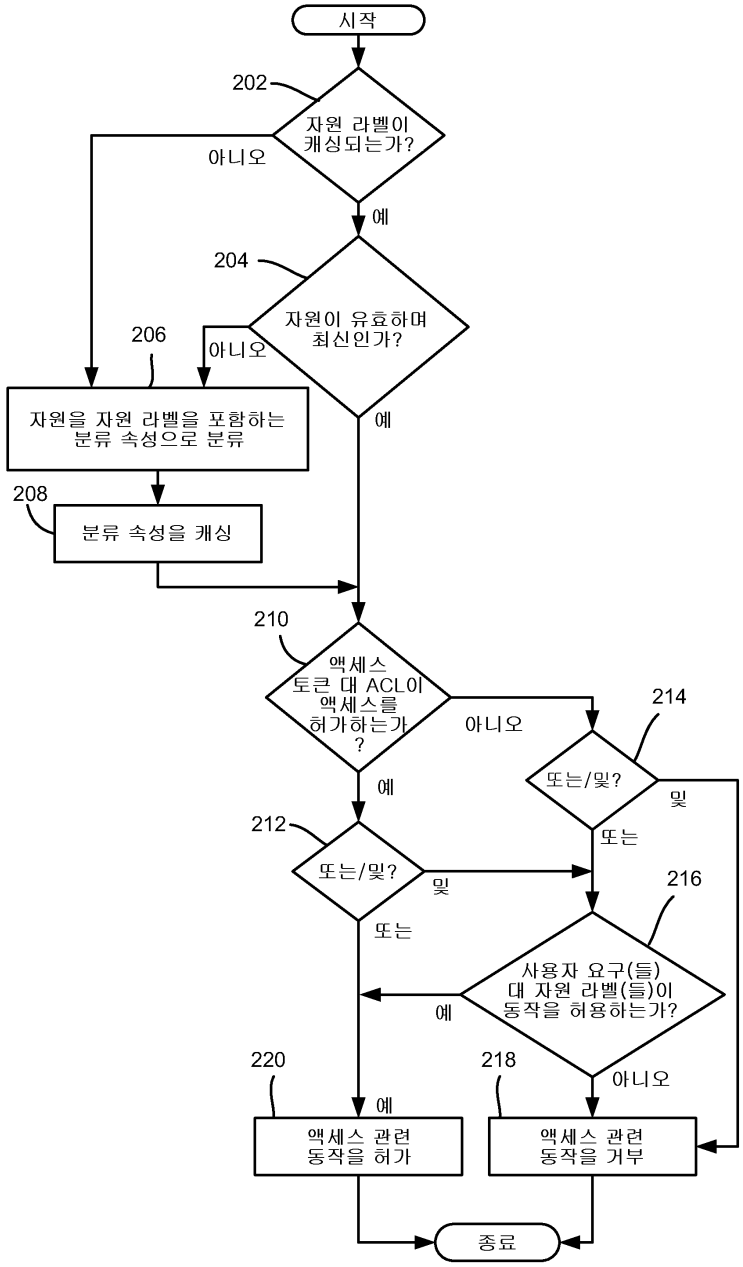
[0064] 본 발명이 다양한 수정 및 대안적 구성을 허용하지만, 특정한 예시적 실시예들이 도면에 도시되며 위에서 상세히 설명되었다. 그러나, 본 발명을 개시된 특정 형태로 제한할 의도는 없으며, 반대로 그 의도는 본 발명의 사상 및 범위 내에 있는 모든 수정, 대안적 구성, 및 균등물을 포괄하는 것으로 이해되어야 한다.

도면

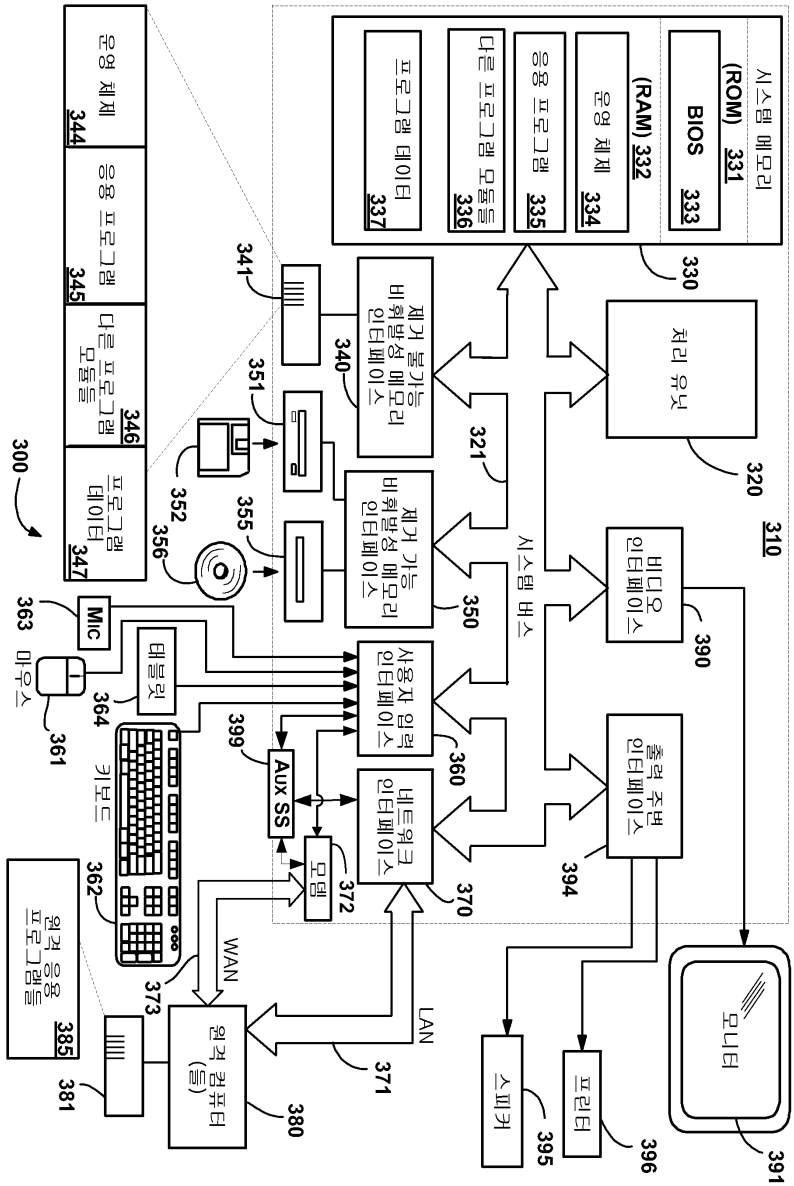
도면1



도면2


시작
202
자원 라벨이 캐싱되는가?
아니오
예
204
자원이 유효하며 최신인가?
206
아니오
예
자원을 자원 라벨을 포함하는 분류 속성으로 분류
208
분류 속성을 캐싱
210
액세스 토큰 대 ACL이 액세스를 허가하는가?
아니오
예
214
또는/및?
및
또는
212
또는/및?
및
또는
216
사용자 요구(들) 대 자원 라벨(들)이 동작을 허용하는가?
예
아니오
220
예
218
액세스 관련 동작을 허가
액세스 관련 동작을 거부
종료

도면3


시스템 메모리
(ROM) 331
BIOS 333
(RAM) 332
운영 체제 334
응용 프로그램 335
다른 프로그램 모듈들 336
프로그램 데이터 337
330
처리 유닛
320
310
시스템 버스
321
제거 불가능 비휘발성 메모리 인터페이스
340
341
제거 가능 비휘발성 메모리 인터페이스
350
351
352
355
356
비디오 인터페이스
390
출력 주변 인터페이스
394
사용자 입력 인터페이스
360
네트워크 인터페이스
370
Aux SS
399
모뎀
372
모니터
391
스피커
395
프린터
396
LAN
WAN
371
373
원격 컴퓨터(들)
380
원격 응용 프로그램들
385
381
300
운영 체제
344
응용 프로그램
345
다른 프로그램 모듈들
346
프로그램 데이터
347
Mic
363
마우스
361
364
태블릿
키보드
362