(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0097274
(43) 공개일자 2014년08월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *G06F 21/31* (2013.01)
(21) 출원번호 10-2014-7014809
(22) 출원일자(국제) 2012년11월21일
심사청구일자 없음
(85) 번역문제출일자 2014년05월30일
(86) 국제출원번호 PCT/US2012/066167
(87) 국제공개번호 WO 2013/081921
국제공개일자 2013년06월06일
(30) 우선권주장
13/308,572 2011년12월01일 미국(US)

(71) 출원인
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
하워드 로버트 맥키
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
미론 티터스 콘스탄틴
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인

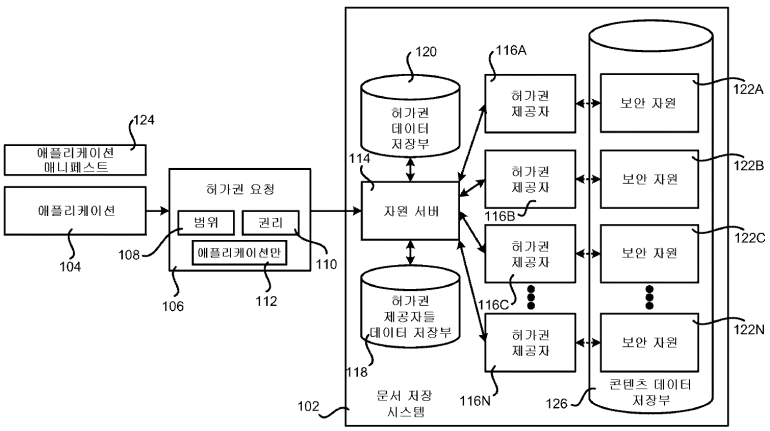
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **보안 자원에 대한 애플리케이션 액세스를 허가하는 기법**

(57) 요 약

본 출원은 자원 서버에 허가권 요청을 제출한다. 요청을 수신함에 응답하여, 자원 서버는 요청된 허가권을 부여하거나 거절할 것을 요청하는 사용자 인터페이스를 생성한다. 허가권이 부여되면, 애플리케이션이 요청된 허가권을 가진다는 것을 나타내는 데이터가 저장된다. 자원에 대한 런타임 요청이 수신될 때, 자원 서버는 해당 요청이 사용자에 의해 이루어진 것인지, 애플리케이션에 의해 이루어진 것인지, 또는 사용자를 대신하여 애플리케이션에 의해 이루어진 것인지를 판단한다. 요청이 애플리케이션에 의해서만 이루어진 것이면, 그 요청은 해당 애플리케이션이 사용자를 대신하는 것이 아닌 직접적인 호출을 통해 자원에 액세스할 허가권을 가진 경우에만 수락된다. 사용자를 대신한 애플리케이션에 의해 요청이 이루어진 경우, 해당 요청은 사용자와 애플리케이션 모두가 충분한 허가권을 가진 경우에만 수락된다.

대 표 도



(72) 발명자

데일러 윌리엄 데이비드

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

쥬 샤오펭

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

아이딘 이레이

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

비라라가반 벤카테쉬

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

특허청구의 범위

청구항 1

문서 저장 시스템 내 보안 자원에 대한 액세스를 허가하기 위한 컴퓨터 구현 방법으로서,

문서 저장 시스템 내 보안 자원에 대한 액션을 수행하라는 요청을 수신하는 단계와,

상기 요청을 수신함에 응답하여, 상기 요청이 사용자에 의해서만 의해 이루어졌는지, 애플리케이션에 의해서만 이루어졌는지, 또는 사용자를 대신하여 애플리케이션에 의해 이루어졌는지를 판단하는 단계와,

상기 요청이 사용자를 대신하여 애플리케이션에 의해 이루어졌다고 판단함에 응답하여, 상기 애플리케이션 및 상기 사용자 모두가 상기 보안 자원에 액세스할 허가권을 가지는 경우에만 상기 요청을 수락하는 단계를 포함하는

컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 요청이 애플리케이션에 의해서만 이루어졌다고 판단함에 응답하여, 상기 애플리케이션이 사용자를 대신하지 않는 직접적인 호출을 통해 상기 보안 자원에 액세스할 허가권을 부여받은 경우에만 상기 요청을 수락하는 단계를 더 포함하는

컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

상기 요청이 사용자를 대신하여 애플리케이션에 의해 이루어졌다고 판단함에 응답하여, 상기 요청된 액션의 수행을 상기 애플리케이션 및 상기 사용자 모두에게 귀속시키는 데이터를 저장하는 단계를 더 포함하는

컴퓨터 구현 방법.

청구항 4

컴퓨터 실행 가능 명령어가 저장된 컴퓨터 판독 가능 저장 매체로서,

상기 명령어는 컴퓨터에 의해 실행될 때 상기 컴퓨터로 하여금

문서 저장 시스템에 의해 보유된 하나 이상의 보안 자원에 액세스할 허가권을 요청하는 허가권 요청을 애플리케이션으로부터 수신하고,

상기 허가권 요청을 수신함에 응답하여, 상기 하나 이상의 보안 자원과 연관된 하나 이상의 허가권 제공자를 식별하고, 각각의 식별된 허가권 제공자로부터 관련 보안 자원에 대해 요청된 상기 허가권을 기술하는 데이터를 요청하고, 상기 허가권 제공자로부터 수신된 상기 데이터를 사용자 인터페이스 안에 모으고, 상기 사용자 인터페이스가 상기 문서 저장 시스템의 현재 사용자에게 디스플레이되게 하고,

상기 사용자 인터페이스를 통해 상기 현재 사용자로부터 상기 애플리케이션에 상기 하나 이상의 보안 자원에 액세스하기 위한 상기 요청된 허가권이 부여됨을 나타내는 표시를 수신하고,

상기 애플리케이션에 상기 요청된 허가권이 부여된다는 표시를 수신함에 응답하여, 상기 애플리케이션이 상기 보안 자원에 대해 상기 애플리케이션에 의한 런타임 요청을 처리하는 데 사용할 상기 하나 이상의 보안 자원에 액세스하도록 하는 상기 요청된 허가권을 가지고 있다는 것을 표시하는 데이터를 저장하도록 하는

컴퓨터 판독 가능 저장 매체.

청구항 5

제4항에 있어서,

상기 컴퓨터에 의해 실행될 때 상기 컴퓨터로 하여금

상기 현재 사용자가 상기 하나 이상의 보안 자원에 액세스할 허가권을 상기 애플리케이션에 부여할 충분한 허가권을 가지는지 여부를 판단하고,

상기 현재 사용자가 상기 하나 이상의 보안 자원에 액세스할 허가권을 상기 애플리케이션에 부여할 충분한 허가권을 가지지 않는다고 판단함에 응답하여 상기 허가권 요청을 거부하도록 하는 컴퓨터 실행 가능 명령어가 더 저장되는

컴퓨터 판독 가능 저장 매체.

청구항 6

제4항에 있어서,

상기 허가권 요청은 사용자를 대신하는 것이 아닌 직접적인 호출을 통해 상기 하나 이상의 보안 자원을 이용하라는 상기 애플리케이션에 의한 요청을 더 포함하는

컴퓨터 판독 가능 매체.

청구항 7

제6항에 있어서,

상기 컴퓨터에 의해 실행될 때 상기 컴퓨터로 하여금

상기 사용자 인터페이스를 통해 상기 현재 사용자로부터 직접 호출을 통해 상기 하나 이상의 보안 자원을 이용하는 허가권이 상기 애플리케이션에 부여됨을 나타내는 표시를 수신하고,

상기 보안 자원에 대한 상기 애플리케이션으로부터의 런타임 요청을 처리할 때 사용하기 위해, 상기 애플리케이션이 사용자를 대신하는 것이 아닌 직접적 호출을 통해 상기 자원을 사용할 허가권을 가지고 있다는 것을 표시하는 데이터를 저장하도록 하는 컴퓨터 실행 가능 명령어가 더 저장되는

컴퓨터 판독 가능 매체.

청구항 8

제4항에 있어서,

상기 허가권 요청은 애플리케이션 매니페스트(manifest)를 통해 상기 문서 저장 시스템에 제공되는

컴퓨터 판독 가능 저장 매체.

청구항 9

제4항에 있어서,

상기 컴퓨터에 의해 실행될 때 상기 컴퓨터로 하여금

상기 애플리케이션으로부터의 상기 허가권 요청을 수신하기에 앞서, 상기 허가권 제공자 각각을 보안 자원의 범

위와 연관되는 것으로서 등록하도록 하는 컴퓨터 실행 가능 명령어가 더 저장되는

컴퓨터 판독 가능 저장 매체.

청구항 10

문서 저장 시스템에 있어서,

문서 저장 시스템에 의해 보유된 하나 이상의 보안 자원에 액세스할 허가권을 요청하는 허가권 요청을 애플리케이션으로부터 수신하고,

상기 허가권 요청을 수신함에 응답하여, 사용자가 상기 허가권 요청을 수락하거나 거부할 것을 요청하는 사용자 인터페이스가 상기 문서 저장 시스템의 상기 사용자에게 디스플레이되도록 하고,

상기 사용자 인터페이스를 통해 상기 사용자로부터 상기 하나 이상의 보안 자원을 액세스하기 위한 상기 요청된 허가권이 상기 애플리케이션에 부여된다는 것을 표시하는 표시를 수신하고,

상기 요청된 허가권이 상기 애플리케이션에 부여된다는 표시를 수신함에 응답하여, 상기 애플리케이션이 상기 보안 자원에 대해 상기 애플리케이션에 의한 런타임 요청을 처리하는 데 사용할 상기 하나 이상의 보안 자원에 액세스하도록 하는 상기 요청된 허가권을 가지고 있다는 것을 표시하는 데이터를 저장하고,

상기 문서 저장 시스템 내 보안 자원에 대한 소정의 액션을 수행하라는 런타임 요청을 수신하고,

상기 요청을 수신함에 응답하여, 상기 요청이 사용자에 의해 이루어진 것인지, 애플리케이션에 의해 이루어진 것인지, 또는 사용자를 대신하여 애플리케이션에 의해 이루어진 것인지를 판단하고,

상기 요청이 사용자를 대신하여 애플리케이션에 의해 이루어졌다고 판단함에 응답하여, 상기 애플리케이션 및 상기 사용자 모두가 상기 보안 자원에 액세스할 허가권을 가지는 경우에만 상기 요청을 수락하도록 구성된 하나 이상의 컴퓨터 시스템을 포함하는

문서 저장 시스템.

명 세 서

배 경 기 술

[0001] 많은 월드 와이드 웹(world wide web("Web")) 애플리케이션들이 웹 애플리케이션의 기능을 확장하는 맞춤형 제3자 애플리케이션들에 대한 설치 및 사용을 허용한다. 이러한 제3자 애플리케이션들은 통상적으로 허가 관점에서 볼 때 웹 애플리케이션의 현재 사용자로서 실행된다. 결과적으로 제3자 애플리케이션들은 통상적으로 웹 애플리케이션과 함께 실행되는 애플리케이션에 대해 정해진 어떤 제한된 한도 내에서 현재의 사용자가 수행할 수 있는 임의의 액션을 통상적으로 수행할 수 있다. 이것은 제3자 애플리케이션을 설치하는 시스템 관리자가 그 애플리케이션에 대해 상당한 신뢰를 가질 것을 요하는데, 이는 그 애플리케이션이 애플리케이션 사용자가 액세스할 수 있는 웹 애플리케이션 안에서 어떠한 정보라도 읽거나, 변경하거나 삭제할 수 있기 때문이다.

[0002] 상술한 문제에 대한 하나의 해법이 제3자 애플리케이션들에 의한 액세스를 웹 애플리케이션에 의해 제공되는 소정 기능에만 한정하는 것이다. 예를 들어, 제3자 애플리케이션은 그 애플리케이션에 노출된 API들(application programming interfaces)을 제한함으로써 웹 애플리케이션의 소정 기능들에 대한 액세스 권한만을 제공받을 수 있다. 상술한 문제에 대한 또 다른 접근법은 애플리케이션을 설치하는 시스템 관리자에 의해 내려지는 신뢰 판정의 범위를 제한하는 것이다. 예를 들어 웹 애플리케이션 안의 환경들은 제3자 애플리케이션들이 다른 환경들의 훼손 위험 없이 분리된 환경들 안에서 설치될 수 있도록 서로 분리될 수 있다. 이러한 해법은 예컨대, 민감한 데이터를 노출하는 환경에 대한 애플리케이션의 액세스를 제한하기 위해 사용될 수 있다. 그러나 이 해법은 제3자 애플리케이션들을 이용하는 가장 일반적인 이유 중 하나가 다양한 환경들에 걸쳐 데이터를 모으기 위한 것이라는 사실을 감안할 때 매우 제한적인 것이다. 결론적으로, 웹 애플리케이션 보급에 걸친 회사의 모든 환경들에 적용하는 애플리케이션들은 이러한 시나리오에서 설치가 어렵거나 불가능하다.

[0003] 상술한 바와 같이, 이러한 제3자 애플리케이션들은 통상적으로 허가 관점에서 볼 때, 웹 애플리케이션의 현재 사용자로서 실행된다. 이는 애플리케이션들이 그 사용자들이 수행 권한을 가진 액션들에 대해서만 수행할 수 있다는 것을 의미한다. 그러나 많은 상황들에 있어서, 사용자나 사용자 그룹에게 애플리케이션 사용을 통해,

그들의 허가권한이 그들이 직접 수행하는 것을 허용하지 않을 액션을 수행할 수 있도록 하는 것이 바람직하다. 예를 들어, 비용 보고 애플리케이션은 소정 조건(가령, 작은 값)이 충족될 때 비용 보고를 승인할 수 있지만, 사용자는 그 애플리케이션을 통해 동작을 수행하지 않고 비용 보고를 바로 승인하는 허가권을 가져서는 안된다. 이러한 유형의 동작은 애플리케이션이 현재의 사용자로서 실행될 때 가능하지 않다. 어떤 시스템들은 애플리케이션들이 시스템 계정에 대한 허가권한을 높여 시스템 안에서 아무 허가 제한도 없게 함으로써 그러한 한계에 대처한다. 그러나, 이러한 해법은 시스템 관리자들이 민감한 정보를 노출하는 환경들에 애플리케이션들을 설치하는 것을 더욱더 주저하게 만들 수 있다.

[0004] 이러한 것들 및 기타 고려사항들과 관련하여 본 명세서에서 이루어진 개시가 제시된다.

발명의 내용

과제의 해결 수단

[0005] 본 명세서에서는 안전한 자원들에 대한 애플리케이션 액세스를 허가하기 위한 개념 및 기술들이 기술된다. 본 명세서에 개시된 기술들의 구현을 통해, 보안 자원의 소유자는 애플리케이션에게 그 보안 자원을 이용하는 특권을 부여할 수 있다. 부여된 특권을 이용하여 애플리케이션은 런타임시, 자원의 소유자와 동일한 정도까지 그 보안 자원을 직접(즉, 사용자 없이) 이용할 수 있다. 그러나 사용자가 보안 자원에 액세스하는 애플리케이션을 이용하는 경우, 자원 사용은 사용자의 특권의 정도까지 제한된다. 이런 식으로, 애플리케이션이 보안 자원을 직접 액세스할 때, 애플리케이션의 특권이 보안 자원 소유자의 수준까지 높아질 수 있다. 그러나 보안 자원에 대한 액세스는 사용자가 그 자원에 액세스하기 위해 상기 애플리케이션을 이용할 때, 사용자의 권한의 정도까지로 제한된다.

[0006] 본 명세서에 제시된 한 양태에 따르면, 문서 저장 애플리케이션과 같은 웹 애플리케이션은 상기 웹 애플리케이션의 기능을 확장하는 맞춤형 제3자 애플리케이션들의 사용을 허용하도록 구성된다. 콘텐츠 데이터베이스의 항목들과 같이 웹 애플리케이션에 의해 관리되는 보안 자원들에 액세스하여 사용할 허가권을 획득하기 위해, 애플리케이션은 먼저, 웹 애플리케이션의 일부로서 실행되는 자원 서버로 허가권 요청을 제출한다. 허가권 요청은 상기 애플리케이션에 의해 요청되는 범위 및 권한을 확인한다. 허가권 요청은 사용자를 대신하는 것이 아닌 직접적인 호출을 통해, 하나 이상의 보안 자원들을 이용할 허가권이 상기 애플리케이션에 부여될 것을 요청하는 것일 수도 있다. 허가권 요청은 HTTP(hypertext transfer protocol) 요청, 애플리케이션 매니페스트(manifest), 웹 애플리케이션에 의해 제공되는 사용자 인터페이스(UI), 웹 애플리케이션에 의해 제공되는 API 또는 다른 방식을 통해 제출될 수 있다.

[0007] 허가권 요청을 수신함에 응답하여, 자원 서버는 허가권이 요청되는 보안 자원들과 관련된 하나 이상의 허가권 제공자들을 식별하도록 구성된다. 그런 다음 자원 서버는 각각의 식별된 허가권 제공자로부터 관련 보안 자원에 대해 요청된 허가권을 기술하는 데이터를 요청한다. 그런 다음 상기 데이터는 웹 애플리케이션의 현재 사용자에게 디스플레이되는 UI 안에 집합된다. UI는 사용자에게 상기 애플리케이션에 요청된 허가권을 부여하거나 거절할 것을 요구한다. 사용자가 요청된 허가권을 상기 애플리케이션에 부여하면, 상기 애플리케이션이 상기 요청된 허가권을 가진다는 것을 나타내는 데이터가 저장된다. 런타임 시, 이러한 데이터는 웹 애플리케이션에 의해 관리되는 보안 자원들에 대한 상기 애플리케이션에 의한 런타임 요청들을 처리하는데 사용된다.

[0008] 보안 자원에 대한 어떤 액션을 수행하라는 런타임 요청이 자원 서버에 의해 수신될 때, 자원 서버는 해당 요청이 사용자에 의해 이루어진 것인지, 애플리케이션에 의해서만 이루어진 것인지, 또는 사용자를 대신하여 애플리케이션에 의해 이루어진 것인지를 판단한다. 요청이 애플리케이션에 의해서만 이루어진 것이면, 자원 서버는 사용자를 대신하는 것이 아닌 직접적인 호출을 통해 상기 보안 자원에 액세스하도록 하는 허가권이 상기 애플리케이션에 상술한 방식을 통해 부여된 경우에만 상기 요청을 수락한다. 사용자를 대신하여 애플리케이션에 의해 요청이 이루어진 경우, 상기 자원 서버는 사용자와 애플리케이션 모두가 상기 요청된 액션을 수행하기 위한 허가권을 가진 경우에만 상기 요청을 수락한다. 자원 서버는 또한, 상기 보안 자원에 대한 액션 수행을 사용자, 애플리케이션, 또는 사용자와 애플리케이션 둘 모두에 귀속시키는 히스토리 데이터를 저장한다.

[0009] 본 요약은 청구된 주제의 주요 특징이나 필수적 특징을 확인하도록 의도된 것이 아니며, 이 요약이 청구된 발명 대상의 범위를 한정하는 데 사용되도록 의도된 것도 아니다. 또한 청구된 발명 대상이 이 개시의 임의의 부분에 언급된 임의의 혹은 모든 단점들을 해결하는 구현예들에 국한되지 않는다.

도면의 간단한 설명

[0010] 도 1은 본 명세서에 개시된 일 실시예에서 애플리케이션 및 문서 저장 시스템의 동작 양태들을 예시한 소프트웨어 구조도이다.

도 2는 본 명세서에 개시된 일 실시예에서 허가권 제공자들을 등록하기 위한 하나의 루틴에 대한 양태들을 보여주는 흐름도이다.

도 3a 및 3b는 본 명세서에 개시된 일 실시예에서 자원 서버에 애플리케이션을 등록하기 위한 하나의 루틴에 대한 양태들을 보여주는 흐름도들이다.

도 4a는 본 명세서에 개시된 일 실시예에서 사용되는 예시적 허가권 요청의 형식 및 구조를 보여주는 데이터 구조도이다.

도 4b는 본 명세서에 개시된 일 실시예에서 애플리케이션에 허가권을 부여하기 위한 하나의 예시적 사용자 인터페이스를 보여주는 사용자 인터페이스도이다.

도 5는 본 명세서에 개시된 일 실시예에서 자원 요청들을 처리하기 위해 사용되는 메커니즘의 양태들을 보여주는 네트워크도이다.

도 6a-6b는 일 실시예에 따른 보안 자원들에 대한 요청들을 처리하기 위한 하나의 루틴의 양태들을 보여주는 흐름도들이다.

도 7은 여기에 제시된 실시예들의 양태들을 구현할 수 있는 컴퓨팅 시스템의 예시적 컴퓨터 하드웨어 및 소프트웨어 구조를 보여주는 컴퓨터 구조도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이하의 상세한 설명은 애플리케이션에 보안 자원들에 대한 액세스를 허가하기 위한 개념들과 기술들에 관한 것이다. 위에서 간략히 논의된 바와 같이, 여기에 개시된 기술들을 사용하여, 웹 애플리케이션과 함께 실행되는 애플리케이션은 런타임 시, 자원 소유자와 동일한 정도까지 보안 자원들을 직접적으로 사용할 수 있다. 사용자가 보안 자원들을 이용하기 위해 애플리케이션을 이용할 때, 사용자와 애플리케이션 모두 보안 자원들을 이용하기 위한 적절한 허가권을 가져야 한다. 이러한 특징 및 다른 특징에 관한 추가 세부사항들이 도 1-7과 관련하여 이하에서 제공될 것이다.

[0012] 여기에 기술된 주제는 하나 이상의 컴퓨터 시스템들 상의 운영체제 및 다양한 프로그램들의 실행과 연계하여 실행되는 프로그램 모듈들의 일반적 맥락에서 기술될 것이지만, 당업자는 다른 구현예들이 다른 타입의 프로그램 모듈들과 조합하여 수행될 수 있다는 것을 인지할 것이다. 일반적으로 프로그램 모듈은 특정 작업을 수행하거나 특정한 추상적 데이터 유형들을 구현하는 루틴, 프로그램, 컴포넌트, 데이터 구조, 및 다른 타입의 구조들을 포함한다. 또한 당업자는 여기 기술된 주제가 핸드헬드 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 또는 프로그래머블 가전기기, 미니 컴퓨터, 메인프레임 컴퓨터 등을 포함하는 다른 컴퓨터 시스템 구성들을 이용하여 실시될 수 있다는 것을 예상할 것이다.

[0013] 이하의 상세한 설명에서는 그 일부를 형성하고 예로서 특정 실시예들이나 예들이 도시되는 첨부된 도면들이 참조된다. 이제 여러 형상들에 걸쳐 유사 참조부호가 유사 구성요소들을 나타내는 도면들을 참조하여, 애플리케이션에 보안 자원에 대한 액세스를 허가하기 위한 컴퓨팅 시스템 및 방법론에 대한 양태들이 기술될 것이다.

[0014] 도 1은 본 명세서에 개시된 일 실시예에서 애플리케이션(104) 및 문서 저장 시스템(102)의 동작 양태들을 예시한 소프트웨어 구조도이다. 문서 저장 시스템(102)은 웹 기반 문서 저장 애플리케이션(미도시)을 실행하도록 구성된 하나 이상의 컴퓨팅 시스템이다. 문서 저장 시스템(102)은 문서 저장 시스템(102)의 허가된 사용자들 사이에서 문서들 및 잠정적 다른 타입의 항목들을 저장하고, 액세스하며 공유하기 위한 기능을 제공한다. 이와 관련하여, 문서 저장 시스템(102)은 사용자가 콘텐츠 데이터 저장부(126)에 저장된 문서들 및 다른 타입의 전자 항목들을 생성, 변경, 삭제, 및 그렇지 않으면 이용할 수 있게 하는 기능을 제공할 수 있다.

[0015] 문서 저장 시스템(102)은 허가권에 기반하여 콘텐츠 데이터 저장부(126) 안의 항목들에 대한 액세스를 제한할 수 있다. 예를 들어 소정 사용자들에게만 콘텐츠 데이터 저장부(126) 안의 항목들의 일부에 액세스하거나 그들을 변경하도록 허가되도록, 문서 저장 시스템(102)의 사용자들에 대해 허가권이 설정될 수 있다. 콘텐츠 데이

터 저장부(126)에 저장된 항목들이 상술한 방식으로 허가권을 이용하여 보안되기 때문에, 그러한 항목들을 여기에서 보안 자원들(122A-122N)(집합적으로 보안 자원들(122))이라 칭한다.

[0016] 보안 자원들(122)은 본 명세서에서 기본적으로 콘텐츠 데이터 저장부(126) 상의 항목들로서 기술되지만, 보안 자원들(122)은 허가권에 기반하여 액세스가 통제되는 어떤 다른 타입의 컴퓨팅 자원일 수도 있다는 것을 이해해야 한다. 본 명세서에 개시된 실시예들이 문서 저장 시스템(102)과 관련하여 기본적으로 기술되지만, 본 명세서에 개시된 실시예들이 그러한 구현예에 국한되는 것인 아니라는 것 또한 이해해야 한다. 그보다 본 명세서에 개시된 실시예들은 어떤 애플리케이션이 보안 자원들에 액세스하도록 허가하는 모든 유형의 컴퓨팅 시스템과 함께 사용될 수 있다.

[0017] 일 실시예에서 문서 저장 시스템(102)은 보안 자원들(122)에 대한 액세스를 통제하기 위한 자원 서버(114)를 포함한다. 자원 서버(114)는 보안 자원들(122)에 액세스하라는 요청을 수신하고 그에 응답하도록 구성된 하나 이상의 소프트웨어 및/또는 하드웨어 구성요소들이다. 자원 서버(114)는 또한 보안 자원들(122)을 이용하기 위해 애플리케이션(104)과 같은 애플리케이션들을 등록하기 위한 기능을 제공한다.

[0018] 애플리케이션(104)은 문서 저장 시스템(102)과 함께 사용하도록 구성된 애플리케이션이다. 예를 들어 애플리케이션(104)은 문서 저장 시스템(102)에 의해 제공되는 기능을 확장할 수도 있다. 애플리케이션(104)은 웹 기반 애플리케이션이거나 문서 저장 시스템(102) 상에서 직접 실행될 수도 있다. 원하는 기능을 제공하기 위해, 애플리케이션(104)은 통상적으로 보안 자원들(122) 중 하나 이상을 이용한다. 애플리케이션(104)이 기본적으로 본 명세서에서는 문서 저장 시스템(102)에 의해 제공되는 기능을 확장하기 위한 애플리케이션으로서 기술되지만, 본 명세서에 사용되는 실시예들은 다른 유형의 애플리케이션들을 통해서도 실시될 수 있다는 것을 이해해야 한다.

[0019] 보안 자원들(122)을 이용하기 위한 권한을 얻기 위해, 애플리케이션(104)은 일 실시예에서 자원 서버(114)로 허가권 요청(106)을 제공한다. 허가권 요청(106)은 애플리케이션(104)에 의해 요청되는 액세스 범위(108) 및 특정 범주에 대해 요청된 허가권들을 규정하는 권리(110)를 정의하는 데이터이다. 허가권 요청(106)은 사용자를 대신하는 것이 아닌 직접적인 호출들을 통해, 하나 이상의 보안 자원들을 이용할 허가권이 상기 애플리케이션(104)에 부여될 것을 요청하는 "애플리케이션만의" 요청(112)을 포함할 수도 있을 것이다. 애플리케이션(104)은 HTTP(hypertext transfer protocol) 요청, 애플리케이션 매니페스트(manifest), 문서 저장 시스템(102)에 의해 제공되는 사용자 인터페이스(UI), 문서 저장 시스템(102)에 의해 제공되는 API 또는 다른 방식을 통해 허가권 요청(106)을 제출할 수 있다. 하나의 예시적 허가권 요청(106)이 도 4a와 관련하여 아래에서 기술될 것이다.

[0020] 애플리케이션(104)으로부터 허가권 요청(106)을 수신함에 따라, 자원 서버(114)는 보안 자원들(122A-122N) 각각에 대한 허가권들의 제공자들로서 등록하였던 하나 이상의 허가권 제공자들(116A-116N)(집합적으로 허가권 제공자들(116))을 식별한다. 예를 들어 도 1에 도시된 예에서, 허가권 제공자(116A)는 보안 자원들(122A)에 대한 허가권들의 제공자로서 등록하였다. 허가권 요청(106)의 범위(108)가 보안 자원(122A)을 포함하면, 자원 서버(114)는 허가권 제공자(116A)를 허가권 요청(106)에 대한 관련 허가권 제공자로서 식별할 것이다.

[0021] 자원 서버(114)에 등록하기 위해, 각각의 허가권 제공자(116)는 자원 서버(114)에게 허가권 제공자가 관련된 자원들의 범위를 알린다. 각각의 허가권 제공자(116)는 또한 자원 서버(114)에 콜백(callback) 함수들을 또한 등록할 수도 있다. 예를 들어 각각의 허가권 제공자(116)는 자원 서버(114)가 보안 자원(122)과 관련된 허가권들을 기술하는 데이터를 획득할 수 있게 하는 데이터를 자원 서버(114)에 등록할 수도 있다. 이하에서 상세히 기술되는 바와 같이, 자원 서버(114)는 이러한 데이터를 허가권 요청(106) 시 애플리케이션(104)에 의해 요청되는 허가권들을 사용자에게 알리는 UI를 구성하는 데 사용할 수 있다.

[0022] 각각의 허가권 제공자(116)는 또한, 허가권 요청(106)이 수락되었다는 통지를 제공할 수 있게 하는 콜백 함수를 등록할 수도 있다. 자원 서버(114)는 허가권 제공자들 데이터 저장부(118) 안에 상기 콜백 함수들을 식별하는 데이터를 포함하는 상기 등록 데이터를 저장한다. 허가권 제공자들(116)을 등록하기 위한 하나의 프로세스에 관한 추가적 세부사항들이 이하에서 도 2와 관련하여 제공될 것이다.

[0023] 허가권 요청(106)과 관련해 자원 서버(114)가 허가권 제공자들(116)을 식별하였으면, 자원 서버(114)는 요청된 허가권들을 기술하는 데이터를 획득하기 위해 각각의 식별된 제공자(116)의 콜백 함수를 호출한다. 자원 서버(114)는 상기 허가권 요청(106) 시 범위(108)와 권리(110)를, 현재의 사용자를 식별하는 현재의 정황과 함께 상기 식별된 허가권 제공자들(116)로 전달할 것이다. 그러면, 각각의 호출된 허가권 제공자(116)는 현재의 사용

자가 허가권 요청(106) 시 요청된 허가권들을 애플리케이션(104)에 부여하기 충분한 특권을 가지는지 여부를 판단한다.

[0024] 해당 사용자가 애플리케이션(104)에 상기 요청된 허가권들을 부여할 정도의 충분한 특권을 가지지 못한 경우, 허가권 요청(106)은 거부될 것이다. 사용자가 허가권 요청(106)을 허락하기 충분한 특권을 가지는 경우, 각각의 허가권 제공자(116)는 애플리케이션(104)에 의해 요청된 허가권들을 사용자에게 표시하는 UI를 구성하는 데 사용될 수 있는 데이터를 자원 서버(114)로 보낼 것이다. 이 데이터는 HTML(hypertext markup language) 형식, 평이한 텍스트, 또는 대화 박스와 같이 UI 요소에 직접 포함시키기 적합한 다른 적절한 형식으로 되어 있을 수 있다.

[0025] 자원 서버가 상기 식별된 허가권 제공자들(116)로부터 응답을 수신했으면, 자원 서버(114)는 그 수신된 데이터를 현재 사용자에게 디스플레이되는 UI에 집합시킨다. UI는 상기 요청된 허가권들의 내용을 기술하고 사용자에게 허가권 요청(106) 시 애플리케이션(104)에 의해 요청된 허가권들을 수락하거나 거부할 것을 요구한다. 그러한 하나의 예시적 UI가 도 4b와 관련하여 아래에서 기술될 것이다. 사용자가 UI를 통해 요청된 허가권들을 애플리케이션(104)에 부여하면, 자원 서버(114)는 허가권 데이터 저장부(120) 안에 상기 애플리케이션(104)이 상기 요청된 허가권을 가진다는 것을 나타내는 데이터를 저장한다. 런타임 시, 자원 서버(114)는 이 데이터를 보안 자원들(122)에 대한 액션을 수행하라는 애플리케이션(104)에 의한 요청들을 처리하기 위해 이용한다. 자원 서버(114)에 의해 수행되는 런타임 처리에 관한 추가적 세부사항들이 도 5 및 6a-6b와 관련하에 이하에서 제공될 것이다.

[0026] 도 2는 본 명세서에 개시된 일 실시예에서 허가권 제공자들(116)을 등록하기 위한 하나의 루틴(200)에 대한 양태들을 보여주는 흐름도이다. 도 2 및 다른 도면들과 관련하여 여기에 기술된 로직 동작들은 (1) 컴퓨팅 시스템 상에서 실행되는 컴퓨터 구현 행위들이나 프로그램 모듈들의 시퀀스 및/또는 (2) 컴퓨팅 시스템 안의 상호연결된 기계 로직 회로들이나 회로 모듈들로 구현된다. 그 구현은 컴퓨팅 시스템의 성능 및 다른 요건들에 좌우되는 선택 사항이다. 따라서 여기에 기술되는 로직 동작들은 동작들, 구조적 소자들, 행위들, 또는 모듈들이라 다양하게 불린다. 이 동작들, 구조적 소자들, 행위들, 및 모듈들은 소프트웨어, 펌웨어, 특수 용도의 디지털 로직, 및 이들의 어떤 조합으로 구현될 수 있다. 또한 도면에 도시되고 여기에 기술된 것보다 많거나 더 적은 동작들도 수행될 수 있다는 것을 이해해야 한다. 이 동작들은 여기에 기술된 실시예와 다른 순서로 수행될 수도 있다.

[0027] 루틴(200)은 허가권 제공자(116)가 등록되어야 하는 보안 자원들의 범위에 대한 지시를 허가권 제공자(116)가 자원 서버(114)에게 제공하는 동작(202)에서 시작한다. 루틴(200)은 이어서, 허가권 제공자(116)가 요청된 허가권을 기술하는 데이터를 획득할 수 있게 하는 콜백 함수를 자원 서버(114)에게 제공하는 동작(204)으로 진행한다. 위에서 간략히 논의된 바와 같이, 자원 서버(114)는 사용자가 허가권 요청(106)을 승인하거나 거부할 것을 요청하는 UI를 생성하는데 이 정보를 이용할 수 있다.

[0028] 동작(204)으로부터 루틴(200)은 자원 서버(114)가 허가권 제공자(116)에게 허가권 요청(106)이 부여되었다고 통지하는데 사용할 수 있는 콜백 함수를 자원 서버(114)에게 제공하는 동작(206)으로 진행한다. 동작들(202, 204, 및 206)에서 제공된 정보는 하나나 여러 개의 데이터 구조들로 제공될 수 있다는 것을 이해해야 한다. 이 정보는 XML(extensible markup language)를 이용하거나, 다른 구조의 언어 포맷을 이용하거나, 또 다른 방식을 모두 이용하여 구성될 수도 있을 것이다.

[0029] 동작(206)으로부터 루틴(200)은 자원 서버(114)가 허가권 제공자들 데이터 저장부(118) 안에 허가권 제공자(116)에 의해 식별된 범위 및 콜백 함수들을 저장하는 동작(208)으로 진행한다. 상기 데이터가 저장되었으면, 루틴(200)은 동작(208)에서 루틴이 종료되는 동작(210)으로 진행한다.

[0030] 도 3a 및 3b는 본 명세서에 개시된 일 실시예에서 자원 서버(114)에 애플리케이션(104)을 등록하기 위한 하나의 루틴(300)에 대한 양태들을 보여주는 흐름도들이다. 루틴(300)은 자원 서버(114)가 허가권 요청(106)을 수신하는 동작에서 시작한다. 루틴(300)은 그런 다음, 자원 서버(114)가 허가권 요청(106)시 기술된 허가권들의 범위와 관련된 허가권 제공자들(116)을 식별하는 동작(304)으로 이어진다. 예를 들어 자원 서버(114)는 범위(108)와 관련된 허가권 제공자들(116)을 식별하기 위해 허가권 제공자들 데이터 저장부(118)에 저장된 정보를 통해 반복할 것이다. 허가권 제공자들(116)이 식별되었으면, 루틴(300)은 동작(304)에서 동작(306)으로 진행한다.

[0031] 동작(306)에서 자원 서버(114)는 요청된 범위(108), 권리(110), 만일 있다면 애플리케이션만의 요청(112), 그리고 현재의 정황을 허가권이 요청되는 등록된 허가권 제공자들(116) 각각에게 전달한다. 이러한 정보를 수신함

에 따라, 각각의 허가권 제공자(116)는 현재의 사용자가 상기 요청된 허가권을 부여하기 충분한 권한을 가지는지를 판단한다. 이것은 예컨대, 허가권 데이터 저장부(120) 안에 저장된, 현재 사용자에 의해 보유된 특권들을 나타내는 데이터를 참조함으로써 수행될 수 있다. 사용자가 애플리케이션(104)에 상기 요청된 허가권들을 부여할 수 없으면, 루틴(300)은 동작(310)에서 허가권 요청(106)이 거부되는 동작(312)으로 진행한다. 또한, 허가권이 부여될 수 없다는 것을 가리키는 UI가 사용자에게 제공될 수 있다. 루틴(300)은 이제 동작(312)에서 루틴이 종료되는 동작(314)으로 진행한다.

[0032] 사용자가 허가권 요청(106)을 수락할 충분한 특권을 보유한 경우, 루틴(300)은 동작(310)에서 동작(316)(도 3b에 도시됨)으로 진행한다. 동작(316)에서, 자원 서버(114)는 각각의 허가권 제공자(116)에게 요청된 허가권을 기술하는 데이터를 얻기 위해, 각각의 식별된 허가권 제공자(116)의 콜백 함수를 호출한다. 이어서, 상기 호출된 허가권 제공자들(116) 각각이 자원 서버(114)에게 상기 요청된 정보를 제공한다. 루틴(300)은 이제 동작(316)에서 동작(318)으로 진행한다.

[0033] 동작(318)에서 자원 서버(114)는 허가권 제공자들(116)로부터 수신된 데이터를 UI 안에 모아서 그 UI를 현재의 사용자에게 제시한다. 상술한 바와 같이, UI는 또한, 사용자에게 애플리케이션(104)에 대해 허가권 요청(106)에 기술된 특권들의 부여를 승인하거나 거부할 것을 요구하기도 한다. 그러한 하나의 UI가 도 4b와 관련하여 아래에서 기술될 것이다.

[0034] 사용자가 애플리케이션(104)에 대해 특권들의 부여를 거부하면, 루틴(300)은 동작(320)에서 동작(322)으로 진행한다. 동작(322)에서 허가권 요청(106)이 거부된다. 또한, 요청된 허가권이 부여될 수 없다는 것을 가리키는 UI가 사용자에게 제공될 수 있다. 루틴(300)은 이제 동작(322)에서 루틴이 종료되는 동작(328)으로 진행한다.

[0035] 사용자가 허가권 요청(106)을 승인하면, 루틴(300)은 동작(320)에서 동작(324)으로 진행한다. 동작(324)에서 자원 서버는 허가권 요청(106)이 허락되었다는 것을 나타내기 위해 각각의 식별된 허가권 제공자(116)에 의해 노출된 콜백 기능을 호출한다. 그런 다음 루틴(300)은 애플리케이션(104)에 대해 상기 요청된 허가권의 부여를 지시하는 데이터가 허가권 데이터 저장부(120)에 저장되는 동작(326)으로 진행한다. 상술한 바와 같이, 이 데이터는 안전 자원들(122)에 대해 애플리케이션(104)으로부터 수신된 요청들이 승인되어야 하는지 거부되어야 하는지 여부를 판단하기 위해 런타임 시 사용된다. 동작(326)으로부터 루틴(300)은 그것이 종료되는 동작(328)으로 진행한다.

[0036] 도 4a는 본 명세서에 개시된 일 실시예에서 사용되는 예시적 허가권 요청(106)의 형식 및 구조를 보여주는 데이터 구조도이다. 특히, 도 4a에 도시된 예시적 허가권 요청(106) 시, 애플리케이션(104)은 네 개의 서로 다른 보안 자원들에 대한 허가권을 요청하고 있다. 그에 따라 허가권 요청(106)은 각각의 자원에 대응하는 XML 요소를 포함한다. 특히, 한 요소는 문서 라이브러리에 대한 특권들의 요청에 해당하고, 한 요소는 사용자 프로파일 저장부에 대한 특권들의 요청에 해당하고, 한 요소는 캘린다에 대한 특권들의 요청에 해당하며, 또 다른 요소는 연락처에 대한 특권들의 요청에 해당한다.

[0037] 특권들이 요청된 각각의 보안 자원에 대해, 허가권 요청(106)은 요청된 권리 또한 특정한다. 예를 들어 도 4a에 도시된 허가권 요청(106)은 연락처를 읽고, 캘린다를 읽고, 문서 라이브러리에 쓰는 권리를 요청한다. 다른 유형의 권리들 또한 요청될 수도 있음을 이해해야 한다. 도 4a에 도시된 허가권 요청은 XML을 이용하여 표현되었지만, 다른 구조나 비구조 언어들 또한 사용될 수도 있다는 것 또한 이해해야 한다. 데이터의 다른 요소들, 구성들 및 배열들 역시, 범위(108), 권리(110), 애플리케이션만의 요청(112) 및 허가권 요청(106)의 어떤 다른 요소들을 표현하는데 이용될 수도 있을 것이다.

[0038] 도 4b는 본 명세서에 개시된 일 실시예에서 애플리케이션(104)에 허가권을 부여하기 위한 하나의 예시적 사용자 인터페이스(400)를 보여주는 사용자 인터페이스도이다. 위에 논의된 바와 같이, 자원 서버(114)는 허가권 요청(106)의 수신에 뒤이어 사용자 인터페이스(400)를 생성한다. 도 4b에 도시된 UI(400)는 도 4a에 도시된 허가권 요청(106)에 기반하여 생성된다.

[0039] 사용자 인터페이스(400)는 사용자에게 애플리케이션이 보안 자원들(122)에 대한 액세스를 요청했다고 설명하는 텍스트를 포함한다. 사용자 인터페이스(400)는 또한 허가권 요청(106) 시 애플리케이션(104)에 의해 요청된 다양한 허가권들을 기술하는 텍스트를 포함한다. 위에서 논의된 바와 같이, 이러한 정보는 콜백 함수를 통해 허가권 요청(106) 시 기술된 범위(108)와 관련된 허가권 제공자들(116)로부터 얻어질 수 있을 것이다. 허가권 제공자들(116)로부터 수신된 정보는 일 실시예에서 필드들(402A-402D) 안에 디스플레이된다.

[0040] 도 4b에 도시된 예에서, 예컨대, 문서 라이브러리에 대해 허가권 제공자(116)로부터 수신된 요청된 허가권을 기

술하는 데이터가 필드 402A에 보여질 수 있다. 사용자 프로파일에 대해 허가권 제공자(116)로부터 수신된 데이터는 필드 402B에 디스플레이될 수 있다. 캘린다에 대해 허가권 제공자(116)로부터 수신된, 요청된 허가권을 기술하는 데이터가 필드 402C에 디스플레이될 수 있다. 연락처에 대해 허가권 제공자(116)로부터 수신된 데이터는 필드 402B에 디스플레이될 수 있다. 현재의 사용자는 요청된 특권들을 부여하기 위해 UI 콘트롤(404B)을 선택할 수 있다. 다른 대안으로서, 현재의 사용자가 허가권 요청(106)을 거부하기 위해 UI 콘트롤(404A)을 선택할 수 있다.

[0041] 도 4b에 도시된 사용자 인터페이스는 다만 예일 뿐으로 더 많거나 더 적은 데이터가 제공될 수도 있다는 것을 이해해야 한다. 예를 들어 애플리케이션만의 요청(112)이 이루어졌다는 것을 나타내는 추가 필드들(402)이 제공될 수 있을 것이다. 또한, 제공된 데이터가 다른 방식으로, 혹은 도 4b에 도시된 것과 다른 UI 콘트롤들을 이용하여 제시될 수도 있을 것이다. 다른 변경들이 당업자에게는 자명할 것이다.

[0042] 도 5는 본 명세서에 개시된 일 실시예에서 런타임 자원 요청들을 처리하기 위해 사용되는 메커니즘의 양태들을 보여주는 네트워크도이다. 도 5에 도시된 예에서, 사용자(502) 및 애플리케이션(104)이 자원 서버(114)로 보안 자원들에 대한 요청들("자원 요청들(504)")을 일으킬 수 있다. 특히, 사용자(502)는 애플리케이션(104)의 사용 없이 문서 저장 시스템(102)을 직접 통하여, 보안 자원(122A)에 대한 자원 요청(504A)을 생성할 수도 있다. 마찬가지로, 애플리케이션(104)은 사용자(502)를 대신하지 않고 직접적으로, 보안 자원(122A)에 대한 자원 요청(504C)을 생성할 수도 있다. 또한, 사용자(502)는 애플리케이션(104) 및 사용자(502)에 의해 이루어지는 자원 요청(504B)을 생성하는데 애플리케이션(104)을 이용할 수도 있다.

[0043] 자원 요청(504)이 사용자(502)만에 의해 이루어지는지, 애플리케이션(104)만에 의해 이루어지는지, 또는 사용자(504)를 대신하여 애플리케이션(104)에 의해 이루어지는지를 판단하기 위하여, 적절한 인증 메커니즘이 사용될 수 있다. 그러한 메커니즘을 통해, 자원 요청(504A)이 사용자(502)만에 의해 이루어질 때 사용자 아이디(506A)가 자원 서버(114)로 제공된다. 자원 요청(504C)이 애플리케이션(104)만에 의해 이루어질 때 애플리케이션 아이디(506C)가 자원 서버(114)로 제공된다. 마찬가지로, 자원 요청(504B)이 사용자(502)를 대신한 애플리케이션(104)에 의해 이루어질 때, 애플리케이션 및 사용자 아이디들(506B)이 자원 서버(114)로 제공된다. 자원 요청들(504)이 이루어질 때 그러한 아이디들(506)을 자원 서버(114)로 제공하기 위한 적절한 프로토콜이 사용될 수 있다. 사용자(502) 및 애플리케이션(104)을 인증하고, 자원 요청(504)이 사용자(502)만에 의해, 애플리케이션(104)만에 의해, 혹은 사용자(502)를 대신한 애플리케이션(104)에 의해 이루어졌을 때 자원 서버(114)에 지시하기 위해 다른 메커니즘들 역시 사용될 수 있을 것이다.

[0044] 자원 요청(504)을 수신함에 따라, 자원 서버(114)는 자원 요청(504)이 사용자(502)에 의해 이루어졌는지, 애플리케이션(104)만에 의해 이루어졌는지, 또는 사용자(502)를 대신하여 애플리케이션(104)에 의해 이루어졌는지를 판단한다. 자원 서버(114)는 그런 다음, 허가권 데이터 저장부(120)로부터 자원 요청(504)이 수락될 수 있는지 혹은 거부되어야 하는지를 판단하기 위한 데이터를 검색한다. 자원 요청(504)이 애플리케이션(104)에 의해서만 이루어진 것이면, 자원 서버(114)는 사용자를 대신하는 것이 아닌 직접적인 호출을 통해 상기 애플리케이션(104)이 상기 보안 자원(122)에 액세스하도록 하는 허가권을 상술한 방식으로 부여받은 경우에만 상기 요청(504)을 수락한다. 사용자(502)를 대신하여 애플리케이션(104)에 의해 자원 요청(504)이 이루어진 경우, 상기 자원 서버(114)는 사용자(502)와 애플리케이션(104) 모두가 상기 요청된 액션을 수행하기 위한 허가권을 가진 경우에만 상기 요청(504)을 수락한다. 자원 서버(114)는 또한, 상기 보안 자원(122)에 대한 액션의 수행을 사용자(502), 애플리케이션(104), 또는 사용자(502)와 애플리케이션(114) 둘 모두에 귀속시키는 데이터를 히스토리 데이터 저장부(508)에 저장할 수도 있다. 이러한 프로세스들에 관한 추가 세부사항들이 도 6a-6b와 관련하여 이하에서 제공될 예정이다.

[0045] 도 6a-6b는 일 실시예에 따른 보안 자원들(122)에 대한 런타임 요청들(504)을 처리하기 위한 하나의 루틴(600)의 양태들을 보여주는 흐름도들이다. 루틴(600)은 자원 서버(114)가 자원 요청(504)을 수신하는 동작(602)에서 시작한다. 자원 요청(504)을 수신함에 따라, 상기 루틴(600)은 수신 요청(504)이 사용자(502)만을 대신하여 이루어졌는지 여부를 판단하는 동작(604)으로 진행한다. 요청(504)이 사용자(502)만을 대신하여 이루어졌으면, 루틴(600)은 동작(604)에서 동작(610)으로 진행한다.

[0046] 동작(610)에서 자원 서버(114)는 허가권 데이터 저장부(120)를 이용하여 요청을 한 사용자(502)가 수신된 자원 요청(504) 시 요청된 액션을 수행하기 충분한 특권을 가지는지를 판단하도록 한다. 사용자(502)가 충분한 특권을 가지지 않으면, 루틴(600)은 동작(612)에서 수신된 자원 요청(504)이 거부되는 동작(614)으로 진행한다. 루틴(600)은 이제 동작(614)에서 루틴이 종료되는 동작(620)으로 진행한다.

[0047] 사용자(502)가 충분한 특권을 가지면, 루틴(600)은 동작(612)에서 수신된 자원 요청(504) 시 요청된 액션이 수행되는 동작(616)으로 진행한다. 예를 들어 보안 자원(122)을 통해 읽기 동작, 쓰기 동작, 또는 다른 유형의 동작이 수행될 수 있을 것이다. 상기 액션이 완료되었으면, 루틴(600)은 자원 서버(114)가 히스토리 데이터 저장부(508) 안에 상기 수행된 액션을 사용자(502)에게 귀속시키는 데이터를 저장하는 동작(618)으로 진행한다. 예를 들어 사용자(502)가 보안 자원(122)을 통해 쓰기 동작을 수행했음을 나타내는 데이터가 저장될 수 있다. 동작(618)으로부터 루틴(600)은 그것이 종료되는 동작(620)으로 진행한다.

[0048] 만일, 동작(604)에서 자원 서버(114)가 수신된 자원 요청(504)이 사용자(502)만에 의해 이루어지지 않았다고 판단한 경우, 루틴(600)은 동작(606)으로 진행한다. 동작(606)에서 자원 서버(114)는 수신된 자원 요청(504)이 사용자(502)를 대신한 애플리케이션(140)에 의해 이루어졌는지 여부를 판단한다. 요청(504)이 사용자(502)만을 대신하여 이루어졌으면, 루틴(600)은 동작(606)에서 동작(622)으로 진행한다.

[0049] 동작(622)에서 자원 서버(114)는 허가권 데이터 저장부(120)를 이용하여 애플리케이션(104) 및 사용자(502) 둘 모두가 수신된 자원 요청(504) 시 요청된 액션을 수행하기 충분한 특권을 가지는지를 판단하도록 한다. 애플리케이션(104)이나 사용자(502) 어느 하나가 충분한 특권을 가지지 않으면, 루틴(600)은 동작(624)에서 수신된 자원 요청(504)이 거부되는 동작(614)으로 진행한다. 루틴(500)은 이제 동작(614)에서 루틴이 종료되는 동작(620)으로 진행한다.

[0050] 애플리케이션(104)과 사용자(502) 모두가 충분한 특권을 가지면, 루틴(600)은 동작(624)에서 수신된 자원 요청(504) 시 요청된 액션이 수행되는 동작(626)으로 진행한다. 상기 액션이 완료되었으면, 루틴(600)은 자원 서버(114)가 히스토리 데이터 저장부(508) 안에 상기 수행된 액션을 애플리케이션(104) 및 사용자(502) 둘 모두에게 귀속시키는 데이터를 저장하는 동작(628)으로 진행한다. 예를 들어 애플리케이션(104)이 사용자(502)를 대신하여 보안 자원(122)을 통해 삭제 동작을 수행했음을 나타내는 데이터가 저장될 수 있다. 동작(628)으로부터 루틴(600)은 그것이 종료되는 동작(620)으로 진행한다.

[0051] 만일, 동작(606)에서 자원 서버(114)가 수신된 자원 요청이 사용자(502) 및 애플리케이션(104) 둘 모두를 대신하여 이루어지지 않았다고 판단한 경우, 루틴(600)은 동작(606)으로부터 동작(608)으로 진행한다. 동작(608)에서 자원 서버(114)는 수신된 자원 요청(504)이 애플리케이션(104)만을 대신하여 이루어졌는지 여부를 판단한다. 수신된 자원 요청(504)이 애플리케이션(104)만을 대신하여 이루어지지 않았다면, 루틴(600)은 동작(608)으로부터, 수신된 자원 요청(504)이 거부되는 동작(614)으로 진행한다. 루틴(600)은 이제 동작(614)에서 루틴이 종료되는 동작(620)으로 진행한다.

[0052] 만일, 자원 서버(114)가 수신된 자원 요청(504)이 애플리케이션(104)만을 대신하여 이루어졌다고 판단한 경우, 루틴(600)은 동작(608)으로부터 동작(630)(도 6b에 도시됨)으로 진행한다. 동작 630에서, 자원 서버(114)는 애플리케이션(104)이 상기 수신된 자원 요청(504) 시 요청된 액션을 수행할 충분한 특권을 가지는지를 판단하기 위해 허가권 데이터 저장부(120)를 이용한다. 애플리케이션(104)이 충분한 특권을 가지지 않으면, 루틴(600)은 동작(632)에서 수신된 자원 요청(504)이 거부되는 동작(634)으로 진행한다. 루틴(600)은 이제 동작(634)에서 루틴이 종료되는 동작(640)으로 진행한다.

[0053] 애플리케이션(104)이 충분한 특권을 가지면, 루틴(600)은 동작(632)에서 수신된 자원 요청(504) 시 요청된 액션이 수행되는 동작(636)으로 진행한다. 상기 액션이 완료되었으면, 루틴(600)은 자원 서버(114)가 히스토리 데이터 저장부(508) 안에 상기 수행된 액션을 애플리케이션(104)에만 귀속시키는 데이터를 저장하는 동작(638)으로 진행한다. 동작(638)으로부터 루틴(600)은 그것이 종료되는 동작(640)으로 진행한다.

[0054] 도 7은 여기에 제시된 실시예들의 양태들을 구현할 수 있는 컴퓨팅 시스템의 예시적 컴퓨터 하드웨어 및 소프트웨어 구조를 보여주는 컴퓨터 구조도이다. 도 7에 도시된 컴퓨터 구조는 종래의 데스크탑, 랩탑 컴퓨터, 또는 서버 컴퓨터를 예시한 것으로, 본 명세서에 개시된 기능을 제공하기 위해 상술한 다양한 소프트웨어 구성요소들을 실행하는데 이용될 수 있다.

[0055] 도 7에 도시된 컴퓨터 구조는 중앙 처리 유닛(CPU)(702), RAM(random access memory)(714) 및 ROM(read only memory)(716)을 포함하는 시스템 메모리(708) 및 메모리(704)를 CPU(702)에 연결하는 시스템 버스(704)를 포함한다. 가령 시동 중에, 컴퓨터(700) 내 구성요소들 사이에서 정보를 전달하는 것을 돕는 기본 루틴들을 포함하는 기본 입출력 시스템(26)(BIOS)(미도시)은 ROM(716)에 저장된다. 컴퓨터(700)는 이하에서 보다 상세히 설명될 운영체제(718), 애플리케이션 프로그램들, 및 다른 프로그램 모듈들을 저장하기 위한 매스 저장 기기(710)를 더 포함한다.

[0056] 매스 저장 기기(710)는 버스(704)에 연결된 매스 저장 제어기(미도시)를 통해 CPU(702)에 연결된다. 매스 저장 기기(710) 및 그것의 관련 컴퓨터 판독 가능 저장 매체는 컴퓨터(700)에 비휘발성 저장부를 제공할 수 있다. 여기에 포함된 컴퓨터 판독 가능 저장 매체에 대한 내용은 하드 디스크나 CD-ROM 드라이브와 같은 매스 저장 기기를 언급하지만, 당업자는 컴퓨터 판독 가능 저장 매체가 컴퓨터(700)에 의해 처리될 수 있는 모든 이용가능한 컴퓨터 저장 매체일 수 있다는 것을 알 수 있을 것이다.

[0057] 한정하는 것이 아닌 예로서, 컴퓨터 판독 가능 저장 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈이나 기타 데이터 같은 정보의 저장을 위해 어떤 방법 또는 기술로 구현된 휘발성 및 비휘발성, 착탈형 및 비착탈형 매체를 포함할 수 있다. 예를 들어 컴퓨터 판독 가능 저장 매체는 RAM, ROM, EPROM, EEPROM, 플래시 메모리 또는 다른 반도체 메모리 기술, CD-ROM, DVD(digital versatile disks), HD-DVD, BLU-RAY 또는 다른 광학 저장부, 마그네틱 카세트, 마그네틱 테이프, 마그네틱 디스크 저장부 또는 다른 마그네틱 저장 소자, 또는 원하는 정보를 저장하는데 사용될 수 있고 컴퓨터(700)에 의해 액세스될 수 있는 어떤 다른 비일시적 매체를 포함하나, 그에 국한되지 않는다.

[0058] 본 명세서에 개시된 컴퓨터 판독 가능 매체는 통신 매체를 또한 포괄한다는 것을 예상할 수 있을 것이다. 통신 매체는 통상적으로 반송파나 다른 전송 메커니즘 같은 변조된 데이터 신호를 통해 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터를 구현하며 어떤 정보 전달 매체를 포함한다. "변조된 데이터 신호"라는 용어는 신호 안에 정보를 인코딩하기 위한 방식으로 세팅되거나 변경되는 신호의 특성들 중 한 개 이상을 가지는 신호를 의미한다. 한정하는 것이 아닌 예로서, 통신 매체는 유선 네트워크나 직접 유선 연결 같은 유선 매체, 및 청각, RF(radio frequency), 적외선 및 다른 무선 매체 같은 무선 매체를 포함한다. 상술한 것 중 어느 조합 역시 컴퓨터 판독 가능 매체의 범위 안에 포함될 수 있을 것이다. 컴퓨터 판독 가능 저장 매체는 통신 매체를 포괄하지 않는다.

[0059] 다양한 실시예들에 따르면 컴퓨터(700)는 네트워크(720)와 같은 네트워크를 통한 원격 컴퓨터들로의 논리 접속을 이용하여 네트워크화된 환경 안에서 동작할 수 있다. 컴퓨터(700)는 버스(704)에 연결된 네트워크 인터페이스 유닛(706)을 통해 네트워크(720)에 연결할 수 있다. 네트워크 인터페이스 유닛(706)은 다른 종류의 네트워크들 및 원격 컴퓨터 시스템들에 연결하는 데 사용될 수도 있다는 것을 이해해야 한다. 컴퓨터(700)는 또한 키보드, 마우스, 또는 전자 스타일러스(도 7에 도시되지 않음)를 포함하는 다수의 다른 장치들로부터의 입력을 수신하여 처리하기 위한 입/출력 제어기(712)를 포함할 수 있다. 마찬가지로 입/출력 제어기는 디스플레이 스크린, 프린터, 또는 다른 종류의 출력 기기(도 7에 역시 도시되지 않음)로 출력을 제공할 수 있다.

[0060] 위에서 간략히 언급한 바와 같이, 네트워킹된 데스크탑, 랩탑, 또는 서버 컴퓨터의 동작을 제어하기 적합한 운영체제를 포함하여 여러 프로그램 모듈들 및 데이터 파일들이 컴퓨터(700)의 매스 저장 기기(710) 및 RAM(714)에 저장될 수 있다. 매스 저장 기기(710) 및 RAM(714)은 또한 하나 이상의 프로그램 모듈들을 저장할 수 있다. 특히, 매스 저장 기기(710) 및 RAM(714)은 애플리케이션(104)이나 자원 서버(114) 또는 다른 종류의 프로그램이나 서비스와 같이, 상술한 기능을 제공하는 하나 이상의 소프트웨어 구성요소들을 저장할 수 있다. 매스 저장 기기(710) 및 RAM(714)은 본 명세서에 개시된 다른 프로그램 모듈들 및 데이터를 저장할 수도 있다.

[0061] 일반적으로 소프트웨어 애플리케이션들이나 모듈들은 CPU(702) 안으로 로딩되어 실행될 때, CPU(702) 및 전반적 컴퓨터(700)를 범용 컴퓨팅 시스템에서 본 명세서에 제시된 기능을 수행하도록 맞춤화된 특수 목적 컴퓨팅 시스템으로 변환할 수 있다. CPU(702)는 개별적으로나 집합적으로 임의 개의 상태들을 취할 수 있는 임의 개의 트랜지스터들이나 다른 개개 회로 요소들로 구성될 수 있다. 더 상세히 말하면, CPU(702)는 소프트웨어나 모듈들 안에 포함된 실행 가능 명령어들에 응하여 하나 이상의 유한 상태 머신으로서 동작할 수 있다. 이러한 컴퓨터 실행 가능 명령어들은 CPU(702)가 상태들 사이에서 어떻게 천이하는지를 특정하여 CPU(702)를 변형함으로써 CPU(702)를 구성하는 트랜지스터들이나 다른 개개 하드웨어 요소들을 물리적으로 변형시킬 수 있다.

[0062] 소프트웨어나 모듈들을 매스 저장 장치 상에서 인코딩하는 것 역시, 매스 저장 장치나 관련 컴퓨터 판독 가능 저장 메체의 물리적 구조를 변형시킬 수 있다. 물리적 구조의 구체적 변형은 이 내용의 각종 구현예들 내 다양한 요인들에 달려있을 수 있다. 그러한 요인들의 예들은 컴퓨터 판독 가능 저장 매체가 일차 저장부를 특징으로 하는지 이차 저장부를 특징으로 하는지 등의 여부를 불문하고 컴퓨터 판독 가능 저장 매체를 구현하는 데 사용되는 기술을 포함할 수 있으나 그에 국한되지 않는다. 예를 들어 컴퓨터 판독 가능 저장 매체가 반도체 기반 메모리로서 구현되는 경우 소프트웨어나 모듈들은 소프트웨어가 그 안에서 인코딩될 때 반도체 메모리의 물리적 상태를 변형시킬 수 있다. 예를 들어 소프트웨어는 반도체 메모리를 구성하는 트랜지스터들, 커패시터들, 또는 다른 개개 회로 요소들의 상태들을 변형시킬 수 있다.

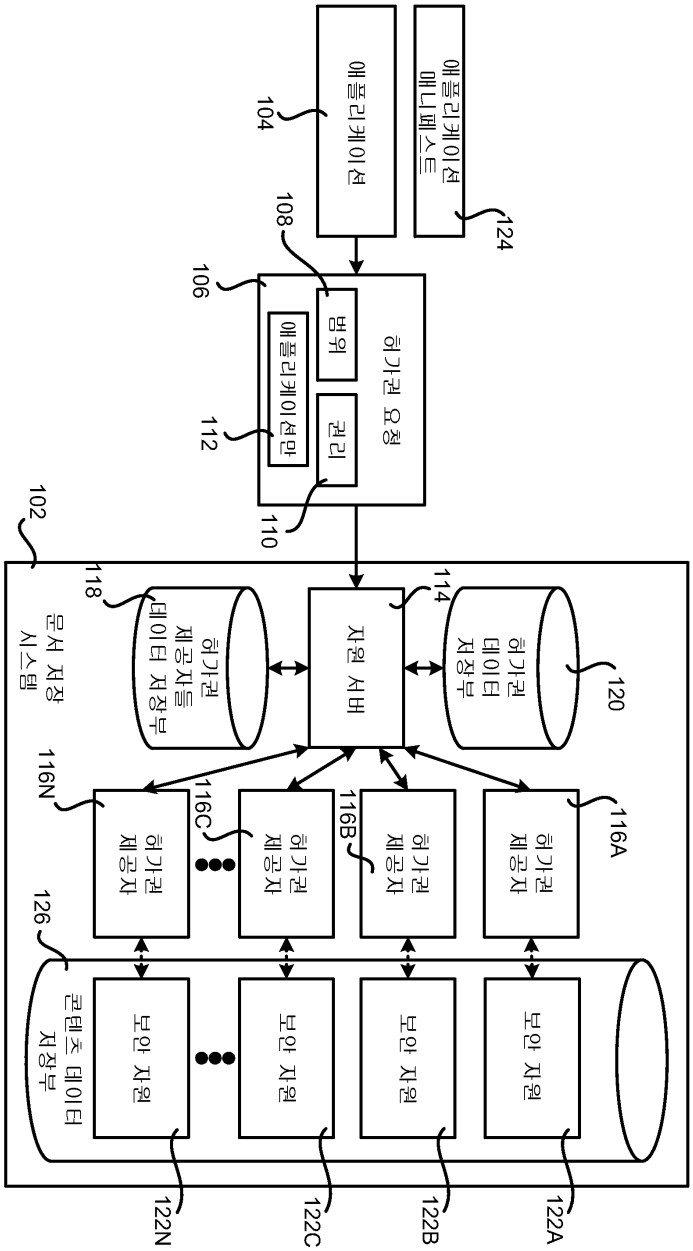
[0063] 다른 예로서 컴퓨터 판독 가능 저장 매체는 자기 또는 광 기술을 이용하여 구현될 수 있다. 그러한 구현예들에서 소프트웨어나 모듈들은 소프트웨어가 그 안에서 인코딩될 때 자기나 광 매체의 물리적 상태를 변형시킬 수 있다. 이러한 변형은 주어진 자기적 매체 내 특정 위치들의 자기적 특성들을 바꾸는 것을 포함할 수 있다. 이러한 변형은 또한 주어진 광 매체 내 특정 위치들의 물리적 특성들이나 특징들을 바꾸어 그 위치들의 광학적 특징들을 변화시키는 것을 포함할 수도 있다. 본 설명의 범위 및 사상에서 벗어나지 않으면서 물리적 매체의 다른 변형들이 가능하고, 상술한 예들은 이 논의를 수월하게 하기 위해서만 주어지는 것이다.

[0064] 상술한 것에 기반하여, 애플리케이션의 보안 자원에 대한 액세스를 허가하기 위한 기술들이 본 명세서에 개시되었다는 것을 알 수 있을 것이다. 여기에 제시된 주제가 컴퓨터 구조의 특징들, 방법적 행위들, 및 컴퓨터 판독 가능 매체에 특정되는 언어를 통해 위에서 기술되었지만, 첨부된 청구범위에 규정된 본 발명이 여기에 기술된 특정한 특징들, 행위들 또는 매체에 꼭 국한되는 것은 아니라는 것을 이해해야 한다. 오히려, 특정한 특징들, 행위들 및 매체들은 청구범위를 구현하는 예시적 형태들로서 개시된다.

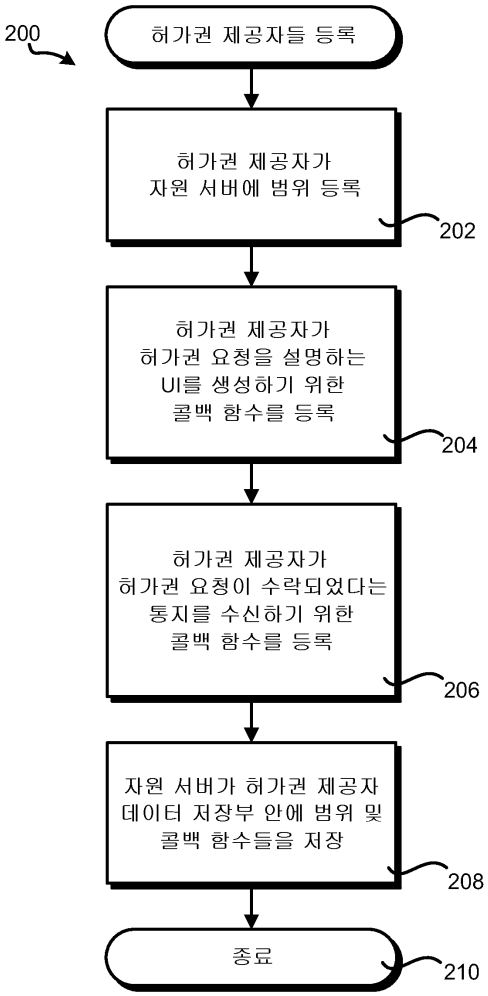
[0065] 상술한 주제는 단지 예시로서 제공되고 한정하는 것으로 해석되지 않아야 한다. 예시되고 기술된 전형적 실시예들 및 애플리케이션들을 따르지 않고 이하의 청구범위에 기술되는 본 발명의 진정한 사상 및 범위로부터 벗어나지 않으면서 여기에 기술된 발명 대상에 대한 다양한 변형 및 변화가 이루어질 수 있다.

도면

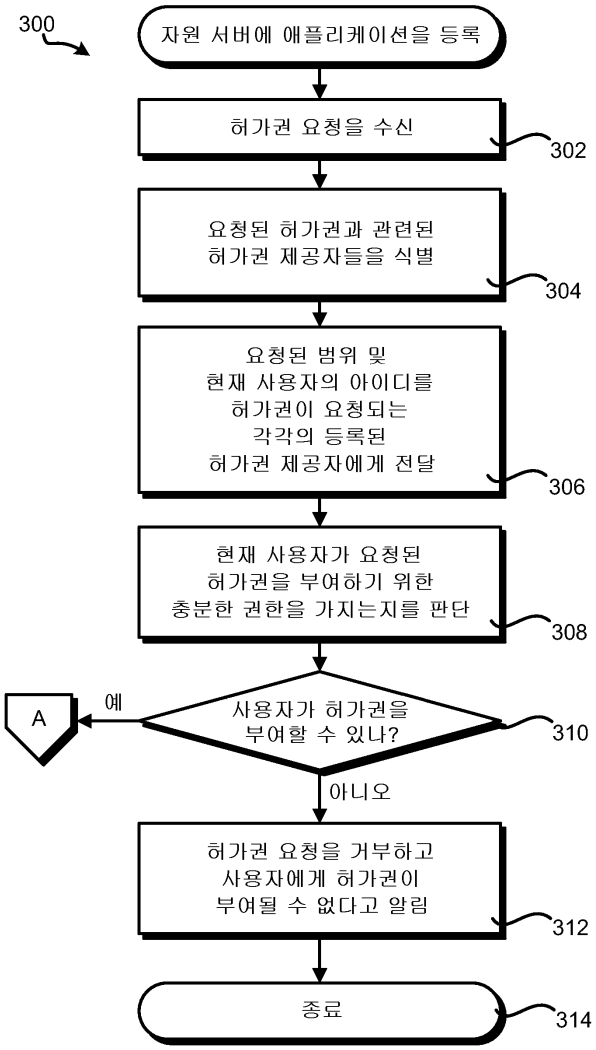
도면1


애플리케이션
104
애플리케이션 매니페스트
124
108
106
범위
권리
애플리케이션만
112
허가권 요청
110
102
문서 저장 시스템
118
허가권 제공자들 데이터 저장부
자원 서버
114
허가권 데이터 저장부
120
116N
116C
116B
116A
허가권 제공자
126
콘텐츠 데이터 저장부
보안 자원
122N
122C
122B
122A

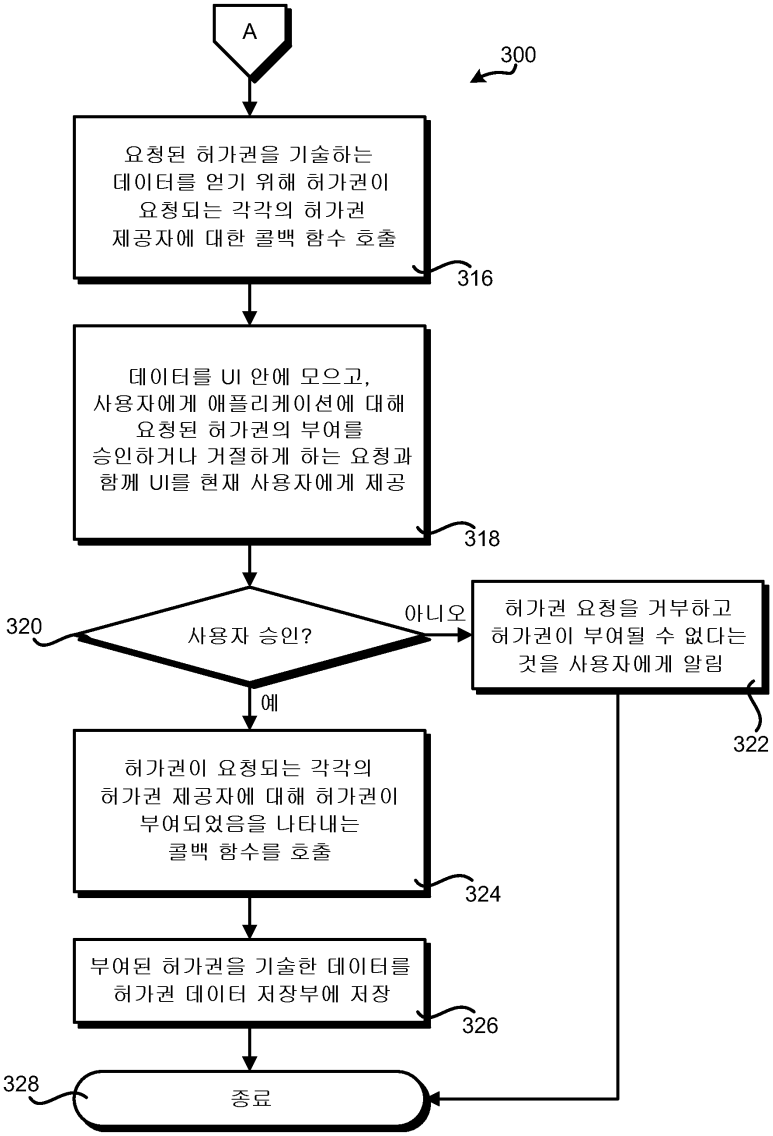
도면2


200
허가권 제공자들 등록
허가권 제공자가
자원 서버에 범위 등록
202
허가권 제공자가
허가권 요청을 설명하는
UI를 생성하기 위한
콜백 함수를 등록
204
허가권 제공자가
허가권 요청이 수락되었다는
통지를 수신하기 위한
콜백 함수를 등록
206
자원 서버가 허가권 제공자
데이터 저장부 안에 범위 및
콜백 함수들을 저장
208
종료
210

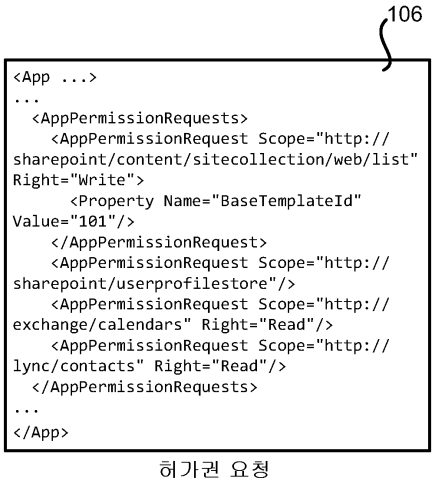
도면3a


300
자원 서버에 애플리케이션을 등록
허가권 요청을 수신
302
요청된 허가권과 관련된
허가권 제공자들을 식별
304
요청된 범위 및
현재 사용자의 아이디를
허가권이 요청되는
각각의 등록된
허가권 제공자에게 전달
306
현재 사용자가 요청된
허가권을 부여하기 위한
충분한 권한을 가지는지를 판단
308
사용자가 허가권을
부여할 수 있나?
310
예
A
아니오
허가권 요청을 거부하고
사용자에게 허가권이
부여될 수 없다고 알림
312
종료
314

도면3b

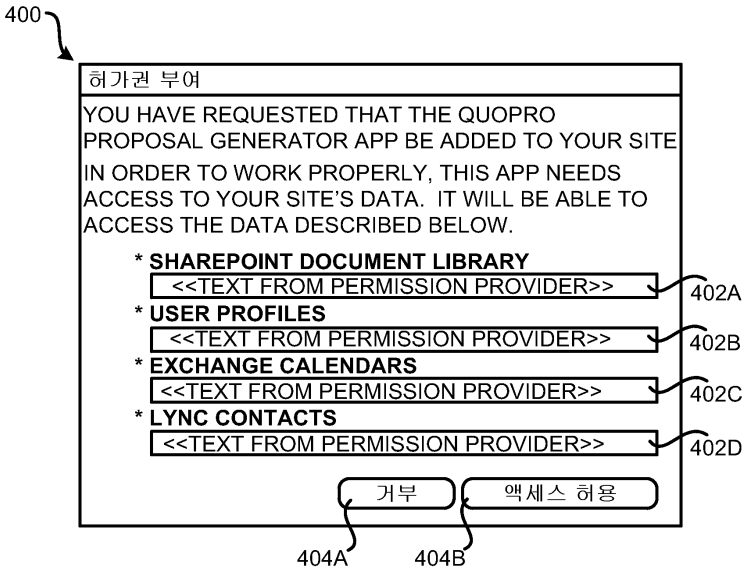


도면4a

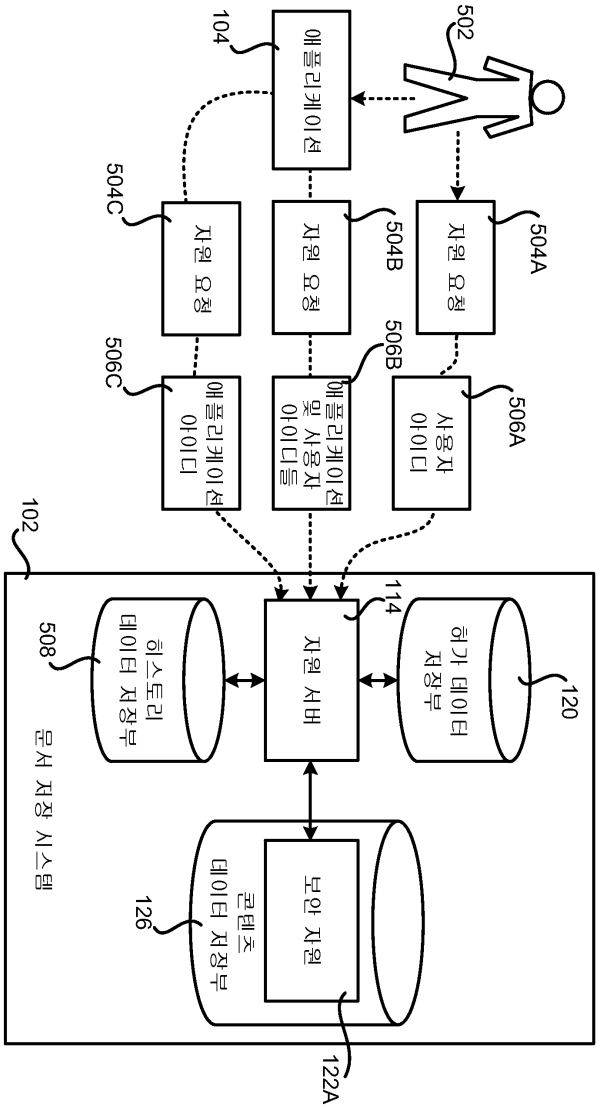


허가권 요청

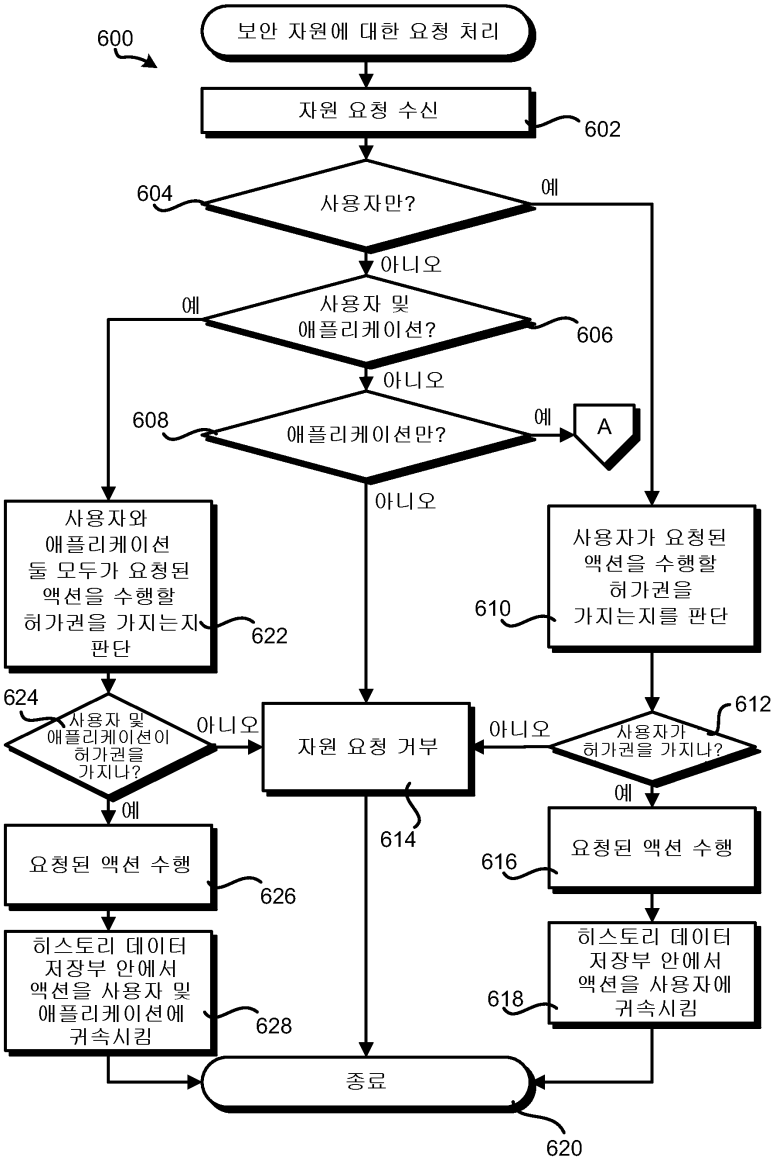
도면4b


400
허가권 부여
YOU HAVE REQUESTED THAT THE QUOPRO PROPOSAL GENERATOR APP BE ADDED TO YOUR SITE
IN ORDER TO WORK PROPERLY, THIS APP NEEDS ACCESS TO YOUR SITE'S DATA. IT WILL BE ABLE TO ACCESS THE DATA DESCRIBED BELOW.
* SHAREPOINT DOCUMENT LIBRARY
<<TEXT FROM PERMISSION PROVIDER>>
402A
* USER PROFILES
<<TEXT FROM PERMISSION PROVIDER>>
402B
* EXCHANGE CALENDARS
<<TEXT FROM PERMISSION PROVIDER>>
402C
* LYNC CONTACTS
<<TEXT FROM PERMISSION PROVIDER>>
402D
거부
액세스 허용
404A
404B

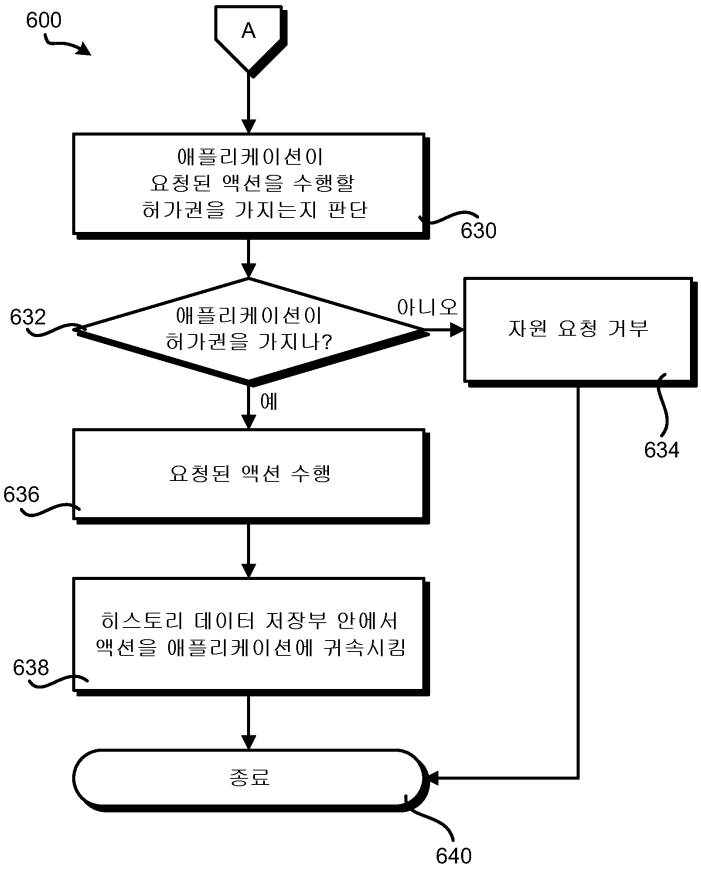
도면5


104
애플리케이션
502
504C
자원 요청
504B
자원 요청
504A
자원 요청
506C
애플리케이션 아이디
506B
애플리케이션 및 사용자 아이디들
506A
사용자 아이디
102
114
508
히스토리 데이터 저장부
자원 서버
허가 데이터 저장부
120
문서 저장 시스템
126
콘텐츠 데이터 저장부
보안 자원
122A

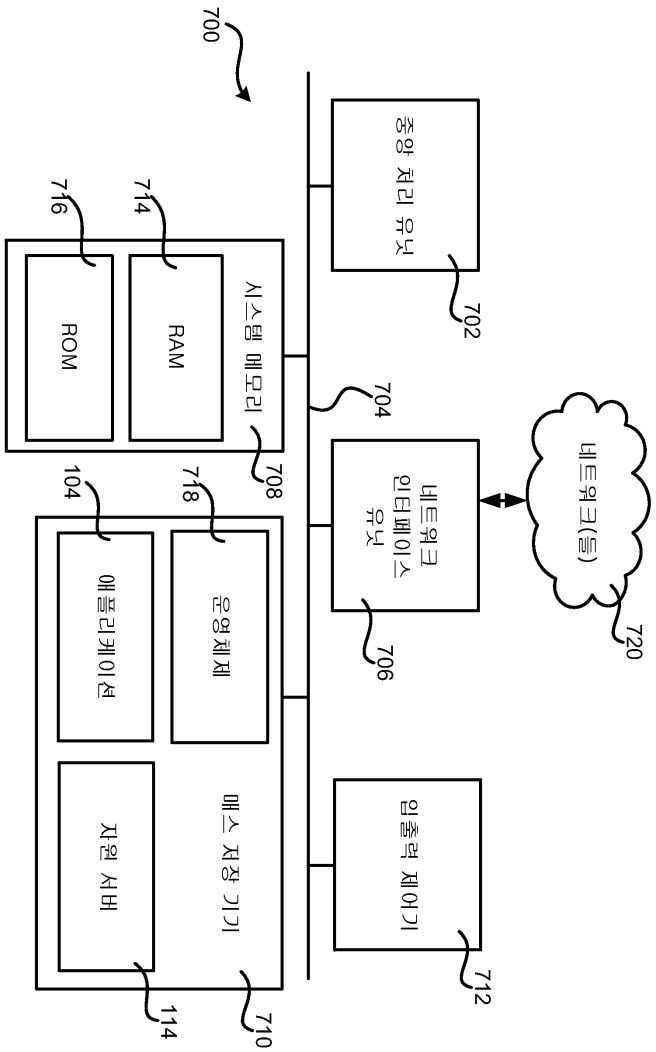
도면6a


600
보안 자원에 대한 요청 처리
자원 요청 수신
602
604
사용자만?
예
아니오
606
사용자 및 애플리케이션?
608
애플리케이션만?
A
사용자와 애플리케이션 둘 모두가 요청된 액션을 수행할 허가권을 가지는지 판단
622
624
사용자 및 애플리케이션이 허가권을 가지나?
자원 요청 거부
614
요청된 액션 수행
626
히스토리 데이터 저장부 안에서 액션을 사용자 및 애플리케이션에 귀속시킴
628
610
사용자가 요청된 액션을 수행할 허가권을 가지는지를 판단
612
사용자가 허가권을 가지나?
616
요청된 액션 수행
618
히스토리 데이터 저장부 안에서 액션을 사용자에 귀속시킴
종료
620

도면6b


600
A
애플리케이션이
요청된 액션을 수행할
허가권을 가지는지 판단
630
632
애플리케이션이
허가권을 가지나?
아니오
자원 요청 거부
634
예
요청된 액션 수행
636
히스토리 데이터 저장부 안에서
액션을 애플리케이션에 귀속시킴
638
종료
640

도면7


700
중앙 처리 유닛
702
시스템 메모리
704
ROM
716
RAM
714
708
네트워크 인터페이스 유닛
706
네트워크(들)
720
104
718
애플리케이션
운영체제
대스 저장 기기
자원 서버
114
710
입출력 제어기
712