(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년12월30일
(11) 등록번호 10-1101085
(24) 등록일자 2011년12월23일

(51) Int. Cl.
G06F 12/14 (2006.01) *G06F 15/00* (2006.01)
(21) 출원번호 10-2004-0057575
(22) 출원일자 2004년07월23일
심사청구일자 2009년07월20일
(65) 공개번호 10-2005-0014678
(43) 공개일자 2005년02월07일
(30) 우선권주장
10/630,162 2003년07월30일 미국(US)
(56) 선행기술조사문헌
WO0079434 A1
US20030061216 A1
KR100343069 B1
US6453419 B1
전체 청구항 수 : 총 16 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
휴디스이레나
미국 98007 워싱턴주 벨레뷰 145번 애비뉴 사우쓰이스트 5607
노비크레브
미국 98006 워싱턴주 벨레뷰 사우쓰이스트 45번 스트리트 14116
(뒷면에 계속)
(74) 대리인
제일특허법인

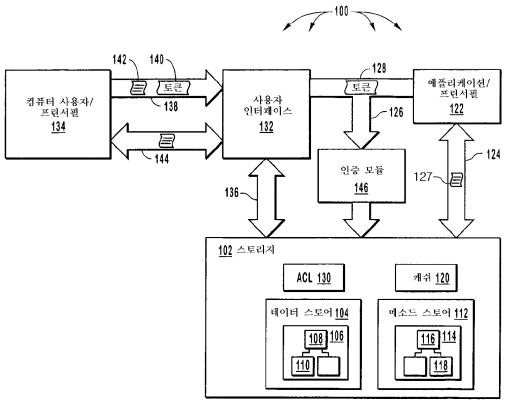
심사관 : 권오성

(54) 데이터 아이템의 구역 기반 보안 관리

(57) 요 약

디지털 보안의 관리에 대해 개시되어 있다. 데이터 아이템 및 메소드 아이템이 컴퓨터 시스템 상에서 볼륨 내에 저장되어 있다. 상기 볼륨은 비중첩 보안 구역으로 분할된다. 각각의 아이템은 보안 구역에 존재한다. 보안 규칙들이 프린서펄에 부여되며, 이 때 보안 규칙들은 특정의 구역 내의 아이템들에 적용된다. 보안 규칙들은 어떤 프린서펄이 어떤 아이템에 대해 무슨 권한(판독, 기록, 삭제 및 실행 등)을 가지고 있는지를 규정한다. 관리 권한은 2개의 보안 구역을 형성하도록 보안 구역을 분할함으로써 프린서펄에 의해 위임될 수 있다. 보안 구역에 대한 관리 권한을 갖는 프린서펄은 보안 구역들 중 하나에 추가의 프린서펄을 할당하면서도 다른 구역에 대한 모든 관리 권한을 유지한다. 따라서, 프린서펄은 어떤 아이템들에 대한 어떤 관리 권한을 그 자신이 배타적으로 보유하면서도 다른 아이템들에 대한 관리 권한을 다른 프린서펄들에 위임할 수 있다.

대 표 도



(72) 발명자

아낸드산제이

미국 98074 워싱턴주 삼마미쉬 사우쓰이스트 2번 플레이스 20902

아가월새미트에이치.

미국 98052 워싱턴주 레드몬드 노쓰이스트 넘버 씨-214 149번 플레이스 8127

래맨발랜세뚜

미국 98052 워싱턴주 레드몬드 노쓰이스트 50번 스트리트 16335

특허청구의 범위

청구항 1

시스템 메모리, 프로세서 및 컴퓨터 판독가능 매체를 포함하는 컴퓨터 시스템으로서, 데이터 스토어(data store) 및 메소드 스토어(method store)가 상기 컴퓨터 판독가능 매체에 저장되어 있고, 상기 데이터 스토어 및 상기 메소드 스토어는 상기 컴퓨터 판독가능 매체 상의 결합된 아이템 계층(combined item hierarchy)에 함께 배열되어 있고, 상기 데이터 스토어는 상기 메소드 스토어 내의 메소드에 의존하는 적어도 하나의 데이터 아이템을 갖고, 상기 메소드 스토어는 상기 데이터 스토어 내의 데이터에 의존하는 적어도 하나의 메소드를 가지며, 상기 결합된 아이템 계층은 하나 이상의 비중첩 보안 구역으로 나뉘어지며, 상기 하나 이상의 비중첩 보안 구역 각각은, 한 비중첩 보안 구역 내의 아이템들에 대한 권한을 갖는 프린서펄(principal)이 그 비중첩 보안 구역 내의 모든 아이템들을 공통 보안 규칙에 따라 균일하게 취급할 수 있도록, 공통 보안 규칙을 갖는 하나 이상의 메소드 아이템과 하나 이상의 데이터 아이템의 그룹으로서 정의되는 것인 컴퓨터 시스템에서, 프린서펄들에 대한 권한들의 보다 효율적인 할당을 용이하게 하기 위하여, 상기 하나 이상의 비중첩 보안 구역을 복수의 비중첩 보안 구역으로 분할하는 방법으로서,

상기 결합된 아이템 계층 내에서 새로운 공통 보안 규칙이 시행될 데이터 아이템들 및 메소드 아이템들의 그룹을 식별하는 단계 -상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹은 현재 상기 하나 이상의 비중첩 보안 구역들 중의 기존의 비중첩 보안 구역 내에 포함되어 있고, 기존의 공통 보안 규칙이 상기 기존의 비중첩 보안 구역 내에서 시행되며, 상기 기존의 공통 보안 규칙과는 다른 상기 새로운 공통 보안 규칙은 상기 기존의 비중첩 보안 구역 내에서 시행됨-;

상기 프로세서가, 전체 데이터베이스보다는 미세하지만(fine) 각 아이템에 대한 할당을 요구하지는 않을 정도로 거친(coarse) 입도(granularity)에서 권한들이 할당될 수 있도록, 상기 하나 이상의 비중첩 보안 구역을 재구성하는 단계

-상기 재구성하는 단계는,

상기 기존의 비중첩 보안 구역을 새로운 비중첩 보안 구역 및 상기 기존의 비중첩 보안 구역의 나머지(remnant)로 분할하는 단계 -상기 기존의 비중첩 보안 구역의 상기 나머지에 대한 상기 새로운 비중첩 보안 구역의 배열은 상기 결합된 아이템 계층 내에서의 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹의 위치에 기초하고, 상기 새로운 비중첩 보안 구역은 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹을 포함하고, 상기 기존의 비중첩 보안 구역의 상기 나머지는 상기 기존의 비중첩 보안 구역으로부터의 적어도 하나의 데이터 아이템 또는 메소드 아이템을 포함하고, 상기 분할하는 단계는 보안 구역들 간의 중첩을 방지하는 방식으로, 그리고 상기 데이터 아이템들 및 메소드 아이템들 중 어느 것도 하나보다 많은 보안 구역에 포함되지 않도록 제한됨-, 및

상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹이 상기 새로운 비중첩 보안 구역 내에 포함됨을 표현하기 위하여, 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 아이템들 각각의 데이터 속성(property)을 조정하는 단계

를 포함함- ;

상기 기존의 비중첩 보안 구역이 분할되었을 때 상기 기존의 비중첩 보안 구역에서 시행되고 있는 상기 기존의 공통 보안 규칙에 기초하여 상기 기존의 비중첩 보안 구역 내의 기존 권한들을 가졌던 임의의 프린서펄에 대하여, 상기 기존의 비중첩 보안 구역을 분할하는 단계에 후속하여, 그리고 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹이 상기 새로운 비중첩 보안 구역에 포함됨을 표현하기 위해 데이터 속성을 조정하는 단계에 후속하여, 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹을 포함하는 상기 새로운 비중첩 보안 구역 내에서 상기 임의의 프린서펄의 기존 권한들을 유지시키는 단계; 및

상기 새로운 공통 보안 규칙에 따라 상기 새로운 비중첩 보안 구역 내의 다른 권한들을 하나 이상의 추가 프린서펄에게 부여하는 단계 -상기 다른 권한들을 상기 새로운 비중첩 보안 구역에 할당하는 것은, 상기 새로운 비중첩 보안 구역으로의 상기 다른 권한들의 할당을 통해 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 각각의 아이템에 상기 다른 권한들을 집합적으로(collectively) 부여하는 것이고, 상기 다른 권한들은

상기 기존 권한들과는 다름-

를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 하나 이상의 추가 프린서펄을 지정하는 것은 하나 이상의 메인 프린서펄에 의해 수행되는 방법.

청구항 3

제1항에 있어서, 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 아이템들 각각의 데이터 속성을 조정하는 단계는, 상기 새로운 비중첩 보안 구역에 대응하는 보안 구역 열거로 상기 아이템들 각각에 라벨을 붙이는 단계를 포함하는 방법.

청구항 4

제1항에 있어서, 상기 권한들은 보안 권한들인 방법.

청구항 5

제1항에 있어서, 상기 권한들은 감사(auditing) 권한들인 방법.

청구항 6

컴퓨터 시스템에서 사용하기 위한 하나 이상의 컴퓨터 판독가능 저장 매체로서,

데이터 스토어 및 메소드 스토어가 상기 하나 이상의 컴퓨터 판독가능 저장 매체에 저장되어 있고, 상기 데이터 스토어 및 상기 메소드 스토어는 상기 컴퓨터 판독가능 저장 매체 상의 결합된 아이템 계층에 함께 배열되어 있고, 상기 데이터 스토어는 상기 메소드 스토어 내의 메소드에 의존하는 적어도 하나의 데이터 아이템을 갖고, 상기 메소드 스토어는 상기 데이터 스토어 내의 데이터에 의존하는 적어도 하나의 메소드를 가지며, 상기 결합된 아이템 계층은 하나 이상의 비중첩 보안 구역으로 나뉘어지며, 상기 하나 이상의 비중첩 보안 구역 각각은, 한 비중첩 보안 구역 내의 아이템들에 대한 관리 권한들을 갖는 프린서펄이 그 비중첩 보안 구역 내의 모든 아이템들을 공통 보안 규칙에 따라 균일하게 취급할 수 있도록, 공통 보안 규칙을 갖는 하나 이상의 메소드 아이템과 하나 이상의 데이터 아이템의 그룹으로서 정의되고,

상기 하나 이상의 컴퓨터 판독가능 저장 매체는, 프로세서에 의해 실행될 때 상기 컴퓨터 시스템으로 하여금, 프린서펄들에 대한 관리 권한들의 보다 효율적인 위임을 용이하게 하기 위하여, 상기 하나 이상의 비중첩 보안 구역을 복수의 비중첩 보안 구역으로 분할하는 방법을 수행하게 하는 컴퓨터 실행가능 명령어들을 또한 저장하고 있고,

상기 방법은,

상기 결합된 아이템 계층 내에서 새로운 공통 보안 규칙이 시행될 데이터 아이템들 및 메소드 아이템들의 그룹을 식별하는 단계 -상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹은 현재 상기 하나 이상의 비중첩 보안 구역들 중의 기존의 비중첩 보안 구역 내에 포함되어 있고, 기존의 공통 보안 규칙은 상기 기존의 비중첩 보안 구역 내에서 시행되며, 상기 기존의 공통 보안 규칙과는 다른 상기 새로운 공통 보안 규칙은 상기 기존의 비중첩 보안 구역 내에서 시행됨-;

전체 데이터베이스보다는 미세하지만 각 아이템에 대한 위임을 요구하지는 않을 정도로 거친 입도에서 관리 권한들이 위임될 수 있도록, 상기 하나 이상의 비중첩 보안 구역을 재구성하는 단계

-상기 재구성하는 단계는,

상기 기존의 비중첩 보안 구역을 새로운 비중첩 보안 구역 및 상기 기존의 비중첩 보안 구역의 나머지로 분할하는 단계 -상기 기존의 비중첩 보안 구역의 상기 나머지에 대한 상기 새로운 비중첩 보안 구역의 배열은 상기 결합된 아이템 계층 내에서의 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹의 위치에 기초하고, 상기 새로운 비중첩 보안 구역은 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹을 포함하고, 상기 기존의 비중첩 보안 구역의 상기 나머지는 상기 기존의 비중첩 보안 구역으로부터의 적어도 하나의 데이터 아이템 또는 메소드 아이템을 포함하고, 상기 분할하는 단계는 보안 구역들 간의 중첩을 방지하는 방식으로, 그리고 상기 데

이터 아이템들 및 메소드 아이템들 중 어느 것도 하나보다 많은 보안 구역에 포함되지 않도록 제한됨-, 및

상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹이 상기 새로운 비중첩 보안 구역 내에 포함됨을 표현하기 위하여, 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 아이템들 각각의 데이터 속성을 조정하는 단계

를 포함함- ;

상기 기존의 비중첩 보안 구역이 분할되었을 때 상기 기존의 비중첩 보안 구역에서 시행되고 있는 상기 기존의 공통 보안 규칙에 기초하여 상기 기존의 비중첩 보안 구역 내의 기존 관리 권한들을 가졌던 임의의 프린서펄에 대하여, 상기 기존의 비중첩 보안 구역을 분할하는 단계에 후속하여, 그리고 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹이 상기 새로운 비중첩 보안 구역에 포함됨을 표현하기 위하여 데이터 속성을 조정하는 단계에 후속하여, 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹을 포함하는 상기 새로운 비중첩 보안 구역 내에서 상기 임의의 프린서펄의 기존 관리 권한들을 유지시키는 단계; 및

상기 새로운 공통 보안 규칙에 따라 상기 새로운 비중첩 보안 구역 내의 다른 권한들을 하나 이상의 추가 프린서펄에게 부여하는 단계 -상기 다른 권한들을 상기 새로운 비중첩 보안 구역에 할당하는 것은, 상기 새로운 비중첩 보안 구역으로의 상기 다른 권한들의 부여를 통해 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 각각의 아이템에 상기 다른 권한들을 집합적으로 부여하는 것이고, 상기 다른 권한들은 상기 기존 권한들과는 다름-

를 포함하는 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 7

제1항에 있어서, 상기 기존의 공통 보안 규칙은 상기 기존의 비중첩 보안 구역의 상기 나머지 내의 아이템들에 대하여 프린서펄이 갖는 권한들을 정의하는 액세스 제어 리스트를 포함하는 방법.

청구항 8

제1항에 있어서, 상기 새로운 공통 보안 규칙은 상기 새로운 비중첩 보안 구역 내의 아이템들에 대하여 프린서펄이 갖는 권한들을 정의하는 액세스 제어 리스트를 포함하는 방법.

청구항 9

제6항에 있어서, 상기 하나 이상의 추가 프린서펄을 지정하는 것은 하나 이상의 메인 프린서펄에 의해 수행되는 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 10

제6항에 있어서, 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 아이템들 각각의 데이터 속성을 조정하는 단계는, 상기 새로운 비중첩 보안 구역에 대응하는 보안 구역 열거로 상기 아이템들 각각에 라벨을 붙이는 단계를 포함하는 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 11

제6항에 있어서, 상기 관리 권한들은 보안 권한들인 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 12

제6항에 있어서, 상기 관리 권한들은 감사 권한들인 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 13

제6항에 있어서, 상기 기존의 공통 보안 규칙은 상기 기존의 비중첩 보안 구역의 상기 나머지 내의 아이템들에 대하여 프린서펄이 갖는 권한들을 정의하는 액세스 제어 리스트를 포함하는 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 14

제6항에 있어서, 상기 새로운 공통 보안 규칙은 상기 새로운 비중첩 보안 구역 내의 아이템들에 대하여 프린서

펄이 갖는 권한들을 정의하는 액세스 제어 리스트를 포함하는 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 15

제1항에 있어서, 상기 새로운 공통 보안 규칙에 따라 상기 새로운 비중첩 보안 구역 내의 다른 권한들을 하나 이상의 추가 프린서펄에 부여하는 단계는, 상기 새로운 비중첩 보안 구역 내의 권한들의 세트의 부여를 통해 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 각 아이템에 대해 상기 권한들의 세트를 상기 하나 이상의 추가 프린서펄에 집합적으로 부여하도록 상기 새로운 비중첩 보안 구역 내의 상기 권한들의 세트를 상기 하나 이상의 추가 프린서펄에 부여하는 단계를 포함하고, 상기 권한들의 세트는 판독, 기입, 삭제 및 실행으로부터 선택된 하나 이상의 권한을 포함하는 방법.

청구항 16

제6항에 있어서, 상기 새로운 공통 보안 규칙에 따라 상기 새로운 비중첩 보안 구역 내의 다른 권한들을 하나 이상의 추가 프린서펄에 부여하는 단계는, 상기 새로운 비중첩 보안 구역 내의 권한들의 세트의 부여를 통해 상기 식별된 데이터 아이템들 및 메소드 아이템들의 그룹 내의 각 아이템에 대해 상기 권한들의 세트를 상기 하나 이상의 추가 프린서펄에 집합적으로 부여하도록 상기 새로운 비중첩 보안 구역 내의 상기 권한들의 세트를 상기 하나 이상의 추가 프린서펄에 부여하는 단계를 포함하고, 상기 권한들의 세트는 판독, 기입, 삭제 및 실행으로부터 선택된 하나 이상의 권한을 포함하는 하나 이상의 컴퓨터 판독가능 저장 매체.

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0015] 본 발명은 일반적으로 데이터 보안 분야에 관한 것이다. 보다 상세하게는, 본 발명은 데이터 아이템 그룹들에 대한 보안 관리에 관한 것이다.

[0016] 정보를 처리할 때, 그 정보의 특정 부분에 대한 액세스를 제한함으로써 그 특정 부분을 어떤 허가된 사용자만이 액세스할 수 있게 하는 것이 바람직한 경우가 종종 있다. 정보가 물리적 문서(예를 들어, 인쇄된 책 또는 장부)에 포함되어 있는 경우, 그 문서는 잠금 장치 및 문서 관리인 등의 물리적 접근 통제를 사용하여 보호될 수 있다. 그렇지만, 오늘날의 세계에서는, 대량의 정보가 디지털 데이터의 형태로 저장된다. 디지털 데이터는 생성, 수정, 복사, 전송 및 삭제가 용이하며, 그 결과 엄청나게 증대된 디지털 데이터가 수많은 장소에 존재하게 되었다. 물리적 문서와 유사하게, 디지털 데이터의 일부분에 대한 액세스를 제한하는 것이 바람직한 경우가 종종 있다. 그렇지만, 엄청난 양의 디지털 데이터 및 디지털 데이터의 생성, 복사, 전송, 수정 및 삭제의 용이성이 디지털 데이터의 보안을 어렵게 만들고 있다.

[0017] 기존의 2가지 통상적인 디지털 데이터 저장 유형은 파일 구조(file structure)와 데이터베이스이다. 파일 구조는 계층적 데이터 저장 시스템으로서, 디지털 데이터를 포함하는 파일들이 폴더에 저장된다. 폴더는 또한 다른 폴더에 저장될 수 있다. 파일 내의 디지털 데이터는 아이템별로 액세스된다. 환언하면, 파일에 액세스할 때, 그 파일 내에 무엇이 있는지 종종 알고 있으며, 그 파일에 대한 액세스는 그 파일 내의 디지털 데이터를 구체적으로 검토 또는 조작하기 위해 행해진다.

[0018] 반면에, 데이터베이스는 일반적으로 디지털 데이터를 물리적 테이블에 저장한다. 물리적 테이블은 일반적으로

어떤 논리적 그룹에 따라 구성되어 있다. 예를 들어, 데이터베이스 내의 물리적 테이블은 디지털 주소록을 포함할 수 있다. 디지털 주소록을 포함하는 테이블은 또한 그 테이블 내의 정보의 부류를 지정하는 컬럼을 가질 수 있다. 예를 들어, 디지털 주소록은 이름, 성, 전화 번호, 주소 등에 대한 컬럼을 포함할 수 있다.

[0019] 파일 시스템과 데이터베이스의 차이점으로 인해, 이들 2가지 디지털 데이터 저장 유형에서의 보안을 구현하는 방법도 서로 다르다. 예를 들어, 파일 구조에서는, 액세스 제어 리스트(access control list, ACL)가 각각의 파일에 할당될 수 있으며, 여기서 ACL은 각각의 사용자가 주어진 파일에 대해 어떤 퍼미션(permission) 또는 액세스 권한을 갖는지를 컴퓨터의 오퍼레이팅 시스템에 알려주는 데이터 구조이다. ACL은 특정의 사용자 또는 사용자 그룹이 판독, 기록 또는 실행 퍼미션 등의 어떤 권한을 갖는 것으로 지정할 수 있다. 파일 구조에서, ACL은 임의의 폴더 또는 그 폴더 내에 존재하는 파일이 잠재적으로 디폴트 값으로 ACL에 기술된 것과 동일한 보안 퍼미션을 갖도록 폴더에 할당될 수 있다. 그렇지만, 관리자는 특정 파일에 대한 액세스 요건에 기초하여 디폴트 보안 퍼미션을 변경할 수 있다. 따라서, 파일을 처리하라는 각각의 요청에 응답하여, 그 파일에 할당된 퍼미션을 결정하기 위해 그 파일에 대한 ACL에 액세스해야만 한다.

[0020] 파일에서 ACL을 사용하는 것의 한가지 단점은 파일 검색 등의 동작을 수행할 때 증가된 오버헤드가 부가된다는 것이다. 예를 들어, 사용자가 일정 유형의 파일 또는 일정 데이터를 포함하는 파일을 지정하는 검색을 작성하는 경우, 그 검색은 그 파일을 검색의 범위에 포함시키기 이전에 사용자가 그 파일에 대해 가지고 있는 보안 퍼미션을 결정하기 위해 먼저 각각의 파일에 대한 ACL을 검사해야만 한다. 예를 들어, 사용자가 액세스조차 할 수 없는 파일의 존재를 누설하는 것은 부적절할 수 있다. 폴더 내의 파일에 대한 디폴트 퍼미션이 변경될 수 있기 때문에, 폴더 레벨 ACL이 잠재적으로 다수의 파일로 하여금 디폴트 값으로 동일한 보안 퍼미션을 갖도록 하는 경우조차도 각각의 파일에 대한 ACL이 검사되어야만 한다.

[0021] 이와 반대로, 데이터베이스 시스템에서의 보안은 ACL을 전체 컬럼에 할당함으로써 행해진다. ACL을 전체 컬럼에 할당하게 되면 단 하나의 ACL에 액세스하여 전체 컬럼의 데이터에 대한 보안 퍼미션을 결정할 수 있기 때문에 보다 효율적으로 검색이 수행될 수 있게 된다. 데이터베이스는 사용자가 컬럼에 액세스하기 위해 적절한 보안 퍼미션을 갖는 경우에 검색이 컬럼에 대해서만 수행될 수 있도록 구성될 수 있다. 따라서, 테이블 내의 각 요소에 대한 퍼미션을 검사할 필요가 없다. 컬럼 기반의 보안 퍼미션 할당의 한가지 단점은 어떤 응용에서 그 입도(granularity)가 너무 거칠 수 있다(too coarse)는 것이다. 예를 들어, 디지털 주소록 엔트리를 나타내는 컬럼 내의 디지털 데이터의 대부분이 일반적인 액세스에 적합할 수 있지만, 사회 보장 번호 또는 다른 유형의 민감한 정보 등의 일부 디지털 데이터에 대한 액세스를 제한하는 것이 바람직할 수 있다. 그렇지만, ACL이 전체 컬럼에 할당되는 경우, 그 컬럼 내의 서로 다른 아이템들 사이에서 보안 퍼미션이 변할 수 없다. 따라서, 주소 및 전화 번호에 대한 액세스도 마찬가지로 제한하지 않고서는 사회 보장 번호에 대한 액세스를 제한하는 방법이 없을 수 있다.

[0022] 따라서, 구성가능한 입도로 ACL이 할당될 수 있게 해주는 보안 시스템이 있으면 유익할 것이다.

발명이 이루고자 하는 기술적 과제

[0023] 본 발명의 측면은 데이터 아이템의 구역 기반 보안 관리에 관한 것이다. 본 발명의 일 실시예에서, 컴퓨터 시스템은 아이템의 적어도 일부분에 대한 권한을 결정한다. 컴퓨터 시스템은 다수의 아이템(item)을 저장하는 볼륨(volume)을 포함하며, 이 볼륨은 적어도 하나의 보안 구역(security zone)으로 분할된다. 컴퓨터 시스템에 저장되어 있는 각각의 아이템은 단 하나의 보안 구역에 존재한다. 각각의 아이템이 단 하나의 보안 구역에 존재하기 때문에, 그 아이템의 보안을 제어하기 위한 규칙들이 생성될 수 있으며, 여기서 이 규칙들은 각각의 개별적인 아이템에 대해 지정될 필요가 없고 그 대신에 그 구역의 서브셋에 적용될 수 있다. 컴퓨터 시스템은 프린서펄(principal)의 신원이 검증되었음을 나타내는 인증 정보에 액세스한다.

[0024] 컴퓨터 시스템은 또한 상기 볼륨의 보안 구역에 대한 보안 규칙(security rule)에 액세스한다. 보안 규칙은 프린서펄 또는 프린서펄 그룹이 아이템들에 대해 갖는 권한을 지정한다. 보안 규칙은 요소 인자, 프린서펄 인자, 및 권한 인자를 포함한다. 요소 인자(element argument)는 예를 들어 요소 경로(element path)를 통해 그에 대한 권한을 부여받은 아이템의 적어도 일부분을 지정한다. 요소 경로를 통해 아이템의 적어도 일부분을 지정하는 것은 데이터 스토어 내의 모든 개별적인 셀(또는 정보)에 대한 규칙을 만들 필요가 없도록 적절한 입도의 규칙 정의를 가능하게 해주는 데 유용하다. 프린서펄 인자(principal argument)는 적어도 하나의 프린서펄을 지정할 수 있다. 적어도 하나의 프린서펄은 아이템의 적어도 일부분에 대한 보안 권한을 부여받는 엔티티이다. 컴퓨터 시스템은 액세스된 보안 규칙에 기초하여 아이템의 적어도 일부분에 대한 검증된 프린서펄의 권한을 식

별한다.

[0025] 본 발명의 다른 실시예에서, 컴퓨터 시스템은 관리 권한을 프린서펄에 위임한다. 컴퓨터 시스템은 다수의 아이템을 저장하는 볼륨을 포함하며, 이 볼륨은 적어도 하나의 비중첩 구역으로 분할된다. 각각의 아이템은 적어도 하나의 비중첩 구역 중의 한 구역에 존재한다. 각각의 아이템이 한 구역에 존재함으로써, 관리 권한은 전체 데이터베이스 테이블보다 더 세밀하지만 각각의 아이템에 대한 위임을 요구하지 않을 정도로 충분히 거친 적절한 입도로 위임될 수 있다. 구역들 각각은 관리 권한을 갖는 하나 이상의 프린서펄을 갖는다. 컴퓨터 시스템은 메인 구역(main zone) 내의 제1 아이템들을 식별한다.

[0026] 이들 제1 아이템은 그에 대한 관리 권한이 위임되어야 하는 아이템이다. 컴퓨터 시스템은 메인 구역을 예를 들어 2개의 구역, 즉 제1 구역과 나머지 메인 구역으로 분할한다. 관리 권한을 갖는 하나 이상의 프린서펄은 나머지 메인 구역 및 제1 구역 둘다에 대한 관리 권한을 보유한다. 제1 구역은 이전에 식별된 제1 아이템을 포함한다. 나머지 메인 구역은 제1 구역에 있는 아이템을 제외하고 메인 구역에 있었던 아이템을 포함한다. 컴퓨터 시스템은 하나 이상의 제1 프린서펄도 제1 아이템에 대한 관리 권한을 갖는 것으로 지정한다.

[0027] 본 발명의 부가의 특징 및 이점이 이하의 설명에 기술되어 있으며, 부분적으로는 그 설명으로부터 명백하게 되거나 또는 본 발명의 실시에 의해 알게 될 수 있다. 본 발명의 특징 및 이점은 첨부된 청구항에 구체적으로 기재된 수단 및 조합에 의해 실현 및 달성될 수 있다. 본 발명의 이들 특징 및 다른 특징은 이하의 설명 및 첨부된 청구항으로부터 보다 명백하게 되거나 또는 이후에 기술되는 바와 같은 본 발명의 실시에 의해 알 수 있다.

발명의 구성 및 작용

[0028] 본 발명의 전술한 이점 및 특징과 그 밖의 이점 및 특징이 달성될 수 있는 방법에 대해 기술하기 위해, 간략히 전술한 본 발명에 대한 보다 상세한 설명이 첨부 도면에 예시되어 있는 본 발명의 구체적인 실시예를 참조하여 이루어질 것이다. 이들 도면이 본 발명의 전형적인 실시예들만을 도시하고 있으며 따라서 본 발명의 범위를 제한하는 것으로 간주해서는 안됨을 염두에 두면서, 첨부 도면을 사용하여 본 발명에 대해 보다 구체적이고 상세하게 기술 및 설명할 것이다.

[0029] 본 발명의 범위는 데이터 아이템에 대한 구역 기반 보안 관리(zone based security administration)를 위한 방법, 시스템, 및 컴퓨터 프로그램 제품까지 미친다. 일 실시예에서, 컴퓨터 시스템은 보안 구역(security zone)에 포함된 데이터 아이템의 적어도 일부분에 대한 보안 권한(security right)을 결정한다. 데이터 항목의 그 일부분은 보안 규칙(security rule)이 셀 레벨(cell level)에서 적용될 필요가 없도록 요소 경로(element path)를 통해 지정된다. 본 발명의 또다른 실시예에서, 컴퓨터 시스템은 관리 권한(즉, 데이터 아이템의 적어도 일부분에 대한 보안을 변경하는 기능)을 프린서펄에 위임한다. 각각의 아이템은 적어도 하나의 비중첩 구역 중의 한 구역에 존재한다. 각각의 아이템이 한 구역에 있기 때문에, 관리 권한은 전체 데이터베이스 테이블보다 미세하지만 각각의 아이템에 대한 위임을 필요로 하지 않도록 아직은 충분히 거친 적절한 입도로 위임될 수 있다.

[0030] 이제 도 1을 참조하면, 본 발명의 측면들이 실시될 수 있는 예시적인 환경이 도시되어 있다. 도 1은 네트워크 아키텍처(100)를 도시한 것이다. 네트워크 아키텍처(100)는 여러가지 데이터 아이템 및/또는 컴퓨터 실행가능 명령어(예를 들어, 메소드)를 저장할 수 있는 스토리지(storage)(102)를 포함한다. 스토리지(102)는 이하의 도 6의 설명에서 기술하는 것을 포함한 다수의 여러가지 저장 매체로 구현될 수 있지만, 이에 한정되는 것은 아니다. 스토리지(102)는 데이터 아이템을 계층적 포맷으로 저장할 수 있는 데이터 스토어(data store)(104)를 포함한다. 예를 들어, 아이템(106)은 하나 이상의 요소(108)를 포함할 수 있다. 데이터 요소는 데이터 요소(108)에 의존하는 속성(110)으로 추가로 세분될 수 있다. 계층적 포맷에서, 데이터 아이템은 상위 레벨 데이터 아이템에 대한 요소 또는 속성일 수 있다.

[0031] 스토리지(102)는 계층적 포맷으로 배열된 메소드를 저장할 수 있는 메소드 스토어(method store)(112)를 더 포함한다. 메소드 아이템(114)은 메소드일 수 있는 요소(116)를 포함한다. 이 요소는 하위 레벨 메소드[예를 들어, 메소드(118)]를 더 포함할 수 있다. 하위 레벨 메소드(118)는 그 자체가 다른 서브 메소드를 마음대로 이용할 수 있는 메소드일 수 있다. 메소드 스토어(112) 및 데이터 스토어(104)가 개별적인 스토어로서 도시되어 있지만, 메소드 스토어(112)와 데이터 스토어(104)는 동일한 계층 구조 내에 함께 배열되어 있을 수 있다. 따라서, 데이터 아이템이 그 자신에 의존하는 메소드를 가질 수 있거나 메소드가 그 자신에 의존하는 데이터 아이템 속성을 가질 수 있다.

[0032] 본 발명의 일 실시예에서, 네트워크 아키텍처(100)는 여러가지 기능을 수행하기 위한 컴퓨터 실행가능 코드인

애플리케이션(122)을 포함한다. 애플리케이션(122)은 통신 채널(124)을 통해 스토리지(102)에 연결되어 있다. 통신 채널(124)은 스크롤(127)과 함께 도시되어 있으며, 여기서 스크롤(127)은 애플리케이션(122)과 스토리지(102) 사이에서 전달될 수 있는 데이터 아이템, 데이터 요소, 데이터 속성, 메소드 아이템, 및 메소드를 나타낸다. 또하나의 통신 채널(126)이 토큰(128) 등의 토큰을 애플리케이션으로부터 인증 모듈(146)로 전송하기 위해 존재한다.

[0033] 토큰(128)은 인증 모듈(146)이 그 토큰을 제공하는 프린서펄의 신원을 결정할 수 있게 해주는 정보를 열거하고 있다. 예를 들어, 본 일례에서, 토큰(128)은 프린서펄, 즉 애플리케이션(122)을 식별해주는 정보를 포함하고 있다. 프린서펄의 신원을 검증하는 프로세스는 종종 인증이라고 한다. 인증 모듈(146)은 토큰과 비교하기 위해 인증 정보의 데이터베이스에 액세스할 수 있다. 본 발명의 일 실시예에서, 이 인증 데이터베이스는 스토리지(102)에 저장되어 있다. 프린서펄이 일단 인증되면, 액세스 제어 리스트(ACL)를 조회하여 그 프린서펄에 대해 지정되어 있는 권한을 검사함으로써 프린서펄에 대한 권한이 결정될 수 있다.

[0034] 스토리지(102)는 프린서펄이 스토리지(102) 내의 아이템에 대해 어떤 권한을 가지고 있는지를 결정하는 데 사용되는 하나 이상의 ACL(130)을 더 포함한다. 일반적으로, ACL은 프린서펄 인자, 권리 인자 및 아이템 인자를 포함한 3개의 인자(argument)를 가지고 있다. 이들 3개의 인자는 함께 어떤 프린서펄이 어떤 아이템에 대해 어떤 권한을 가지고 있는지를 지정한다. 인증된 토큰(128)을 사용하여, 애플리케이션(122)이 데이터 스토어(104) 내의 아이템에 액세스하거나 메소드 스토어(112) 내의 메소드를 실행할 권한을 갖는 것으로 결정될 수 있다. 본 일례에서는 단 하나의 ACL이 도시되어 있지만, 본 발명의 실시예들에서 ACL은 다수의 보안 규칙을 나타내며 각각의 보안 규칙이 아이템에 대한 권한을 프린서펄에 부여함을 이해해야 한다.

[0035] 본 발명의 일 실시예에서, 부여될 수 있는 4가지 권한은 판독(read), 기록(write), 삭제(delete) 및 실행(execute)이다. 판독, 기록 및 삭제 권한은 부여되면 프린서펄이 데이터 아이템(106) 등의 데이터 아이템 또는 요소(108) 등의 요소 또는 속성(110) 등의 속성을 각각 검토, 조작 및 삭제할 수 있게 해준다. 실행 권한은 부여되면 애플리케이션(122) 등의 프린서펄이 메소드(118) 등의 메소드를 호출할 수 있게 해준다.

[0036] 네트워크 아키텍처(100)는 사용자 인터페이스(132)를 더 포함할 수 있다. 사용자 인터페이스(132)는 컴퓨터 사용자(134)가 네트워크 아키텍처(100)와 상호 작용할 수 있게 해준다. 사용자 인터페이스(132)는 통신 경로(136)를 통해 스토리지(102)와 연결되어 있다. 네트워크 아키텍처(100)에 도시된 또다른 통신 경로는 토큰(140) 및 질의 또는 요청(142)을 컴퓨터 사용자(134)로부터 사용자 인터페이스(132)로 전송하는 데 사용되는 경로(138)이다. 존재하는 또다른 통신 경로는 통신 경로(144)이며, 이를 통해 데이터 아이템, 요소 및 속성이 컴퓨터 사용자(134)와 사용자 인터페이스(132) 사이에서 전송될 수 있다. 사용자 인터페이스(132)는 통신 경로(136)를 통해 스토리지(102)로의 데이터 아이템, 요소 및 속성의 전송과, 스토리지로부터의 데이터 아이템, 요소 및 속성의 전송을 용이하게 해준다.

[0037] 본 발명의 일 실시예에서, 컴퓨터 사용자(134)가 데이터 스토어(104) 내의 데이터 아이템에 액세스하거나 메소드 스토어(112) 내의 메소드를 실행하기 위해, 컴퓨터 사용자(134)는 데이터 아이템에 액세스하거나 메소드를 실행하기 위해 허가를 받아야만 한다. 이를 용이하게 하기 위해, 컴퓨터 사용자(134)에 의해 토큰(140)이 통신 경로(138)를 통해 사용자 인터페이스(132)로 전송된다. 사용자 인터페이스(132)는 토큰(140)을 통신 경로(126)를 통해 인증 모듈(146)로 보낸다. 이어서, 인증 모듈(146)은 컴퓨터 사용자(134)의 신원을 검증한다. ACL(130) 등의 ACL은 컴퓨터 사용자(134)가 데이터 스토어(104) 내의 데이터 아이템 및 메소드 스토어(112) 내의 메소드에 대해 갖는 권한을 결정한다.

[0038] 본 발명의 일 실시예에서, ACL(130)은 데이터 스토어(104) 및 메소드 스토어(112) 내의 아이템에 대한 관리 권한을 갖는 관리 프린서펄에 의해 생성될 수 있다. 관리 프린서펄은 관리 권한을 갖는 복수의 프린서펄 중 하나일 수 있다. 본 발명의 일 실시예에서, 관리 권한을 갖는 복수의 프린서펄은 이하에 보다 상세히 설명하는 보안 구역에 존재하는 모든 아이템에 대해 동일하다.

[0039] 도 1은 네트워크 아키텍처(100)를 도시하고 있지만, 본 발명의 실시예들은 분산 컴퓨팅 환경, 도 6에 도시되고 기술된 것과 같은 단일 컴퓨터 시스템, 또는 각종의 다른 적당한 시스템을 비롯한 다수의 여러가지 아키텍처에서 구현될 수 있음을 이해해야 한다.

[0040] 보안 구역의 개념은 도 2 및 도 3을 살펴봄으로써 보다 확실히 이해될 수 있다. 도 2는 스토리지(102) 등의 스토리지에서의 아이템들의 계층적 레이아웃을 도시한 것이다. 도 2에 도시된 일례에서, 아이템들은 볼륨(202) 내에 도시되어 있다. 전술한 바와 같이, 볼륨(202)은 도 6에 도시하고 기술된 것들 등의 임의의 적당한 저장

장소에 존재할 수 있다. 볼륨(202)은 스토리지(102) 내의 모든 아이템들 전부를 포함한다. 일례에서, 전체 볼륨(202)은 단 하나의 구역을 포함할 수 있다. 따라서, 복수의 프린서펄이 구역/볼륨(202) 내의 모든 아이템들에 대한 관리 권한, 즉 그에 대한 보안을 변경하는 기능을 갖는다. 본 발명의 다른 실시예들에서는, 도 3에 도시한 바와 같이, 볼륨은 구역(302) 및 구역(304) 등의 다수의 구역으로 분리되어 있다. 각각의 구역은 관리 권한을 갖는 여러가지 복수의 프린서펄을 가질 수 있다. 따라서, 볼륨(202)을 구역(302) 및 구역(304)으로 분할함으로써, 관리 권한이 다른 프린서펄로 위임될 수 있다.

[0041] 이제, 도 4를 참조하면, 권한을 다른 프린서펄로 위임하는 방법이 방법 400에 도시되어 있다. 본 발명의 일 실시예에서, 방법 400은 도 1의 네트워크 아키텍처(100) 등의 컴퓨터 시스템에서 실시되며, 여기서 데이터 아이템(106) 및 메소드 아이템(114) 등의 아이템은 도 2에 도시한 볼륨(202) 등의 볼륨에 저장되어 있다. 볼륨은 구역(302) 및 구역(304) 등의 적어도 하나의 비중첩 구역으로 분할된다. 방법 400은 각각의 아이템이 적어도 하나의 비중첩 구역 중의 한 구역에 존재하는 것도 생각하고 있다. 각각의 구역은 하나 이상의 관리 프린서펄을 갖는다. 관리 프린서펄은 자신이 속해 있는 특정의 구역에 대한 보안 및/또는 감사를 관리한다. 방법 400은 적어도 하나의 비중첩 구역에 포함되어 있는 구역에 포함된 제1 아이템에 대한 관리 권한을 다른 프린서펄에 위임하는 것과 관련하여 구성되어 있다.

[0042] 방법 400은 제1 구역을 형성하는 기능 결과 지향적 단계(단계 408)를 포함한다. 단계 408은 제1 구역을 형성하는 임의의 대응 동작들을 포함할 수 있다. 그렇지만, 도 4의 예시적인 방법에서, 단계 408은 메인 구역 내의 제1 아이템을 식별하는 대응 동작(동작 402)을 포함한다. 동작 402는 컴퓨터 시스템이 메인 구역 내의 제1 아이템을 식별하는 동작을 포함할 수 있다. 예를 들어, 네트워크 아키텍처(100) 내의 컴퓨터 시스템은 볼륨(202)으로부터의 아이템을 식별할 수 있다. 식별된 제1 아이템은 그 구역의 관리 프린서펄 중 하나 이상이 그에 대한 관리 권한을 위임하고자 하는 아이템일 수 있다.

[0043] 단계 408은 메인 구역을 제1 구역과 나머지 메인 구역으로 분할하는 대응 동작(동작 404)을 더 포함한다. 동작 404는 컴퓨터 시스템이 메인 구역을 제1 구역과 나머지 메인 구역으로 분할하는 동작을 포함할 수 있다. 예를 들어, 네트워크 아키텍처(100) 내의 컴퓨터 시스템은 볼륨(202)을 구역(302) 및 구역(304)으로 분할할 수 있다. 2개의 구역이 동작 404로부터 형성되는 동안, 하나 이상의 메인 프린서펄이 제1 구역과 나머지 메인 구역 둘다에 대한 관리 권한을 보유한다.

[0044] 메인 구역의 분할이 제1 아이템을 제1 구역에 위치시키는 반면, 나머지 메인 구역은 처음에 메인 구역에 있었지만 제1 아이템에 포함되지 않는 그 부분의 아이템을 포함한다. 분할의 일례가 도 3에 도시되어 있다. 예를 들어, 메인 구역은 볼륨(202)일 수 있다. 분할은 구역(302)과 구역(304)이 생기게 한다. 볼륨은 처음에 아이템(306 내지 328)을 포함하고 있었지만, 분할이 아이템(324 내지 328)을 하나의 구역(즉, 제1 구역)에 있게 하고 아이템(306 내지 322)을 또하나의 구역(즉, 나머지 메인 구역)에 있도록 만든다. 이 때, 구역(302, 304)의 관리 프린서펄은 동일하다.

[0045] 방법 400은 하나 이상의 제1 프린서펄이 또한 제1 아이템에 대한 관리 권한을 갖는 것으로 지정하는 동작(동작 406)을 더 포함한다. 동작 406은 컴퓨터 시스템이 하나 이상의 제2 프린서펄이 또한 제1 아이템에 대한 관리 권한을 갖는 것으로 지정하는 동작을 포함할 수 있다. 예를 들어, 네트워크 아키텍처(100) 내의 컴퓨터 시스템은 하나 이상의 제1 프린서펄이 구역(302) 내의 아이템들에 대한 관리 권한을 갖는 것으로 지정할 수 있다.

[0046] 동작 406은 관리 권한을 하나 이상의 부가의 프린서펄에 양도함으로써 달성될 수 있다. 따라서, 메인 프린서펄 및 하나 이상의 부가의 프린서펄 모두는 그 구역의 아이템들에 대한 관리 권한을 갖는다. 예를 들어, 구역(302)이 제1 구역인 경우, 하나 이상의 메인 프린서펄 및 하나 이상의 제1 프린서펄 모두는 구역(302) 내의 아이템들에 대한 관리 권한을 갖는다. 관리 권한은 보안 권한 또는 감사 권한 중 어느 하나일 수 있다.

[0047] 방법 400은 또한 하나 이상의 제1 프린서펄이 하나 이상의 메인 프린서펄에 의해 변경가능하도록 되어 있을 수 있다. 즉, 메인 프린서펄의 어느 것이라도 하나 이상의 제1 프린서펄에 프린서펄을 부가하거나 하나 이상의 제1 프린서펄로부터 프린서펄을 제거할 수 있다.

[0048] 방법 400은 또한 제1 구역 내의 아이템들에 제1 구역에 대응하는 구역 열거(zone enumeration)로 라벨을 붙이는 단계를 포함할 수 있다. 예를 들어, 도 3에 도시한 바와 같이, 구역(302) 내의 아이템들에는 구역 열거(330)로 라벨이 붙여져 있다. 구역 열거(330)는 어느 아이템이 어느 구역에 존재하는지를 추적하는 데 유용하다. 메인 구역이 분할되어 있는 경우, 나머지 메인 구역 및 제1 구역은 이 2개의 구역이 어떤 중첩 아이템도 갖지 않도록 하기 위해 검사된다. 구역이 분할되는 경우 그 구역들이 비중첩인지를 검사하는 한, 제1 구역 및 나머지 메인

구역과 중첩 아이템이 있는지 다른 구역을 검사할 필요가 없다. 구역 열거는 또한 아이템들 간에 새로운 관계가 부가되는 경우 중첩이 없도록 하는 데 유용하다. 예를 들어, 아이템이 다른 아이템과 연관되는 경우, 모든 연관된 아이템은 동일 구역에 있어야만 한다. 이것은 구역 열거를 조회함으로써 달성될 수 있다.

[0049] 도 1에 도시한 ACL에 저장되어 있는 것과 같은 보안 규칙은 구역(302) 등의 제1 구역이 생성된 후에 그 제1 구역에 부가될 수 있다. 본 발명의 일 실시예에서, 제1 구역은 이전에 메인 구역에 있었던 임의의 보안 규칙을 자동적으로 포함한다. 본 발명의 다른 실시예들에서, 제1 구역은 생성된 이후에 어떤 보안 규칙도 포함하지 않으며 모든 새로운 보안 규칙이 그 제1 구역에 대해 생성되어야만 한다.

[0050] 구역은 또한 재결합될 수 있다. 구역은 이 구역이 생성된 때에 생성된 다른 구역과 재결합되거나 또는 이 구역이 생성된 때에 생성된 다른 구역으로부터 언젠가 생성되는 구역과 결합되어야만 한다. 나머지 메인 구역이 제2 구역을 형성하기 위해 분할된 이후에 그 구역이 재결합되는 경우 한가지 문제가 발생한다. 예를 들어, 도 3에서 아이템(320)을 제2 구역으로 그룹화하는 반면 아이템(308 내지 318 및 322)은 그 후의 나머지 메인 구역에 있도록 하기 위해 분할선(332)에 의해 나타낸 바와 같이 분할이 행해진다. 그럼에도 불구하고, 제1 구역과 그 후의 나머지 메인 구역을 재결합함으로써 새로운 구역이 생성될 수 있다. 이 경우, 그 후의 나머지 메인 구역은 그의 관리 프린서펄로서 메인 구역에 대한 최초의 프린서펄을 갖는 구역이다. 재결합된 구역은 그의 프린서펄로서 메인 구역에 대한 최초의 프린서펄을 갖는다.

[0051] 구역이 재결합될 때, 양쪽 구역의 보안 규칙은 그대로 유지된다. 또한, 새로 생성된 구역에서 다른 보안 규칙들이 정의될 수 있다.

[0052] 이제 도 5를 참조하면, 본 발명의 측면을 사용하여 보안 권한을 결정하는 방법이 방법 500으로서 도시되어 있다. 방법 500은 도 1에 도시된 네트워크 아키텍처(100) 등의 컴퓨터 시스템에서 실시될 수 있다. 컴퓨터 시스템은 데이터 아이템(106) 및 메소드 아이템(114) 등의 아이템을 포함한다. 이 아이템은 도 2에 도시한 볼륨(202) 등의 컴퓨터 시스템 상의 볼륨 내에 존재한다. 이 볼륨은 적어도 하나의 보안 구역으로 분할된다. 각각의 아이템은 하나의 보안 구역 내에 존재한다. 이의 일례가 도 3에 도시되어 있다. 구역(302) 내의 아이템[아이템(324 내지 326)]의 어느 것도 구역(304) 내에 존재하지 않는다. 게다가, 구역(304) 내의 아이템[아이템(306 내지 322)]의 어느 것도 구역(302)에 존재하지 않는다.

[0053] 방법 500은 프린서펄의 신원이 검증되었음을 나타내는 인증 정보에 액세스하는 동작(동작 502)을 포함한다. 동작 502는 컴퓨터 시스템이 프린서펄의 신원이 검증되었음을 나타내는 인증 정보에 액세스하는 동작을 포함할 수 있다. 예를 들어, 네트워크 아키텍처(100) 내의 컴퓨터 시스템은 인증 모듈(146)에 의해 제공된 인증 정보 또는 캐쉬(120)에 저장된 인증 정보에 액세스할 수 있다. 본 발명의 일 실시예에서, 동작 502는 도 1에 도시한 인증 모듈 등의 인증 모듈(146)에 의해 수행된다.

[0054] 인증 모듈은 토큰(128) 또는 토큰(140) 등의 토큰을 프린서펄로부터 수신할 수 있다. 이어서 인증 모듈은 프린서펄의 신원을 검증하기 위해 토큰 내의 정보를 인증 모듈(146)이 이용가능한 정보와 비교한다. 이 정보는 인증 정보를 포함하는 데이터베이스에서 입수할 수 있다. 패스워드, 암호화된 문자열, 스마트 카드 등의 물리적 키, 지문 등의 생체 키, 음성 분석 등과 같은 몇가지 서로 다른 유형의 토큰이 존재한다. 사용될 수 있는 2가지 특정의 토큰은 윈도즈 토큰(windows token) 및 인증된 XrML 라이센스 세트이다. 동작 502는 또한 도 1에 도시한 캐쉬(120) 내의 엔트리 등의 캐쉬 엔트리를 조회함으로써 수행될 수 있다. 구체적으로 말하면, 본 발명의 일 실시예에서, 토큰이 인증 모듈(146)에 의해 일단 인증되었으면, 동일 세션에서의 프린서펄의 차후의 인증이 이제 캐쉬 내의 엔트리를 조회함으로써 행해질 수 있도록 정보가 캐쉬(120)에 위치될 수 있다.

[0055] 방법 500은 보안 규칙에 액세스하는 동작(동작 504)을 포함한다. 예를 들어, 네트워크 아키텍처(100) 내의 컴퓨터 시스템은 ACL(130)로부터의 보안 규칙에 액세스할 수 있다. 보안 규칙은 보안 구역에 대해 존재한다. 본 발명의 일례에서 보안 규칙은 도 1에 도시한 ACL(130)로서 구현될 수 있다. 보안 규칙은 3가지 인자, 즉 요소 인자, 프린서펄 인자, 및 권한 인자를 가질 수 있다. 요소 인자는 요소 경로를 통해 아이템의 적어도 일부분을 지정한다.

[0056] 예를 들어, 보안 규칙이 도 3의 아이템(312)에 대한 권한을 부여한 경우, 요소 인자는 306.308.312 등의 아이템(312)으로의 경로를 지정한다. 이 경로는 최상위 아이템, 즉 아이템(306), 아이템(306)에 의존하는 아이템, 즉 아이템(308), 및 마지막으로 보안이 적용되는 아이템, 즉 아이템(308)에 의존하는 아이템(312)을 포함한다. 본 발명의 또다른 실시예에서, 보안 규칙은 복수의 속성을 포함하는 복합 요소(complex element)인 요소를 지정할 수 있다. 이 경우, 그 요소의 모든 속성에 대한 액세스가 허용될 수 있다. 예를 들어, 요소 경로가 306.310인

경우, 프린서펄은 요소(310)는 물론 요소(316 내지 322)를 비롯한 요소(310)에 의존하는 모든 요소에 대한 권한을 갖는다.

[0057] 게다가, 보안 규칙은 프린서펄이 어떤 유형의 요소에만 액세스하는 것으로 규정할 수 있다. 예를 들어, 복합 요소는 몇가지 서로 다른 속성을 갖는 것이다. 복합 요소의 한가지 구체적인 일례가 디지털 주소록에서의 유형 이름의 요소이다. 유형 이름의 요소는 이름(first name), 성(last name) 및 중간 이름(middle name) 속성을 포함할 수 있다. 사용자가 다른 요소 뿐만 아니라 유형 이름 요소를 포함하는 아이템에 대한 권한을 부여받으면, 그 사용자는 보안 규칙에 유형 이름을 규정함으로써 그 유형 이름 요소로만 제한될 수 있다.

[0058] 보안 규칙은 데이터 아이템의 적어도 일부분으로부터 적어도 하나의 요소를 배제시키는 거부 액세스 제어 엔트리(ACE)(deny access control entry)를 더 포함할 수 있다. 예를 들어, 규칙은 아이템(310)에 대한 권한을 갖는 것으로 규정할 수 있다. 전술한 바와 같이, 아이템(310)만이 지정되어 있는 경우, 프린서펄은 아이템(316, 318, 320, 322)에 대한 권한을 갖는다. 그렇지만, 규칙은 거부 ACE를 사용하여 프린서펄이 아이템(320)을 배제한 아이템(310)에 대한 권한을 갖는 것으로 규정할 수 있다.

[0059] 보안 규칙은 보안 권한을 갖는 프린서펄을 지정하는 프린서펄 인자를 포함한다. 본 발명의 일 실시예에서, 프린서펄은 도 1에 도시한 컴퓨터 사용자(134) 등의 컴퓨터 사용자이다. 본 발명의 또다른 실시예에서, 프린서펄은 네트워크 아키텍처(100) 상에서 실행되는 애플리케이션(122)과 같은 컴퓨터 시스템 상에서 실행되는 애플리케이션일 수 있다. 프린서펄 인자는 권한을 부여받을 수 있는 일단의 프린서펄을 지정할 수 있다. 예를 들어, 프린서펄 인자는 모든 네트워크 관리자를 포함할 수 있다. 보안 규칙은 또한 거부 ACE를 포함할 수 있으며, 이 경우 거부 ACE는 일단의 프린서펄로부터 적어도 하나의 프린서펄을 제외시킨다.

[0060] 예를 들어, 규칙이 모든 네트워크 관리자를 포함하는 반면 특정의 관리자를 배제시키는 일단의 프린서펄을 지정할 수 있다. 거부 ACE에 의해 배제된 특정의 네트워크 관리자가, 다른 보안 규칙에서, 네트워크 관리자가 배제되었던 보안 규칙에서의 것과 동일한 권한을 부여받은 경우, 그 네트워크 관리자는 지정된 보안 권한을 갖게 된다. 예를 들어, 한 보안 규칙이 X를 제외한 모든 관리자가 아이템 Y에 대한 권한을 갖는 것으로 규정하고 제2 보안 규칙이 관리자 X가 아이템 Y에 대한 권한을 갖는 것으로 규정하는 경우, 관리자 X는 아이템 Y에 대한 권한을 갖는다. 관리자 X의 아이템 Y에 대한 권한을 제거하기 위해, 아이템 Y에 대한 권한을 부여하는 모든 규칙에서 관리자 X를 배제시키기 위해 거부 ACE가 사용될 수 있다. 본 발명의 일 실시예에서의 보안 규칙은 권한이 부여될 수 있음을 의미하는 권한 부여(grant)이다. 거부 규칙을 생성함으로써 프린서펄로부터 권한을 빼앗아갈 수 없으며, 오히려 프린서펄로부터 어떤 권한을 박탈시키기 위해서는 권한 부여 규칙 모두가 수정 또는 제거되어야만 한다.

[0061] 보안 규칙은 또한 권한 인자를 포함할 수 있다. 본 발명의 여러가지 실시예들은 판독, 기록, 삭제 및 실행 권한을 비롯한 권한을 고려하고 있다. 판독 권한이 아이템에 대한 프린서펄에 부여되는 경우, 그 권한은 일반적으로 프린서펄이 볼 수는 있지만 변경 또는 삭제할 수는 없는 데이터 아이템과 관련되어 있다. 기록 권한이 아이템에 대한 프린서펄에 부여되는 경우, 그 권한은 일반적으로 프린서펄이 볼 수 있고 편집할 수는 있지만 삭제할 수는 없는 데이터 아이템과 관련되어 있다. 삭제 권한이 아이템에 대한 프린서펄에 부여되는 경우, 그 권한은 일반적으로 프린서펄이 볼 수 있고, 편집할 수 있으며 삭제할 수 있는 데이터 아이템과 관련되어 있다. 실행 권한이 아이템에 부여되어 있는 경우, 그 권한은 일반적으로 프린서펄이 실행되도록 할 수 있는 메소드 아이템과 관련되어 있다.

[0062] 방법 500은 액세스된 보안 규칙에 근거하여 아이템의 적어도 일부분에 대한 검증된 프린서펄의 권한을 식별하는 동작(동작 506)을 포함한다. 동작 506은 컴퓨터 시스템이 액세스된 보안 규칙에 근거하여 아이템의 적어도 일부분에 대한 검증된 프린서펄의 권한을 식별하는 동작을 포함할 수 있다. 예를 들어, 네트워크 아키텍처(100) 내의 컴퓨터 시스템은 ACL(130)로부터 액세스된 보안 규칙에 기초하여 아이템(324)에 대한 검증된 프린서펄의 권한을 식별할 수 있다. 이와 같이, 본 발명의 일 실시예에서, 네트워크 아키텍처(100)는 컴퓨터 사용자(134) 또는 애플리케이션(122) 등의 프린서펄이 스토리지(102)에 저장된 아이템에 대해 어떤 액세스 권한을 갖는지를 결정할 수 있다.

[0063] 방법 500은 또한 프린서펄이 보안 규칙의 프린서펄 인자에 지정되어 있는 경우 보안 규칙에 규정된 프린서펄 권한을 부여할 수 있다.

[0064] 방법 500은 또한 질의 요소 인자를 포함하는 질의를 수신할 수 있다. 질의를 전송하는 프린서펄이 질의 요소 인자에서 요소에 대한 적절한 권한을 갖는 경우, 방법 500은 그 질의의 결과를 반환한다. 예를 들어, 프린서펄

이 "녹색"인 어떤 아이템 내의 모든 요소를 요청하는 질의를 전송하고 그 프린서펄이 그 아이템 또는 그 아이템 내의 모든 요소에 대한 권한을 갖는 경우, 녹색인 요소들이 반환되어진다. 프린서펄이 그 아이템 내의 모든 요소에 대한 권한을 갖지 않는 경우, 프린서펄이 녹색인 아이템 내의 요소들 일부에 대한 권한을 가지고 있더라도 질의는 "없음"(not found)을 반환하게 된다. 이것은 보안 규칙이 각각의 요소와 관련되도록 요구하지 않음으로써 효율적인 검색이 여전히 수행될 수 있도록 행해진다. 따라서, 프린서펄이 모든 "녹색" 요소를 찾아내기 위한 질의를 전송하고자 경우, 그 프린서펄은 프린서펄이 그에 대한 권한을 갖지 않는 것을 제외한 모든 요소에 대한 질의를 전송할 수 있다. 따라서, 예를 들어 프린서펄이 도 3에 도시한 요소(320)을 제외한 아이템(310)에 대한 권한을 갖는 경우, 그 프린서펄은 아이템(320)을 제외한 아이템(310)에서 녹색인 모든 요소를 요청해야만 한다.

[0065] 방법 500은 또한 보안 규칙 자체를 수정하기 위한 권한을 제어할 수 있다. 이 경우, 보안 규칙은 [도 2 및 도 3의 볼륨(202) 등의] 볼륨 내에 아이템으로서 포함되어 있다. 이어서, 보안 규칙에 대한 보안이 다른 보안 규칙을 사용하여 설정될 수 있다.

[0066] 본 발명의 일 실시예에서, 사용자가 아이템의 효과적인 보안을 질의할 수 있게 해주는 API가 제공된다. 이 API는 일련의 보안 규칙에 기초하여 보안을 계산한다. 이 API는 이하의 도 6에서 기술되는 것과 같은 실행가능 프로그램 코드일 수 있다.

[0067] 본 발명의 범위 내의 실시예들은 또한 컴퓨터 실행가능 명령어 또는 데이터 구조를 담고 있거나 이를 그 위에 저장하고 있는 컴퓨터 판독가능 매체를 포함한다. 이러한 컴퓨터 판독가능 매체는 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있다. 제한이 아닌 예로서, 이러한 컴퓨터 판독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장 장치, 자기 디스크 저장 장치 또는 다른 자기 저장 장치, 또는 원하는 프로그램 코드 수단을 컴퓨터 실행가능 명령어 또는 데이터 구조의 형태로 담고 있거나 저장하는 데 사용될 수 있고 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 정보가 네트워크 또는 다른 통신 연결(유선, 무선, 또는 유선이나 무선의 조합)을 통해 컴퓨터로 전송 또는 제공되는 경우, 컴퓨터는 당연히 그 연결을 컴퓨터 판독가능 매체로서 본다. 따라서, 임의의 이러한 연결을 컴퓨터 판독가능 매체라고 불러도 무방하다. 상기한 것들의 조합도 컴퓨터 판독가능 매체의 범위 내에 포함되어야 한다. 컴퓨터 실행가능 명령어는 예를 들면 범용 컴퓨터, 특수 목적 컴퓨터 또는 특수 목적 프로세싱 장치로 하여금 어떤 기능 또는 일군의 기능들을 수행하도록 하는 명령어 및 데이터를 포함한다.

[0068] 도 6 및 이하의 설명은 본 발명이 구현될 수 있는 적당한 컴퓨팅 환경에 대한 간략하고 개괄적인 설명을 제공하기 위한 것이다. 꼭 그럴 필요는 없지만, 본 발명은 네트워크 환경에서 컴퓨터에 의해 실행되는, 프로그램 모듈 등의 컴퓨터 실행가능 명령어의 일반적인 관점에서 기술되어질 것이다. 일반적으로, 프로그램 모듈은 특정의 작업을 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로그램, 오브젝트, 컴포넌트, 데이터 구조 등을 포함한다. 컴퓨터 실행가능 명령어, 관련 데이터 구조, 및 프로그램 모듈은 본 명세서에 개시된 방법들의 단계를 실행하기 위한 프로그램 코드 수단의 일례를 나타낸다. 특정의 일련의 이러한 실행가능 명령어 또는 관련 데이터 구조는 이러한 단계들에 기술되어 있는 기능을 구현하기 위한 대응하는 동작의 일례를 나타낸다.

[0069] 당업자라면 본 발명이 퍼스널 컴퓨터, 핸드헬드 장치, 멀티-프로세서 시스템, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터 등을 비롯한 여러가지 유형의 컴퓨터 시스템 구성을 갖는 네트워크 컴퓨팅 환경에서 실시될 수 있음을 잘 알 것이다. 본 발명은 또한 작업들이 통신 네트워크를 통해 (유선 링크, 무선 링크, 또는 유선 링크나 무선 링크의 조합에 의해) 연결되어 있는 국부 또는 원격 프로세싱 장치에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 국부 및 원격 메모리 저장 장치 둘다에 위치할 수 있다.

[0070] 도 6을 참조하면, 본 발명을 구현하기 위한 예시적인 시스템은 프로세싱 유닛(621), 시스템 메모리(622), 및 시스템 메모리(622)를 비롯한 여러가지 시스템 컴포넌트를 프로세싱 유닛(621)에 연결시키는 시스템 버스(623)를 포함하는 종래의 컴퓨터(620) 형태의 범용 컴퓨팅 장치를 포함한다. 시스템 버스(623)는 메모리 버스나 메모리 콘트롤러, 주변 버스, 및 각종의 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스를 비롯한 여러가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리는 판독 전용 메모리(ROM, 624) 및 랜덤 액세스 메모리(RAM, 625)를 포함한다. 시동 중과 같은 때에 컴퓨터(620) 내의 구성 요소들 간의 정보 전송을 돕는 기본 입출력 시스템(BIOS, 626)은 ROM(624)에 저장될 수 있다.

[0071] 컴퓨터(620)는 또한 자기 하드 디스크(639)로부터 판독하거나 그 디스크에 기록하기 위한 자기 하드 디스크 드라이브(627), 분리형 자기 디스크(629)로부터 판독하거나 그 디스크에 기록하기 위한 자기 디스크 드라이브

(628), 및 CD-ROM이나 기타 광학 매체 등의 분리형 광학 디스크(631)로부터 판독하거나 그 디스크에 기록하기 위한 광학 디스크 드라이브(630)를 포함할 수 있다. 자기 하드 디스크 드라이브(627), 자기 디스크 드라이브(628), 및 광학 디스크 드라이브(630)는 각각 하드 디스크 드라이브 인터페이스(632), 자기 디스크 드라이브 인터페이스(633), 및 광학 드라이브 인터페이스(634)에 의해 시스템 버스(623)에 연결된다. 이들 드라이브 및 그들의 관련 컴퓨터 판독가능 매체는 컴퓨터 실행가능 명령어, 데이터 구조, 프로그램 모듈, 및 컴퓨터(620)의 기타 데이터에 대한 비휘발성 저장을 제공한다. 본 명세서에 기술된 예시적인 환경이 자기 하드 디스크(639), 분리형 자기 디스크(629), 및 분리형 광학 디스크(631)를 사용하고 있지만, 자기 카세트, 플래쉬 메모리 카드, DVD, 베르누이 카트리지, RAM, ROM 등을 비롯한 데이터를 저장하기 위한 다른 유형의 컴퓨터 판독가능 매체가 사용될 수 있다.

[0072] 오퍼레이팅 시스템(635), 하나 이상의 애플리케이션 프로그램(636), 기타 프로그램 모듈(637), 및 프로그램 데이터(638)를 비롯한 하나 이상의 프로그램 모듈을 포함하는 프로그램 코드 수단은 하드 디스크(639), 자기 디스크(629), 광학 디스크(631), ROM(624), 또는 RAM(625) 상에 저장될 수 있다. 사용자는 키보드(640), 포인팅 장치(642), 또는 마이크로폰, 조이스틱, 게임 패드, 위성 안테나, 스캐너 등과 같은 다른 입력 장치(도시 생략)를 통해 명령 및 정보를 컴퓨터(620)에 입력할 수 있다. 이들 및 다른 입력 장치는 종종 시스템 버스(623)에 연결된 직렬 포트 인터페이스(646)를 통해 프로세싱 유닛(621)에 연결된다. 다른 대안에서, 입력 장치는 병렬 포트, 게임 포트 또는 유니버설 직렬 버스(USB) 등의 다른 인터페이스에 의해 연결될 수 있다. 모니터(647) 또는 다른 디스플레이 장치도 비디오 어댑터(648) 등의 인터페이스를 통해 시스템 버스(623)에 연결된다. 모니터 이외에, 퍼스널 컴퓨터는 일반적으로 스피커 및 프린터 등의 다른 주변 출력 장치(도시 생략)를 포함한다.

[0073] 컴퓨터(620)는 원격 컴퓨터(683, 693) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(683, 693)는 각각 또하나의 퍼스널 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 다른 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(620)와 관련하여 전술한 구성요소들의 대부분 또는 그 전부를 포함할 수 있다. 도 6에 도시한 논리적 연결은 본 명세서에서 제한이 아닌 예로서 제공되어 있는 근거리 통신망(LAN, 651) 및 원거리 통신망(WAN, 652)을 포함한다. 이러한 네트워킹 환경은 사무실 규모 또는 기업 규모의 컴퓨터 네트워크, 인트라넷 및 인터넷에서 통상적인 것이다.

[0074] 컴퓨터(620)는 LAN 네트워킹 환경에서 사용되는 경우, 네트워크 인터페이스 또는 어댑터(653)를 통해 로컬 네트워크(651)에 연결된다. 컴퓨터(620)는 WAN 네트워킹 환경에서 사용되는 경우, 모뎀(654), 무선 링크, 또는 인터넷 등의 원거리 통신망(652)을 통해 통신을 설정하기 위한 다른 수단을 포함할 수 있다. 내장형 또는 외장형일 수 있는 모뎀(654)은 직렬 포트 인터페이스(646)를 통해 시스템 버스(623)에 연결된다. 네트워크 환경에서, 컴퓨터(620)와 관련하여 도시된 프로그램 모듈 또는 그의 일부분은 원격 메모리 저장 장치에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 원거리 통신망(652)을 통해 통신을 설정하는 다른 수단이 사용될 수 있음을 잘 알 것이다.

[0075] 본 발명은 본 발명의 사상 또는 필수적인 특징을 벗어나지 않고 다른 특정의 형태로 구현될 수 있다. 기술된 실시예들은 모든 점에서 제한적이 아닌 예시적인 것으로 간주되어야 한다. 따라서, 본 발명의 범위는 이상의 설명보다는 오히려 첨부된 청구항들에 의해 나타내어진다. 청구항의 균등물의 의미 및 범위 내에 속하는 모든 변경들은 그의 범위 내에 포함된다.

발명의 효과

[0076] 본 발명은 데이터 아이템의 구역 기반 보안 관리를 제공한다.

도면의 간단한 설명

[0001] 도 1은 본 발명의 원리들에 따라 보안을 관리할 수 있는 시스템을 포함하는 예시적인 네트워크 아키텍처를 나타낸 도면.

[0002] 도 2는 본 발명의 원리들에 따라 아이템을 저장하고 규칙을 정의하는 예시적인 계층적 볼륨을 나타낸 도면.

[0003] 도 3은 본 발명의 원리들에 따라 보안 구역으로 분할되는 예시적인 계층적 볼륨을 나타낸 도면.

[0004] 도 4는 본 발명의 어떤 실시예의 특징들을 사용하여 권리를 위임하는 예시적인 방법을 나타낸 도면.

[0005] 도 5는 본 발명의 어떤 실시예의 특징들을 사용하여 보안 권한을 결정하는 예시적인 방법을 나타낸 도면.

[0006] 도 6은 본 발명의 원리에 적합한 오퍼레이팅 환경을 나타낸 도면.

[0007] <도면의 주요 부분에 대한 부호의 설명>

[0008] 102: 스토리지

[0009] 104: 데이터 스토어

[0010] 112: 메소드 스토어

[0011] 120: 캐쉬

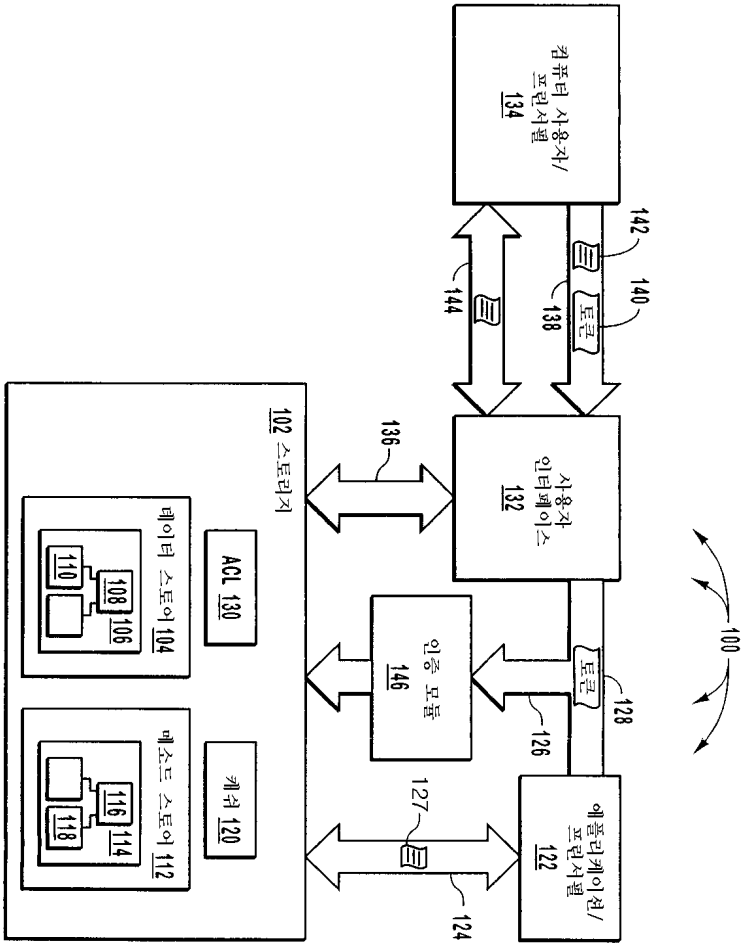
[0012] 122: 애플리케이션

[0013] 132: 사용자 인터페이스

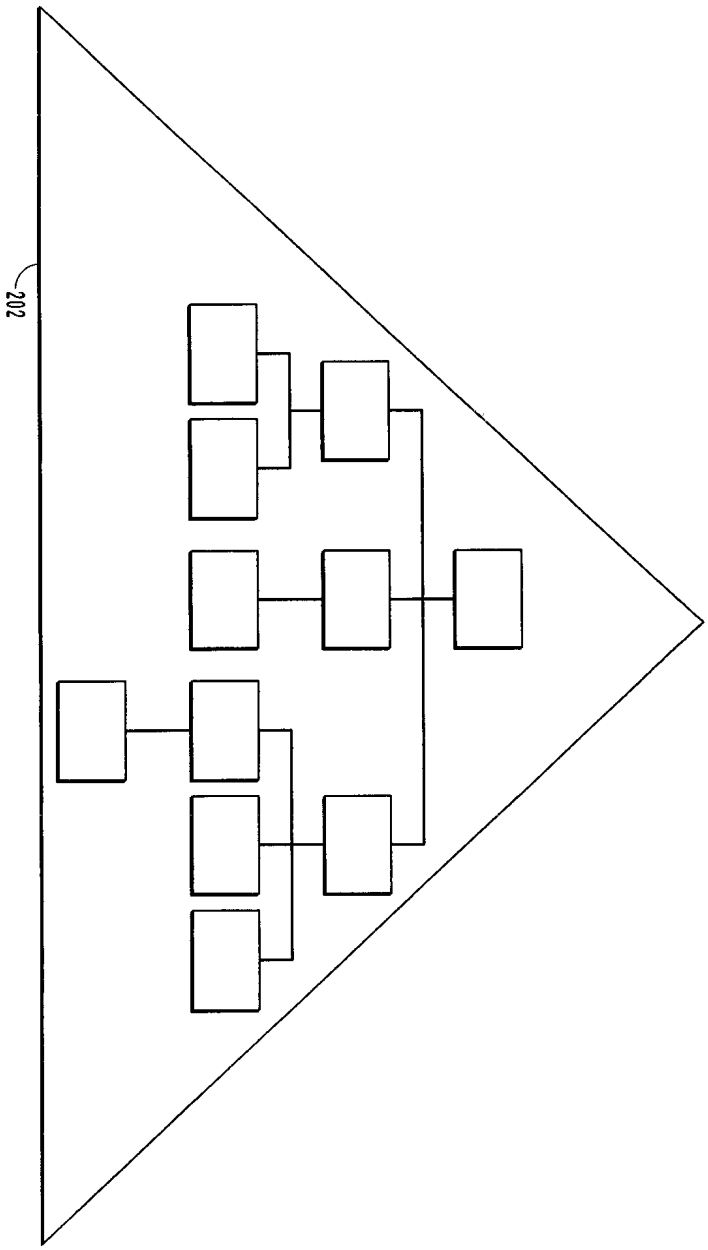
[0014] 134: 컴퓨터 사용자

도면

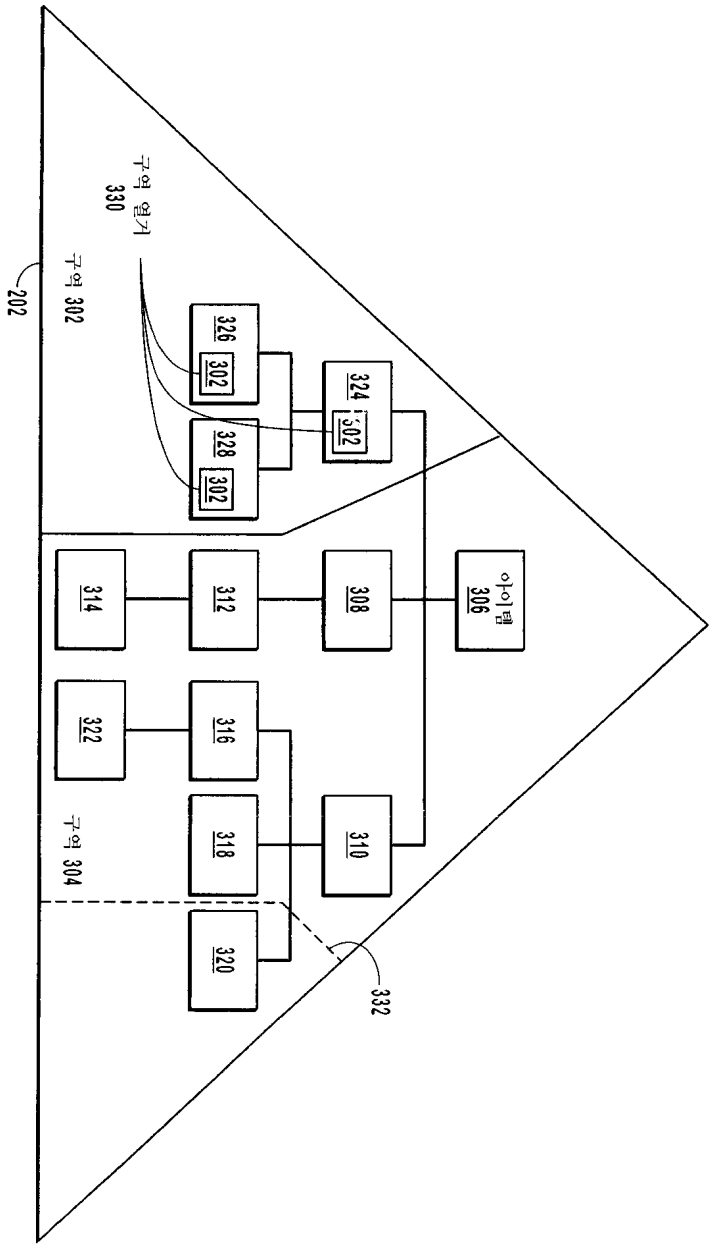
도면1



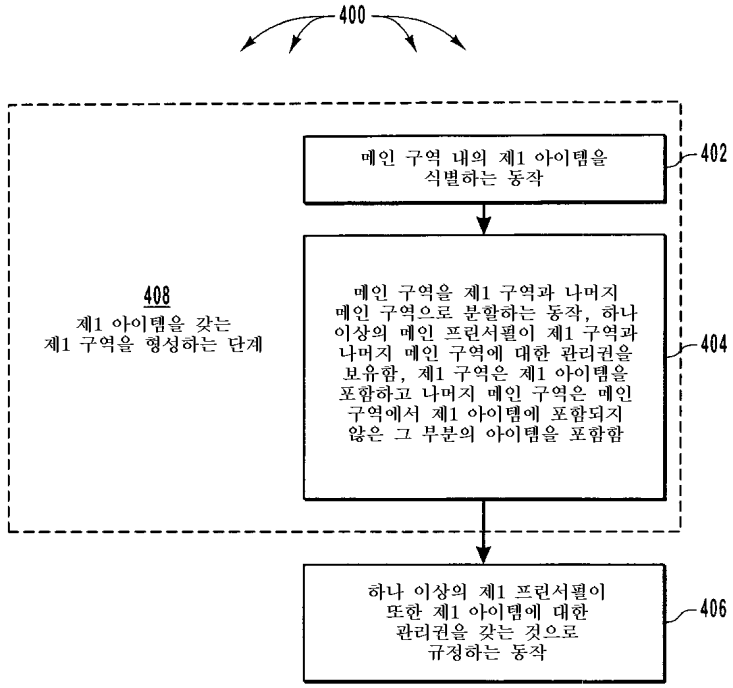
도면2



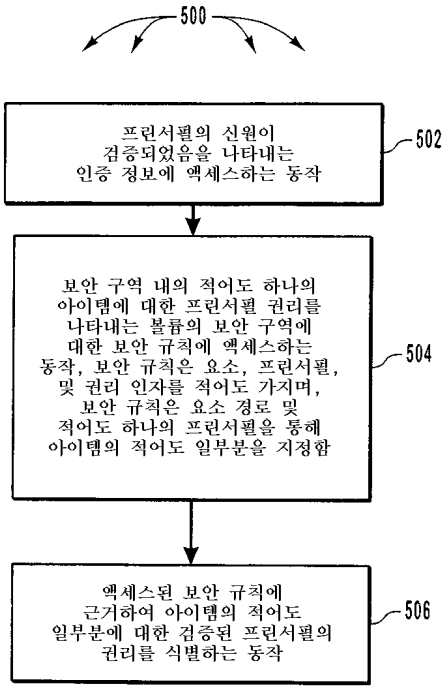
도면3


202
구역 302
구역 열거
330
326
302
328
302
324
302
314
312
308
아이템
306
322
316
318
310
구역 304
320
332

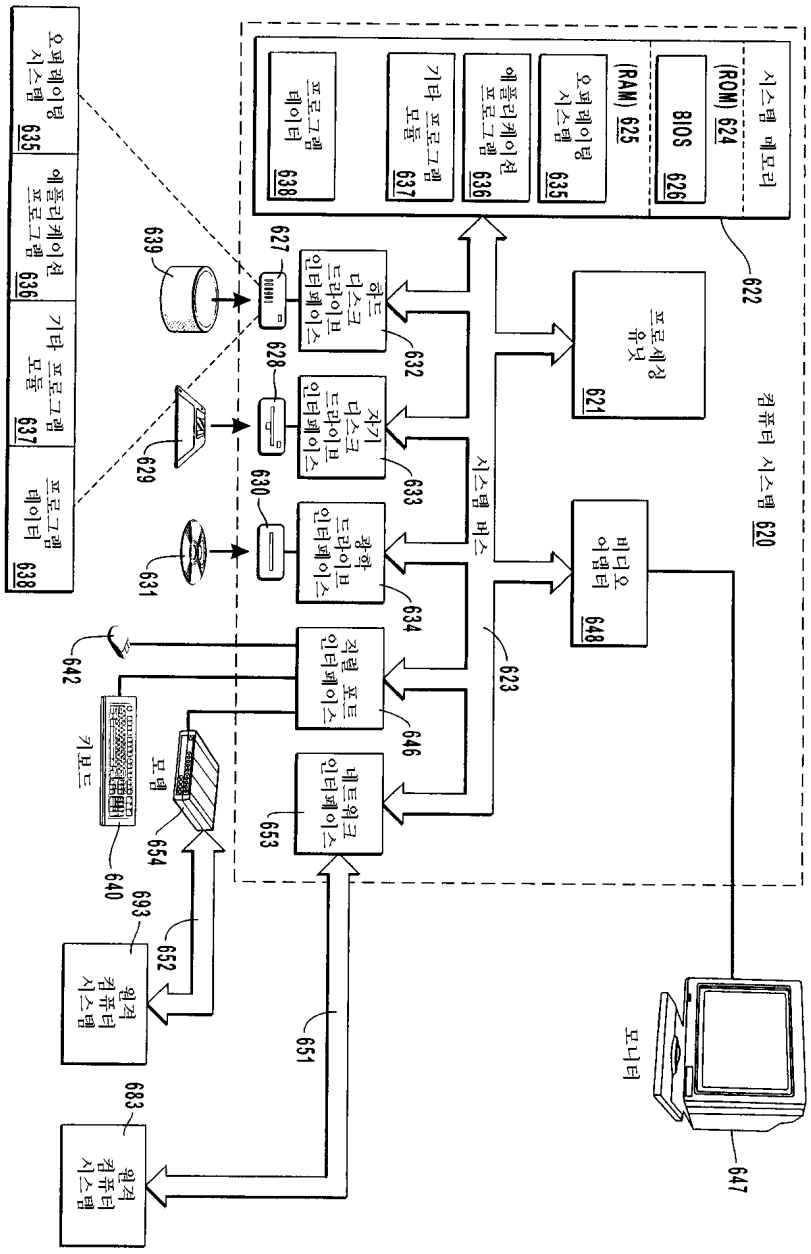
도면4


400
메인 구역 내의 제1 아이템을 식별하는 동작
402
408
제1 아이템을 갖는 제1 구역을 형성하는 단계
메인 구역을 제1 구역과 나머지 메인 구역으로 분할하는 동작, 하나 이상의 메인 프린서펄이 제1 구역과 나머지 메인 구역에 대한 관리권을 보유함, 제1 구역은 제1 아이템을 포함하고 나머지 메인 구역은 메인 구역에서 제1 아이템에 포함되지 않은 그 부분의 아이템을 포함함
404
하나 이상의 제1 프린서펄이 또한 제1 아이템에 대한 관리권을 갖는 것으로 규정하는 동작
406

도면5


500
프린서펄의 신원이 검증되었음을 나타내는 인증 정보에 액세스하는 동작
502
보안 구역 내의 적어도 하나의 아이템에 대한 프린서펄 권리를 나타내는 볼륨의 보안 구역에 대한 보안 규칙에 액세스하는 동작, 보안 규칙은 요소, 프린서펄, 및 권리 인자를 적어도 가지며, 보안 규칙은 요소 경로 및 적어도 하나의 프린서펄을 통해 아이템의 적어도 일부분을 지정함
504
액세스된 보안 규칙에 근거하여 아이템의 적어도 일부분에 대한 검증된 프린서펄의 권리를 식별하는 동작
506

도면6


시스템 메모리
(ROM) 624
BIOS 626
(RAM) 625
오퍼레이팅 시스템 635
애플리케이션 프로그램 636
기타 프로그램 모듈 637
프로그램 데이터 638
622
컴퓨터 시스템 620
프로세싱 유닛 621
시스템 버스
623
비디오 어댑터 648
하드 디스크 드라이브 인터페이스 627
자기 디스크 드라이브 인터페이스 628
광학 드라이브 인터페이스 630
632
633
634
직렬 포트 인터페이스 646
네트워크 인터페이스 653
639
629
631
642
키보드 640
모뎀 654
651
652
693
683
원격 컴퓨터 시스템
원격 컴퓨터 시스템
모니터 647
오퍼레이팅 시스템 635
애플리케이션 프로그램 636
기타 프로그램 모듈 637
프로그램 데이터 638