



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년07월10일
(11) 등록번호 10-2833163
(24) 등록일자 2025년07월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) G06F 21/55 (2013.01)
G06F 21/60 (2013.01) G06F 21/62 (2013.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/44 (2013.01)
G06F 21/554 (2013.01)
(21) 출원번호 10-2021-7037327
(22) 출원일자(국제) 2020년04월13일
심사청구일자 2023년03월13일
(85) 번역문제출일자 2021년11월16일
(65) 공개번호 10-2022-0009388
(43) 공개일자 2022년01월24일
(86) 국제출원번호 PCT/US2020/027877
(87) 국제공개번호 WO 2020/236338
국제공개일자 2020년11월26일
(30) 우선권주장
16/415,690 2019년05월17일 미국(US)
(56) 선행기술조사문헌
KR1020190002241 A*
KR1020190015273 A*
US20120054847 A1*
US20190103968 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이선싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원
마이크로소프트 웨이
(72) 발명자
슈워츠 조나단 데이비드
미국 워싱턴주 98052-6399 레드몬드 원 마이크로
소프트 웨이 마이크로소프트 테크놀로지
라이선싱, 엘엘씨
타누스카야 아나스타시야
미국 워싱턴주 98052-6399 레드몬드 원 마이크로
소프트 웨이 마이크로소프트 테크놀로지
라이선싱, 엘엘씨
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 11 항

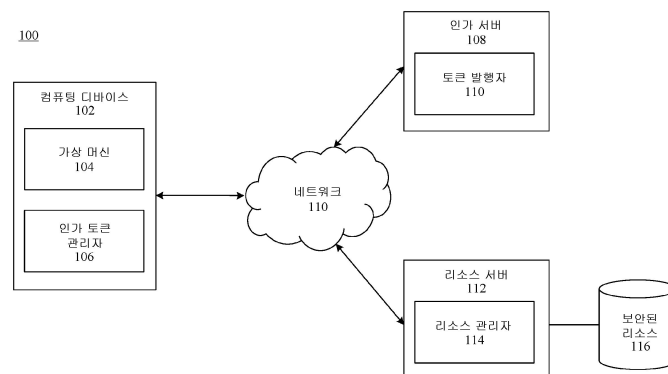
심사관 : 문남두

(54) 발명의 명칭 통합되고 격리된 애플리케이션에서 랜섬웨어 경감

(57) 요약

보안된 방식으로 리소스에 액세스할 수 있게 하기 위한 방법, 시스템, 장치 및 컴퓨터 프로그램 제품이 제공된다. 제 1 컴퓨팅 환경에서 실행되는 애플리케이션으로부터 토큰 요청이 제 2 컴퓨팅 환경에서 수신될 수 있다. 제 2 컴퓨팅 환경은 제 1 컴퓨팅 환경이 신뢰되지 않을 수 있다고 표시하는 신뢰 레벨을 수신된 토큰 요
(뒷면에 계속)

대표도



청에 할당할 수 있다. 토큰 요청은 신뢰 레벨과 함께 인가 서버에 제공되어 제 2 컴퓨팅 환경의 신뢰 레벨을 나타내는 신뢰 표시를 포함하는 인가 토큰을 생성할 수 있다. 제 2 컴퓨팅 환경에서 실행되는 애플리케이션이 인가 토큰을 리소스 관리자에게 전송하여 리소스에 액세스할 때, 리소스 관리자는 액세스를 제공하기 전에, 리소스의 백업을 생성하는 것과 같은 리소스를 보호하는 예방 조치를 수행하도록 구성될 수 있다.

(52) CPC특허분류

G06F 21/602 (2013.01)

G06F 21/604 (2013.01)

G06F 21/62 (2013.01)

H04L 9/3213 (2013.01)

H04L 9/3268 (2013.01)

명세서

청구범위

청구항 1

인가 토큰을 제공하기 위한 시스템으로서,

프로세서와,

상기 프로세서에 결합된 메모리를 포함하되, 상기 메모리는 상기 프로세서에 의해 실행될 때 동작들을 수행하는 컴퓨터 실행 가능 명령어를 포함하며, 상기 동작들은:

토큰 발행자에 의해 가상 머신과 인가 토큰 관리자를 포함하는 클라이언트 디바이스로부터 토큰 요청을 수신하는 것 - 상기 토큰 요청은 상기 가상 머신의 사용자에게 대한 아이덴티티 정보와 상기 인가 토큰 관리자에 의해 상기 토큰 요청에 할당된 신뢰 레벨을 포함하되, 상기 토큰 요청은, 상기 클라이언트 디바이스의 외부에 저장되는 보안된 리소스에 액세스하라는 애플리케이션에 의한 요청에 응답하여 상기 가상 머신에서 실행되는 상기 애플리케이션에 의해 생성되고, 상기 토큰 요청은 인가 토큰을 요청하고, 상기 신뢰 레벨은 상기 가상 머신의 동작 특성에 기초하여 상기 가상 머신이 신뢰할 수 있는지 여부를 표시하고, 상기 동작 특성은 상기 가상 머신에서 실행되는 운영 체제의 아이덴티티 또는 상기 애플리케이션의 아이덴티티 중 적어도 하나를 포함하고, 상기 가상 머신은 상기 토큰 요청을 상기 인가 토큰 관리자에게 제공함 - 과,

상기 토큰 발행자에 의해, 상기 토큰 발행자의 아이덴티티 서비스 또는 아이덴티티 공급자를 사용하여 상기 아이덴티티 정보를 검증하는 것 - 상기 아이덴티티 서비스 또는 상기 아이덴티티 공급자는 상기 사용자에게 대한 상기 아이덴티티 정보를 검증하도록 구성되고, 상기 아이덴티티 정보는 사용자 로그인 자격증명, 사용자 별칭, 계정 번호 또는 생체 인식 정보 중 적어도 하나를 포함함 - 과,

상기 토큰 발행자에 의해, 마킹된 인가 토큰을 생성하는 것 - 상기 마킹된 인가 토큰은 상기 가상 머신의 상기 신뢰 레벨을 표시하는 신뢰 표시를 포함하고, 상기 가상 머신에 의해 생성되는 상기 토큰 요청에 기반함 - 과,

상기 토큰 발행자에 의해, 상기 신뢰 표시를 포함하는 상기 마킹된 인가 토큰을 상기 인가 토큰 관리자에게 전송하는 것 - 상기 마킹된 인가 토큰은 상기 애플리케이션이 상기 보안된 리소스에 액세스하는 것을 결정하는 데 사용됨 -

을 포함하는,

시스템.

청구항 2

제1항에 있어서,

상기 신뢰 표시는, 상기 가상 머신의 상기 신뢰 레벨이 상기 가상 머신이 신뢰되는지 여부를 결정하는데 사용되는 임계 신뢰 레벨 미만임을 표시하는,

시스템.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 토큰 발행자는 상기 가상 머신에서 실행되는 상기 애플리케이션이 상기 클라이언트 디바이스의 하나 이상의 보안된 리소스에 액세스하는 것을 허용하도록 구성된 적어도 하나의 마킹된 인가 토큰을 생성하도록 구성되는,

시스템.

청구항 5

삭제

청구항 6

제4항에 있어서,

상기 마킹된 인가 토큰은 상기 애플리케이션이 상기 보안된 리소스에 관독 전용 액세스를 할 수 있게 하는 시스템.

청구항 7

보안된 방식으로 리소스에 액세스할 수 있게 하기 위한 방법으로서,

호스트 컴퓨팅 디바이스의 인가 토큰 관리자에서, 상기 호스트 컴퓨팅 디바이스 내에서 실행되는 가상 머신에서 실행되는 애플리케이션으로부터 토큰 요청을 수신하는 단계 - 상기 토큰 요청은 상기 호스트 컴퓨팅 디바이스의 외부에 저장된 보안된 리소스에 대한 액세스를 요청하고 상기 애플리케이션의 사용자에 대한 아이덴티티 정보를 포함함 - 와,

상기 토큰 요청이 상기 애플리케이션에 의해 개시되었다는 결정에 기초하여, 상기 인가 토큰 관리자가 상기 토큰 요청에 신뢰 레벨을 할당하는 단계 - 상기 신뢰 레벨은 상기 애플리케이션 또는 상기 가상 머신의 신뢰성을 표시하고 상기 가상 머신의 동작 특성에 기초하는 값이며, 상기 동작 특성은 상기 가상 머신에서 실행되는 운영 체제의 아이덴티티 또는 상기 애플리케이션의 아이덴티티 중 적어도 하나를 기술함 - 와,

토큰 발행자에 상기 토큰 요청 및 상기 신뢰 레벨을 제공하는 단계 - 상기 토큰 발행자는 상기 아이덴티티 정보를 검증하도록 구성된 아이덴티티 검증기를 포함함 - 와,

상기 인가 토큰 관리자에 의해 상기 토큰 발행자로부터 상기 신뢰 레벨을 표시하는 신뢰 표시를 포함하는 마킹된 인가 토큰을 획득하는 단계와,

상기 인가 토큰 관리자에 의해 상기 마킹된 인가 토큰을 상기 가상 머신으로 제공하는 단계와,

상기 가상 머신에 의해 상기 마킹된 인가 토큰을 상기 보안된 리소스에 액세스를 갖는 저장소 위치에 제공하는 단계 - 상기 저장소 위치는 상기 호스트 컴퓨팅 디바이스의 외부에 위치함 - 와,

상기 가상 머신에 의해, 상기 애플리케이션이 상기 보안된 리소스에 액세스하도록 허용되는지 여부를 표시하는 액세스 결정을 수신하는 단계를 포함하는,

방법.

청구항 8

삭제

청구항 9

제7항에 있어서,

상기 신뢰 표시는 상기 애플리케이션이 신뢰되지 않는다는 것을 표시하는,

방법.

청구항 10

제7항에 있어서,

상기 마킹된 인가 토큰을 수신하는 것에 응답하여 상기 보안된 리소스를 보호하기 위해 상기 저장소 위치에서 예방 조치를 수행하는 단계를 더 포함하는,

방법.

청구항 11

제10항에 있어서,

상기 예방 조치는 상기 마킹된 인가 토큰을 수신하는 것에 응답하여 상기 보안된 리소스의 백업의 생성을 포함하는,

방법.

청구항 12

제10항에 있어서,

상기 마킹된 인가 토큰을 수신하는 것에 응답하여, 상기 저장소 위치에 의해, 상기 보안된 리소스에의 판독 전용 액세스를 승인하는 단계를 더 포함하는,

방법.

청구항 13

제7항에 있어서,

상기 저장소 위치는,

상기 마킹된 인가 토큰을 수신하는 것과,

상기 마킹된 인가 토큰으로부터 상기 신뢰 표시를 추출하는 것과,

상기 추출된 신뢰 표시에 기초하여 예방 조치가 수행되어야 한다고 결정하는 것

에 응답하여 상기 예방 조치를 수행하는,

방법.

청구항 14

삭제

청구항 15

컴퓨터 프로그램 명령어가 기록된 컴퓨터 판독 가능 저장 매체로서,

프로세서로 하여금 제7항 및 제9항 내지 제13항 중 어느 한 항의 방법을 수행할 수 있게 하기 위한 컴퓨터 프로그램을 포함하는,

컴퓨터 판독 가능 저장 매체.

발명의 설명**배경 기술**

[0001]

격리된 컴퓨팅 배열에서, 애플리케이션은 컴퓨팅 호스트의 메인 컴퓨팅 환경으로부터 부분적으로 또는 완전히 격리된 환경에서 실행될 수 있다. 이러한 격리된 배열은 애플리케이션에 의해 호스트 환경의 리소스에 액세스하는 것을 제한 및/또는 방지함으로써 호스트 환경에 추가 보안을 제공할 수 있다. 많은 경우에 있어서, 격리된 환경에서 실행되는 애플리케이션은 신뢰될 수 없거나 또는 악의적인 활동에 취약할 위험이 더 높아질 수 있으며, 그런 까닭에 보안 관점에서 애플리케이션과 호스트 환경 간의 격리 장벽은 더 중요해진다. 다시 말해서, 악성 코드가 애플리케이션의 격리된 환경에서 실행되더라도, 호스트 환경에 미치는 위험은 격리 장벽으로 인해 최소화될 수 있다.

[0002]

그러나, 사용자의 경험을 강화하기 위해, 이를테면 격리된 환경의 애플리케이션에 의한 호스트 환경의 파일로의 액세스를 허용함으로써, 의도적으로 격리 장벽에서 특정 구멍이 존재할 수 있다. 격리 장벽에서 이러한 구멍은 격리된 환경과 호스트 환경 간의 통합을 개선할 수 있지만, 사용자 경험을 강화하려는 이러한 걸보기에 무해한 시도는 그럼에도 불구하고 호스트 환경에 대한 보안 취약성을 불러일으킬 수 있다. 예를 들어, 격리된 환경에

진입할 수 있는 랜섬웨어라고 하는 악성 코드는 호스트 환경에 저장된 사용자의 개인 데이터를 공격자만 알고 있는 암호화 키로 암호화할 수 있을 수 있다. 이러한 상황에서, 사용자는 자신의 데이터에 액세스할 수 있는 자기의 능력을 되찾기 위해 공격자에게 몸값을 지불해야 한다. 따라서 애플리케이션이 격리되어 있을 수 있더라도, 격리 장벽에 있는 구멍은 여전히 이러한 취약점 및 다른 유형의 취약점을 초래할 수 있다.

발명의 내용

[0003] 본 요약은 아래의 상세한 설명에서 추가로 설명되는 개념의 선택을 단순화된 형태로 소개하기 위해 제공된다. 본 요약은 청구된 주제의 주요 특징 또는 필수 기능을 식별하려는 것이 아니며, 청구된 주제의 범위를 제한하는데 사용하려는 것도 아니다.

[0004] 보안된 방식으로 리소스로의 액세스를 가능하게 하기 위한 방법, 시스템, 장치 및 컴퓨터 프로그램 제품이 제공된다. 제 1 컴퓨팅 환경(예를 들어, 가상 머신)에서 실행되는 애플리케이션으로부터의 토큰 요청은 제 2 컴퓨팅 환경(예를 들어, 호스트 컴퓨팅 환경)에서 수신될 수 있다. 호스트 컴퓨팅 환경은 제 1 컴퓨팅 환경이 신뢰되어서는 안 된다고 표시하는 신뢰 레벨과 같은 신뢰 레벨을 수신된 토큰 요청에 할당할 수 있다. 신뢰 레벨과 함께 토큰 요청은 토큰의 아이덴티티 정보를 검증하고 신뢰 표시를 포함하는 인가 토큰(authorization token)을 생성할 수 있는(예를 들어, 인가 서버 상의) 토큰 발행자에게 제공될 수 있다. 신뢰 표시는 예를 들어, 제 2 컴퓨팅 환경의 신뢰 레벨을 표시할 수 있다. 호스트 컴퓨팅 환경은 인가 토큰을 획득하고 이것을 애플리케이션에 제공할 수 있다. 제 2 컴퓨팅 환경에서 실행되는 애플리케이션이 인가 토큰을 리소스 관리자에게 전송하여 리소스에 액세스할 때, 리소스 관리자는 액세스를 제공하기 전에, 이를테면 리소스의 백업을 생성하기 전에 예방 조치를 수행하도록 구성될 수 있다.

[0005] 본 발명의 추가 특징 및 장점뿐만 아니라 다양한 실시예의 구조 및 동작은 첨부 도면을 참조하여 아래에서 상세히 설명된다. 본 발명은 본 명세서에서 설명된 특정 실시예로 제한되지 않는다는 것에 유의한다. 이러한 실시예는 본 명세서에서 예시적인 목적으로만 제시된다. 추가 실시예는 본 명세서에 포함된 교시에 기초하여 관련 기술 분야(들)의 통상의 기술자에게 명백할 것이다.

도면의 간단한 설명

[0006] 본 명세서에 포함되고 명세서의 일부를 형성하는 첨부 도면은 본 출원의 실시예를 예시하며, 상세한 설명과 함께, 더 나아가 실시예의 원리를 설명하고 관련 기술분야의 통상의 기술자가 실시예를 만들고 사용할 수 있도록 하는 역할을 한다.

도 1은 예시적인 실시예에 따른, 보안된 방식으로 리소스로의 액세스를 제공하기 위한 시스템의 블록도를 도시한다.

도 2는 예시적인 실시예에 따른, 신뢰 표시를 포함하는 인가를 애플리케이션에 제공하기 위한 방법의 흐름도를 도시한다.

도 3은 예시적인 실시예에 따른, 보안된 방식으로 네트워크 리소스로의 액세스를 제공하기 위한 시스템의 블록도를 도시한다.

도 4는 예시적인 실시예에 따른, 신뢰 표시를 포함하는 인가 토큰을 생성하기 위한 방법의 흐름도를 도시한다.

도 5는 예시적인 실시예에 따른, 리소스를 보호하는 예방 조치를 수행하기 위한 방법의 흐름도를 도시한다.

도 6은 예시적인 실시예에 따른, 보안된 방식으로 로컬 리소스로의 액세스를 제공하기 위한 시스템의 블록도를 도시한다.

도 7은 예시적인 실시예를 구현하는 데 사용될 수 있는 예시적인 컴퓨팅 디바이스의 블록도를 도시한다.

본 발명의 특징 및 장점은 같은 참조 문자가 전체에 걸쳐 대응하는 요소를 식별하는 도면과 함께 제시될 때 아래에서 제시된 상세한 설명으로부터 더욱 명백해질 것이다. 도면에서, 같은 참조 번호는 일반적으로 동일한, 기능적으로 유사한 및/또는 구조적으로 유사한 요소를 나타낸다. 요소가 처음 나오는 도면은 대응하는 참조 번호의 가장 왼쪽 숫자(들)에 의해 표시된다.

발명을 실시하기 위한 구체적인 내용

[0007] I. 소개

- [0008] 본 명세서 및 첨부 도면은 본 발명의 특징을 포함하는 하나 이상의 실시예를 개시한다. 본 발명의 범위는 개시된 실시예로 제한되지 않는다. 개시된 실시예는 본 발명을 예시하는 것일 뿐이며, 개시된 실시예의 변형된 버전 또한 본 발명에 포함된다. 본 발명의 실시예는 본 명세서에 첨부된 청구항에 의해 정의된다.
- [0009] 명세서에서 "일 실시예", "실시예", "예시적인 실시예" 등을 언급하는 것은 설명된 실시예가 특정 특징, 구조 또는 특성을 포함할 수 있지만, 모든 실시예가 반드시 특정 기능, 구조 또는 특성을 포함하지 않을 수 있다는 것을 시사한다. 더욱이, 이러한 문구는 반드시 동일한 실시예를 언급하는 것은 아니다. 또한, 특정 특징, 구조 또는 특성이 예시적인 실시예와 관련하여 설명될 때, 이것은 명시적으로 설명되지 않은 다른 실시예와 관련하여 그러한 특징, 구조 또는 특성에 영향을 미치는 관련 기술분야의 통상의 기술자의 지식 범위 내에 있다고 생각된다.
- [0010] 논의에서, 달리 언급되지 않는 한, 본 개시내용의 예시적인 실시예의 특징 또는 특징들의 조건 또는 관계 특성을 수식하는 "실질적으로" 및 "약"과 같은 형용사는 조건 또는 특징이 이것이 의도되는 애플리케이션에 대한 실시예의 동작에 용인 가능한 허용 오차 내로 정의된다는 것을 의미하는 것으로 이해된다.
- [0011] 다수의 예시적인 실시예가 다음과 같이 설명된다. 본 명세서에 제공된 임의의 섹션/하위 섹션 제목은 제한하려는 의도된 것이 아니라는 것을 유의한다. 실시예는 본 문서 전체에 걸쳐 설명되며, 임의의 유형의 실시예는 임의의 섹션/하위 섹션에 포함될 수 있다. 뿐만 아니라, 임의의 섹션/하위 섹션에 개시된 실시예는 임의의 방식으로 동일한 섹션/하위 섹션 및/또는 다른 섹션/하위 섹션에서 설명된 임의의 다른 실시예와 결합될 수 있다.
- [0012] II. 예시적 구현
- [0013] 격리된 컴퓨팅 배열에서, 애플리케이션은 컴퓨팅 호스트의 메인 컴퓨팅 환경으로부터 부분적으로 또는 완전히 격리된 환경에서 실행될 수 있다. 이러한 격리된 배열은 애플리케이션에 의해 호스트 환경의 리소스에 액세스하는 것을 제한 및/또는 방지함으로써 호스트 환경에 추가 보안을 제공할 수 있다. 많은 경우에 있어서, 격리된 환경에서 실행되는 애플리케이션은 신뢰될 수 없거나 또는 악의적인 활동에 취약할 위험이 더 높아질 수 있으며, 그런 까닭에 보안 관점에서 애플리케이션과 호스트 환경 간의 격리 장벽은 더 중요해진다. 다시 말해서, 악성 코드가 애플리케이션의 격리된 환경에서 실행되더라도, 호스트 환경에 미치는 위험은 격리 장벽으로 인해 최소화될 수 있다.
- [0014] 그러나, 사용자의 경험을 강화하기 위해, 이룰테면 격리된 환경의 애플리케이션에 의한 호스트 환경의 파일로의 액세스를 허용함으로써, 의도적으로 격리 장벽에서 특정 구멍이 존재할 수 있다. 격리 장벽에서 이러한 구멍은 격리된 환경과 호스트 환경 간의 통합을 개선할 수 있지만, 사용자 경험을 강화하려는 이러한 겉보기에 무해한 시도는 그럼에도 불구하고 호스트 환경에 대한 보안 취약성을 불러일으킬 수 있다. 예를 들어, 격리된 환경에 진입할 수 있는 랜섬웨어라고 하는 악성 코드는 호스트 환경에 저장된 사용자의 개인 데이터를 공격자만 알고 있는 암호화 키로 암호화할 수 있을 수 있다. 이러한 상황에서, 사용자는 자신의 데이터에 액세스할 수 있는 자기의 능력을 되찾기 위해 공격자에게 몸값을 지불해야 한다. 따라서 애플리케이션이 격리되어 있을 수 있더라도, 격리 장벽에 있는 구멍은 여전히 이러한 취약점 및 다른 유형의 취약점을 초래할 수 있다.
- [0015] 본 명세서에 설명된 실시예는 신뢰성 있는 방식으로 리소스에 액세스할 수 있게 하는 시스템을 제공함으로써 이러한 문제 및 다른 문제를 해결한다. 예시적인 시스템에서, 그로부터 적어도 부분적으로 격리된 다른 환경(예를 들어, 제 1 환경의 가상 머신에서 실행되는 애플리케이션)으로부터 토큰 요청을 수신하는 제 1 환경은 신뢰 표시를 포함하는 인가 토큰을 획득할 수 있다. 신뢰 표시는 토큰 요청이 개시된, 악의적인 활동에 취약할 수 있는 신뢰성 없는 환경을 포함할 수 있는, 환경의 신뢰 레벨을 나타낼 수 있다. 애플리케이션이 인가 토큰을 사용하여 신뢰성 있는 리소스에 액세스하려고 시도할 때, 리소스 공급자는 예방 조치를 취할 수 있다.
- [0016] 이러한 방식으로, 리소스는 악의적인 활동 또는 악의적인 코드, 이룰테면 권한 없는 엔티티가 사용자의 리소스(예를 들어, 데이터 또는 서비스)에 접근하려고 시도하는 임의의 다른 유형의 맬웨어, 악성 코드 또는 위반에 대해 보호될 수 있다. 예를 들어, 공격자가 몸값을 모으려는 시도로 사용자의 데이터를 암호화하려고 시도하더라도, 공격자가 인가 토큰에 포함된 신뢰 표시에 기초한 데이터에 액세스할 때 사용자 리소스의 백업 복사본이 자동으로 생성될 수 있다. 공격자가 액세스할 수 없는 방식으로 저장 및/또는 암호화될 수 있는 사용자의 리소스의 백업 복사본은 나중에 사용자에게 의해 복원될 수 있어 사용자는 공격자에게 몸값을 지불할 필요가 없다. 이와 같이, 덜 신뢰성 있는 컴퓨팅 환경의 악의적인 활동에 기인한 피해가 줄어들거나 완전히 방지될 수 있다.
- [0017] 본 명세서에서 설명된 바와 같이 보안된 방식으로 리소스에 액세스할 수 있게 하는 것은 네트워크 및/또는 네트워크에 연결된 리소스(예를 들어, 컴퓨팅 디바이스, 저장 디바이스 등)의 보안을 개선하는 것을 비롯한 수많은

장점을 갖는다. 예를 들어, 신뢰 표시를 포함하는 인가 토큰을 제공함으로써, 인가 토큰을 수신하는 것에 응답하여 리소스로의 액세스를 제공할 수 있는 리소스 제공자(네트워크를 통해 액세스 가능한 로컬 리소스 제공자 또는 리소스 서버일 수 있음)는 리소스를 보호하는 하나 이상의 예방 조치, 이를테면 리소스의 백업 복사본 만들기, 액세스의 범위 제한(예를 들어, 판독/기입 액세스 대신에 판독 전용 액세스만 제공), 강화된 인증 절차의 수행(예를 들어, 이중 인증(two-factor authentication)) 또는 다른 예방 조치를 취할 수 있다. 결과적으로, 덜 안전한 환경으로 간주되는 환경으로부터 개시되는 악의적인 활동에 대해 리소스가 보호될 수 있다. 뿐만 아니라, 리소스 제공자는 그 안에 내장된 신뢰 표시를 포함하는 인증 토큰(authentication token)을 수신할 수 있기 때문에, (예를 들어, 특정 애플리케이션이 이러한 인가 토큰으로 비정상적인 개수의 리소스에 액세스하는 경우) 리소스 제공자는 비정상적인 네트워크 활동의 존재를 검출하도록 구성될 수 있다. 결과적으로, 네트워크에 걸쳐서 및/또는 네트워크에 연결된 리소스 내에서 발생하는 악의적인 활동이 본 명세서에서 설명된 바에 따라 억제, 감소 및/또는 방지될 수 있다.

[0018] 예시적인 실시예는 다음과 같이 보안된 방식으로 리소스로의 액세스를 제공하기 위한 시스템 및 방법에 대해 설명된다. 예를 들어, 도 1은 예시적인 실시예에 따른, 시스템(100)의 블록도를 도시한다. 도 1에 도시된 바와 같이, 시스템(100)은 네트워크(110)에 의해 통신 가능하게 연결된 컴퓨팅 디바이스(102), 인가 서버(108) 및 리소스 서버(112), 및 리소스 서버(112)에 연결된 보안된 리소스(secured resource)(116)를 포함한다. 시스템(100)은 도 1에 예시된 것을 비롯한 임의의 수의 컴퓨팅 디바이스 및/또는 서버를 포함하고 명시적으로 예시되지 않은 하나 이상의 추가 디바이스를 선택적으로 포함할 수 있다. 도 1에 도시된 바와 같이, 컴퓨팅 디바이스(102)는 그 안에서 호스팅되는 가상 머신(104), 및 인가 토큰 관리자(106)를 포함한다. 아래에서 더 자세히 설명되는 바와 같이, 인가 토큰 관리자(106)는 가상 머신(104)에서 실행되는 애플리케이션으로부터 토큰 요청을 수신하고, 신뢰 표시가 있는 인가 토큰을 획득하고, 신뢰 표시를 포함하는 인가 토큰을 가상 머신(104)의 애플리케이션에 제공하도록 구성될 수 있다. 인가 서버(108)는 토큰 발행자(110)를 포함한다. 리소스 서버(112)는 리소스 관리자(114)를 포함한다. 도 1이 가상 머신(104)에서 실행되는 애플리케이션과 관련하여 설명되지만, 이러한 구현은 제한하는 것으로 의도되지 않는다. 나중에 설명되는 바와 같이, 토큰 요청이 유래할 수 있는 다른 유형의 부분적으로 및/또는 완전히 격리된 컴퓨팅 환경이 또한 고려된다. 시스템(100)은 다음과 같이 추가적으로 설명된다.

[0019] 네트워크(110)는 근거리 네트워크(local area network)(LAN), 광역 네트워크(Wide Area Network)(WAN), 개인 영역 네트워크(Personal Area Network)(PAN), 인터넷과 같은 통신 네트워크의 조합, 및/또는 또는 가상 네트워크 중 임의의 하나 이상을 포함할 수 있다. 예시적인 구현에서, 컴퓨팅 디바이스(102), 인가 서버(108), 리소스 서버(112), 및/또는 보안된 리소스(116)는 네트워크(110)를 통해 서로 통신 가능하게 연결될 수 있다. 구현에서, 컴퓨팅 디바이스(102), 인가 서버(108), 리소스 서버(112) 및/또는 보안된 리소스(116) 중 임의의 하나 이상은 하나 이상의 애플리케이션 프로그래밍 인터페이스(application programming interface)(API)를 통해 및/또는 다른 인터페이스 및/또는 기술에 따라 통신할 수 있다. 컴퓨팅 디바이스(102), 인가 서버(108), 리소스 서버(112), 및/또는 보안된 리소스(116)는 서로 통신을 가능하게 하는 적어도 하나의 네트워크 인터페이스를 각각 포함할 수 있다. 유선 또는 무선의 이러한 네트워크 인터페이스의 예는 IEEE 802.11 무선 LAN(wireless LAN)(WLAN) 무선 인터페이스, 마이크로웨이브 액세스를 위한 전세계 상호 운용성(Worldwide Interoperability for Microwave Access)(Wi-MAX) 인터페이스, 이더넷 인터페이스, 범용 직렬 버스(Universal Serial Bus)(USB) 인터페이스, 셀룰러 네트워크 인터페이스, 블루투스(Bluetooth)TM 인터페이스, 근거리 통신(near field communication)(NFC) 인터페이스 등을 포함한다. 네트워크 인터페이스의 추가 예는 본 명세서의 다른 곳에서 설명된다.

[0020] 컴퓨팅 디바이스(102)는 그 안에서 또는 네트워크(110)를 통한 하나 이상의 다른 컴퓨팅 디바이스를 통해 실행, 호스팅 및/또는 저장될 수 있는 하나 이상의 애플리케이션, 운영 체제, 가상 머신, 저장 디바이스 등을 포함할 수 있는 한 명 이상의 사용자(예를 들어, 개별 사용자, 가족 사용자, 기업 사용자, 정부 사용자 등)의 임의의 컴퓨팅 디바이스를 포함한다. 일부 예에서, 컴퓨팅 디바이스(102)는 본 명세서에 설명된 바와 같이, 인증 서버(108) 및/또는 리소스 서버(112)와 같은 하나 이상의 서버 디바이스에 액세스하여 하나 이상의 보안된 리소스(116)에 액세스할 수 있다. 컴퓨팅 디바이스(102)는 수십, 수백, 수천, 수백만, 또는 훨씬 더 많은 수의 컴퓨팅 디바이스를 비롯한 임의의 수의 컴퓨팅 디바이스를 포함할 수 있다. 컴퓨팅 디바이스(102)의 컴퓨팅 디바이스는 각각 이동 컴퓨터 또는 이동 컴퓨팅 디바이스(예를 들어, 마이크로소프트[®] 서피스(Surface)[®] 디바이스, 개인 휴대 정보 단말기(personal digital assistant)(PDA), 랩톱 컴퓨터, 노트북 컴퓨터, 애플 아이패드(Apple iPad)TM와 같은 태블릿 컴퓨터, 넷북 등), 이동 전화, 웨어러블 컴퓨팅 디바이스 또는 다른 유형의 이동 디바이스, 또는 데스크톱 컴퓨터 또는 PC(personal computer), 또는 서버와 같은 고정 컴퓨팅 디바이스를 비롯한 임의

의 유형의 고정 또는 이동 컴퓨팅 디바이스일 수 있다. 컴퓨팅 디바이스(102)는 물리적 머신으로 제한되지 않고, 가상 머신과 같은 다른 유형의 머신 또는 노드를 포함할 수 있다. 컴퓨팅 디바이스(102)는 각각 API를 통해 및/또는 다른 메커니즘에 의해 인가 서버(108) 및/또는 리소스 서버(112)와 인터페이스할 수 있다. 임의의 수의 프로그램 인터페이스가 존재할 수 있다는 것을 유의한다.

[0021] 인가 서버(108)는 하나 이상의 인가 토큰을 그러한 토큰을 요청하는 네트워크(110)의 컴퓨팅 디바이스에 발행하기 위한 임의의 컴퓨팅 디바이스, 서버, 및/또는 서비스를 포함할 수 있다. 아래에서 더 자세히 설명되는 바와 같이, 인가 토큰은 컴퓨팅 디바이스, 컴퓨팅 환경 및/또는 애플리케이션이 리소스에 액세스할 수 있게 하는 임의의 객체(예를 들어, 한 세트의 데이터)를 포함할 수 있다. 예를 들어, 인가 토큰은 토큰에 대한 식별자, 연관된 로그인 세션에 대한 식별자, 액세스를 요청하는 애플리케이션에 대한 식별자, 액세스를 요청하는 애플리케이션의 사용자에게 대한 사용자 식별자 및 인가 토큰에 의해 제공된 하나 이상의 특권의 표시 중 하나 이상을 포함하는 파일 또는 다른 객체일 수 있다.

[0022] 일부 예에서, 인가 서버(108)는 이것으로 제한되는 것은 아니지만, 사용자 로그인 자격증명(예를 들어, 사용자 이름 및/또는 비밀번호), 사용자 별칭, 계정 번호, 생체 인식 정보 또는 리소스로서의 액세스를 보호하는 데 사용할 수 있는 임의의 다른 정보 또는 자격증명을 비롯한, 인가 토큰을 요청하는 엔티티의 아이덴티티 정보를 검증하도록 구성된 아이덴티티 서비스 또는 아이덴티티 제공자를 포함할 수 있다. 구현에 따르면, 인가 서버(108)의 토큰 발행자(110)는 토큰이 요청되고/되거나 리소스(예를 들어, 보안된 리소스(116))에 액세스하는 데 사용되는 것으로 의도되는 환경의 신뢰 레벨을 나타낼 수 있는 신뢰 표시를 더 포함하는, 컴퓨팅 디바이스(102)에 전송을 위한 토큰을 생성하고 발행할 수 있다. 일부 예에서, 인가 서버(108)는 검증된 아이덴티티 정보에 기초하여, 인가 서버(108)와 관련이 없고/없거나 인가 서버와 제휴되지 않은 복수의 리소스로서의 액세스를 제공하도록 구성될 수 있다. 또 다른 일부 예에서, 인가 서버(108) 및/또는 리소스 서버(112)는 제휴된 엔티티를 포함할 수 있고/있거나 단일 서버 또는 서버의 집합체에서 구현될 수 있다.

[0023] 리소스 서버(112)는 컴퓨팅 디바이스(102)의 사용자에게 의해 보안된 리소스(116)로의 액세스를 호스팅하고, 관리하고/하거나 제공하기 위한 임의의 하나 이상의 컴퓨팅 디바이스, 서버, 서비스, 로컬 프로세스, 원격 머신, 웹 서비스 등을 포함할 수 있다. 예를 들어, 리소스 서버(112)는 조직의 구내에 위치하고/하거나 조직의 로컬 네트워크에 연결된 서버, 원격에 위치한 서버, 클라우드 기반 서버(예를 들어, 분산 방식의 하나 이상의 서버), 또는 보안된 리소스(116)를 호스팅하고, 관리하고/하거나 보안된 리소스로서의 액세스를 제공할 수 있는 임의의 다른 디바이스 또는 서비스를 포함할 수 있다. 보안된 리소스(116)는 이것으로 제한되는 것은 아니지만, 컴퓨팅 또는 프로세싱 리소스, 소프트웨어 리소스(예를 들어, 서비스형 소프트웨어(Software as a Service)(SaaS), 서비스형 플랫폼(Platform as a Service)(PaaS) 등), 저장 리소스(예를 들어, 물리적 저장 디바이스, 로컬 저장 디바이스, 클라우드 기반 저장소, 하드 디스크 드라이브, 솔리드 스테이트 드라이브, 랜덤 액세스 메모리(Random Access Memory)(RAM) 디바이스 등), 데이터베이스 등을 비롯한, 네트워크에 연결된 임의의 유형의 리소스를 포함할 수 있다.

[0024] 예를 들어, 보안된 리소스(116)는 개인 정보, 교육 정보, 건강 정보, 전문 정보, 조직 또는 회사 정보, 은행 또는 다른 금융 기록, 법적 문서, 전기 정보(biographic information), 이를테면 출생 증명서, 운전 면허증, 여권 등과 같은 기밀의, 중요한, 사적인, 안전한 및/또는 그렇지 않다면 공공 보급을 위해 의도되지 않은 임의의 데이터를 저장하기 위한 저장 디바이스를 포함할 수 있다. 이러한 예는 예시일 뿐이며, 보안된 리소스(116)는 로컬로든 및/또는 클라우드 기반 저장소에서도 관계없이 임의의 디바이스에 저장될 수 있는 임의의 다른 유형의 데이터(기밀 정보 및 비기밀 정보 둘 모두를 포함함)를 포함할 수 있다. 일부 예에서, 보안된 리소스(116)는 이를테면 판독/기입 액세스가 데이터의 소유자에 의해서만 제공될 수 있도록 비밀번호 보호, 암호화(예를 들어, 공개 및 개인 키 암호화, 대칭 키 등) 또는 관련 기술분야에서 통상의 기술자에 의해 인식되는 바와 같은 임의의 다른 안전한 방식을 통해, 안전한 방식으로 저장될 수 있다.

[0025] 예시적인 실시예에서, 컴퓨팅 디바이스(102)는 이것으로 제한되는 것은 아니지만, 호스트 컴퓨팅 환경(예를 들어, 컴퓨팅 디바이스(102)의 주요 운영 체제가 실행 중인 환경) 및 호스트 컴퓨팅 환경으로부터 완전히 또는 부분적으로 격리될 수 있는 하나 이상의 다른 컴퓨팅 환경을 비롯한, 복수의 컴퓨팅 환경을 포함할 수 있다. 예를 들어, 이러한 격리된 환경은 가상 머신(104) 및/또는 그 안에서 실행되는 애플리케이션을 포함할 수 있다. 예에서, 가상 머신(104) 및/또는 그 안에서 실행되는 애플리케이션은 격리 메커니즘(예를 들어, 호스트 운영 체제에 의해 관리되는 컨테이너 등)에 의해, 격리 장벽에서 제공된 "구멍"이 없는 격리된 환경 외부의 리소스 또는 격리된 환경에서 실행되는 애플리케이션이 (예를 들어, 호스트 컴퓨팅 환경에 저장된 및/또는 네트워크(110)를 통해 액세스 가능한 다른 디바이스에 저장된) 외부 리소스에 액세스하도록 허용하는 인가 토큰에 액세스하

는 것이 제한될 수 있다.

- [0026] 예에서, 가상 머신(104)의 애플리케이션이 가상 머신(104) 외부의 리소스에 액세스하기를 원할 때, 애플리케이션은 적절한 인가 토큰에 대한 토큰 요청을 인가 토큰 관리자(106)에게 제공할 수 있다. 구현에 따르면, 인가 토큰(106)은 토큰 요청에 신뢰 레벨을 할당하도록 구성될 수 있다. 신뢰 레벨은, 예를 들어, 가상 머신(104) 및/또는 그 안에서 실행되는 애플리케이션이 신뢰성이 없고/없거나 손상 또는 위반되기 쉽다고 표시할 수 있다. 인가 토큰 관리자(106)는 인가 토큰을 획득하기 위해 토큰 요청 및 할당된 신뢰 레벨을 토큰 발행자(110)에게 제공할 수 있다. 토큰 발행자(110)는 아이덴티티 정보(예를 들어, 로그인 자격증명)를 검증하고 그 안에 내장된 신뢰 표시를 포함하는 인가 토큰을 생성할 수 있다. 토큰 발행자(110)는 내장된 신뢰 표시를 포함하는 인가 토큰을 인가 토큰 관리자(106)에 제공할 수 있으며, 인가 토큰 관리자는 인가 토큰을 가상 머신(104)에서 실행되는 요청 애플리케이션에 제공할 수 있다.
- [0027] 애플리케이션이 인가 토큰을 사용하여 보안된 리소스(116)와 같은 외부 리소스에 액세스하려고 시도할 때, 리소스 관리자(114)는 인가 토큰 내의 신뢰 표시를 추출할 수 있다. 따라서, 신뢰 표시가 인가 토큰이 (예를 들어, 랜섬웨어 공격과 같은 다양한 유형의 악의적인 거동에 취약할 수 있는) 신뢰성 없는 환경에서 시작되었다고 표시하는 경우, 리소스 관리자(114)는 애플리케이션에 액세스를 제공하기 전에 보안된 리소스(116)를 보호하는 예방 조치(예를 들어, 백업 생성)를 수행할 수 있다.
- [0028] 구현은 도 1에 도시된 예시적인 배열로 제한되지 않는다는 것을 유의하고 이해한다. 오히려, 네트워크(110)는 임의의 방식으로 연결된 (이것으로 제한되는 것은 아니지만 머신 및/또는 가상 머신을 비롯한) 임의의 수의 컴퓨팅 디바이스 및/또는 서버를 포함할 수 있다. 예를 들어, 컴퓨팅 디바이스(102)가 인가 서버(108), 리소스 서버(112) 및 보안된 리소스(116)와 별개로 도시되어 있지만, 실시예에서, 컴퓨팅 디바이스(102), 인가 서버(108), 리소스 서버(112) 및/또는 보안된 리소스(또는 그 안의 컴포넌트)는 같은 위치에 있거나, 서로 멀리 떨어져 위치할 수 있거나, 단일 컴퓨팅 디바이스 또는 가상 머신에서 구현될 수 있거나, 또는 도 1에서 명시적으로 예시되지 않은 하나 이상의 추가 컴퓨팅 디바이스 또는 가상 머신에서 구현되거나 그에 걸쳐 분산될 수 있다. 인가 토큰 관리자, 토큰 발행자(110), 리소스 관리자(114) 및 보안된 리소스(116)가 컴퓨팅 디바이스에서 구현될 수 있는 배열의 예는 도 6에 예시되어 있으며, 아래에서 더 자세히 설명된다.
- [0029] 인가 토큰 관리자(106)는 보안된 방식으로 리소스에 액세스할 수 있도록 다양한 방식으로 동작할 수 있다. 예를 들어, 인가 토큰 관리자(106)는 도 2에 따라 동작할 수 있다. 도 2는 예시적인 실시예에 따른, 신뢰 표시를 포함하는 인가를 애플리케이션에 제공하기 위한 방법의 흐름도(200)를 도시한다. 예시를 위해, 흐름도(200) 및 인가 토큰 관리자(106)는 도 3과 관련하여 다음과 같이 설명된다.
- [0030] 도 3은 예시적인 실시예에 따른, 보안된 방식으로 네트워크 리소스로서의 액세스를 제공하기 위한 시스템(300)의 블록도를 도시한다. 도 3에 도시된 바와 같이, 시스템(300)은 컴퓨팅 디바이스(102), 인가 서버(108) 및 리소스 서버(112)의 예시적인 구현을 포함한다. 컴퓨팅 디바이스(102)는 가상 머신(104) 및 인가 토큰 관리자(106)를 포함한다. 가상 머신(104)은 그 안에서 실행되는 애플리케이션(302)을 포함할 수 있다. 인가 토큰 관리자(106)는 신뢰 레벨 할당기(304) 및 토큰 요청기(306)를 포함할 수 있다. 인가 서버(108)는 토큰 발행자(110)를 포함한다. 토큰 발행자(110)는 아이덴티티 검증기(314) 및 토큰 생성기(316)를 포함한다. 리소스 서버는 리소스 관리자(114)를 포함한다. 리소스 관리자(114)는 리소스 액세스 제공기(318) 및 리소스 보호기(320)를 포함한다. 리소스 관리자(114)는 보안된 리소스(116) 및 리소스 스냅샷(322)에 연결될 수 있다. 도 3의 시스템(300)에 도시된 바와 같이, 인가 토큰 관리자(106)는 토큰 요청(308) 및 연관된 신뢰 레벨(310)을 토큰 발행자(110)에게 전송할 수 있다. 토큰 발행자(110)는 그 안에 내장될 수 있는 신뢰 표시를 포함하는 인가 토큰(312)을 생성할 수 있다. 인가 토큰 관리자(106)는 인가 토큰을 애플리케이션(302)에 제공할 수 있다. 이어서, 애플리케이션(302)이 인가 토큰을 리소스 관리자(114)에 제공하여 보안된 리소스(116)에 액세스할 때, 리소스 관리자(114)는 이러한 리소스로서의 액세스를 제공하기 전에 보안된 리소스(116)를 보호하는 예방 조치를 수행하도록 구성될 수 있다. 흐름도(200) 및 시스템(300)은 다음과 같이 더 자세히 설명된다.
- [0031] 도 2의 흐름도(200)는 단계(202)에서 시작한다. 단계(202)에서, 리소스에 액세스하기 위해 제 1 컴퓨팅 환경으로부터 적어도 부분적으로 격리된 제 2 컴퓨팅 환경에서 실행되는 애플리케이션으로부터 토큰 요청이 수신된다. 예를 들어, 도 3을 참조하면, 신뢰 레벨 할당기(304)는 애플리케이션(302)으로부터 토큰 요청(324)을 수신하도록 구성될 수 있다. 가상 머신(104)은 다른 컴퓨팅 환경(예를 들어, 컴퓨팅 디바이스(102)의 주요 운영 체제가 실행 중인 수 있는 호스트 환경)으로부터 부분적으로 또는 완전히 격리된 컴퓨팅 환경을 포함할 수 있다. 예를 들어, 가상 머신(104)은 (예를 들어, 호스트 환경에서 실행되는 운영 체제와 동일하거나 상이한 유형의) 운영

체제 및/또는 그 안에서 실행되는 하나 이상의 애플리케이션을 포함할 수 있다. 가상 머신(104)은 컴퓨팅 디바이스(102)의 메인 운영 체제 위에서 실행된다. 애플리케이션(302)은 이것으로 제한되는 것은 아니지만, 가상 머신(104)에 설치된 또는 원격 컴퓨트 또는 서버, 웹 애플리케이션, 웹 서비스 또는 가상 머신(104) 상에서 또는 가상 머신 내에서 실행될 수 있는 임의의 다른 코드 또는 바이너리로부터 액세스되는 소프트웨어 패키지를 비롯한 가상 머신(104) 상에서 실행될 수 있는 임의의 유형의 애플리케이션을 포함할 수 있다.

[0032] 예시적인 실시예에서, 이것으로 제한되는 것은 아니지만, 가상 머신(104)의 사용자에 의해 실행되는 애플리케이션, 애플리케이션(302) 및/또는 가상 머신(104)을 잠재적으로 활용할 수 있는 사용자에 의해 액세스되는 원격 서비스 또는 웹사이트, 및/또는 가상 머신(104) 및/또는 애플리케이션(302) 자체의 본래 양상의 유형을 비롯한, 가상 머신(104) 또는 애플리케이션(302)은 임의의 수의 요인으로 인해 신뢰될 수 없다(예를 들어, 안전하지 않거나 악성 코드의 실행에 취약할 수 있다)(예를 들어, 가상 머신(104) 상에서 실행되는 운영 체제는 전체적으로 신뢰성 없는 것으로 간주될 수 있다).

[0033] 컴퓨팅 디바이스(102)가 가상 머신 및 그 안에서 실행되는 애플리케이션을 포함할 수 있다고 도 3에 도시되지만, 구현은 이러한 특정 배열로 제한되지 않는다. 예를 들어, 대신에 컴퓨팅 디바이스(102) 상의 격리된 컴퓨팅 환경은 게스트, 프라이빗 또는 익명 모드에서 실행되는 애플리케이션과 같은, 컴퓨팅 디바이스(102) 상에서 (예를 들어, 호스트 환경의 동일한 주요 운영 체제 상에서) 실행되는 애플리케이션, 하나의 또는 완전히 또는 부분적으로 격리된 컨테이너 또는 샌드박스형 프로세스 또는 애플리케이션을 포함하는 배열, (동일한 또는 상이한 회로 보드 또는 마더보드 상의) 제 2 CPU의 컴퓨팅 환경으로부터 분리된 제 1 중앙 프로세싱 유닛(central processing unit)(CPU)의 컴퓨팅 환경, 또는 완전하거나 부분적인 격리 경계가 실행 애플리케이션과 호스트 컴퓨팅 환경 사이에서 구현될 수 있는 다른 모드 또는 배열을 포함할 수 있다.

[0034] 예에서, 애플리케이션(302)은 사용자 상호작용을 통해 또는 가상 머신(104) 상에서 실행되는 소프트웨어에 응답하여, 보안된 리소스(116)와 같은 가상 머신(104) 외부의 리소스에 연결하려고 시도할 수 있다. 예를 들어, 애플리케이션(302)은 가상 머신(104) 및/또는 컴퓨팅 디바이스(102)로부터 멀리 떨어진 클라우드 기반 파일 서버에 연결하려고 시도할 수 있다. 이러한 보안된 리소스(116)에 액세스하기 위해, 애플리케이션(302)은 리소스 관리자(114)에 적절한 인가 토큰을 제공해야 할 수 있다. 구현에서, 애플리케이션(302)에 의해 생성된 이러한 인가 토큰에 대한 토큰 요청은 토큰 요청이 호스트 컴퓨팅 환경에 제공되도록 리디렉션될 수 있다. 예를 들어, 도 3을 참조하면, 애플리케이션(302)에 의해 개시된 인가 토큰에 대한 요청은 애플리케이션이 특정 리소스에 액세스하려고 한다는 것을 표시하는 신뢰 레벨 할당기(304)로 리디렉션될 수 있다. 신뢰 레벨 할당기(304)는 컴퓨팅 디바이스(102)의 가상 머신(104)과 호스트 컴퓨팅 환경 사이에 구현된 격리 장벽에서 제공된 하나 이상의 구멍을 통해 이러한 요청을 수신할 수 있다.

[0035] 신뢰 레벨 할당기(304)에 의해 애플리케이션(302)으로부터 수신된 인가 요청은, 다른 것 중에서도, 액세스가 요청되는 리소스의 식별(예를 들어, 보안된 리소스(116)의 식별), 요청 애플리케이션의 식별, 적절한 인가 엔티티(예를 들어, 아이덴티티 제공자)에 대한 로그인 자격증명, 요청된 액세스의 유형(예를 들어, 관독 전용 액세스, 관독/기입 액세스 등), 토큰이 요청된 시간 길이 및 관련 기술분야에서 통상의 기술자에 의해 인식되는 인가 토큰 요청과 연관될 수 있는 임의의 다른 정보를 포함할 수 있다.

[0036] 단계(204)에서, 신뢰 레벨이 토큰 요청에 할당된다. 예를 들어, 도 3을 참조하면, 신뢰 레벨 할당기(304)는 가상 머신(104)에서 실행되는 애플리케이션(302)에 의해 수신되는 토큰 요청(324)에 신뢰 레벨을 할당하도록 구성될 수 있다. 일부 예에서, 앞에서 설명된 바와 같이, 가상 머신(104) 및/또는 그 안에서 실행되는 하나 이상의 애플리케이션은 신뢰성 없는 것으로 간주될 수 있다. 그러한 예에서, 신뢰 레벨 할당기(304)는 (예를 들어, 애플리케이션(302) 및/또는 가상 머신(104)을 식별함으로써) 토큰 요청을 요청하는 엔티티가 신뢰성 없다는 것을 표시하는 신뢰 레벨을 할당할 수 있다. 일부 추가 구현에서, 신뢰 레벨 할당기(304)는 미리 결정된 척도에 기초하여 토큰 요청의 신뢰성의 레벨을 표시할 수 있는 영숫자 값과 같은 등급을 포함하는 신뢰 레벨을 할당할 수 있다.

[0037] 예에서, 신뢰 레벨 할당기(304)는 다양한 방식으로 신뢰 레벨을 할당할 수 있다. 예를 들어, 신뢰 레벨 할당기(304)는 가상 머신(104)의 아이덴티티, 가상 머신(104) 상에서 실행되는 운영 체제 및/또는 그 안에서 실행될 수 있는 임의의 다른 애플리케이션(302)과 같은 격리된 컴퓨팅 환경의 특성에 관한 미리 결정된 지식(예를 들어, 데이터베이스 또는 다른 데이터 구조에 저장되어 있음)에 기초하여 신뢰 레벨을 할당할 수 있다. 하나의 예시적인 예에서, 신뢰 레벨 할당기(304)는 격리된 환경으로부터 유래하는 특정 유형의 토큰 요청(또는 모든 토큰 요청)이 신뢰성 없다고 자동적으로 간주하고 그에 따라 각각의 이러한 토큰 요청에 감소된 신뢰 레벨을 할당

할 수 있다. 다른 예에서, 신뢰 레벨 할당기(304)는 컴퓨팅 디바이스(102) 상의 격리된 환경의 일부로서 호스팅될 수 있는 특정 애플리케이션, 운영 체제 또는 가상 머신과 연관된 토큰 요청에 감소된 신뢰 레벨을 할당할 수 있다. 또 다른 예에서, 신뢰 레벨 할당기(304)는 즉각적인 결정에 기초하여 애플리케이션(302)으로부터 수신된 토큰 요청에 신뢰 레벨을 할당할 수 있다. 신뢰 레벨은 숫자 값(예를 들어, 0 내지 10 범위, "0"은 신뢰 없음을 의미하고 "10"은 가장 높은 신뢰를 의미함), 텍스트 값(예를 들어, "높음", "중간", "낮음", "없음" 등), 영숫자 값, 문자열 등을 비롯한 임의의 형태로 표시될 수 있다.

[0038] 단계(206)에서, 토큰 요청의 신뢰 레벨에 대응하는 신뢰 표시를 포함하는 인가 토큰이 획득된다. 예를 들어, 도 3을 참조하면, 토큰 요청기(306)는 토큰 발행자(110)로부터 신뢰 표시를 포함하는 인가 토큰(312)을 획득할 수 있다. 토큰 요청기(306)는 다양한 방식으로 인가 토큰(312)을 획득할 수 있다. 도 3에 도시된 예시적인 배열에서, 예를 들어, 토큰 요청기(306)는 신뢰 레벨 할당기(304)로부터 신뢰 레벨(310)을 획득(328)하도록 구성될 수 있다. 토큰 요청기(306)는 하나 이상의 API 또는 네트워크 호출에 따라 토큰 발급자(110)의 아이덴티티 검증기(314)에게 신뢰 레벨(332)을 전송(310)할 수 있을 뿐만 아니라, 토큰 요청(308)을 전송(330)할 수 있다. 토큰 요청(308)은 로그인 자격증명, 액세스될 리소스의 식별, 요청된 액세스의 범위 등과 같이 이전에 설명된 바와 같은 요청된 액세스와 연관된 정보를 포함할 수 있다. 토큰 요청(308)은 신뢰 레벨 할당기(304)에 의해 애플리케이션(302)으로부터 (예를 들어, 리소스에 액세스하기 위해) 수신된 토큰 요청 및 연관된 신뢰 레벨에 대응할 수 있다. 예를 들어, 신뢰 레벨이 가상 머신(104) 및/또는 애플리케이션(302)이 신뢰되지 않는다고 표시하는 신뢰 레벨을 할당하는 경우, 토큰 요청기(306)는 요청된 리소스에 액세스할 수 있게 하는 토큰을 획득하기 위해 토큰 요청(306) 및 할당된 신뢰 레벨(310)을 적절한 토큰 발행 서비스에 전송할 수 있다.

[0039] 구현에서, 토큰 요청(308)은 신뢰 레벨(310)과 별개로 (예를 들어, 상이한 데이터 패킷으로, 순차적으로, 비순차적으로 등) 전송될 수 있다. 일부 다른 예에서, 토큰 요청(308)과 신뢰 레벨(310)은 (예를 들어, 동일한 데이터 패킷 또는 데이터 패킷의 세트의 일부로서) 함께 전송될 수 있다. 예를 들어, 신뢰 레벨(310)은 토큰 요청(308)에 태그, 식별자, 마킹, 플래그, 클레임, 메타데이터, 요청과 연관된 새로운 또는 수정된 범위 등으로서 첨부되거나, 이에 포함되거나, 또는 그렇지 않으면 이와 함께 전송될 수 있다. 구현은 이러한 예시적인 예로 제한되지 않으며, 토큰 요청(308)과 함께 토큰 요청의 신뢰성 정보를 나타낼 수 있는 신뢰 레벨(310)을 토큰 발행자(예를 들어, 토큰 발행자(110))에게 전송하는 임의의 다른 방식을 포함할 수 있다.

[0040] 예에서, 토큰 생성기(316)는 토큰이 사용될 수 있는 환경의 신뢰 레벨을 나타내는 신뢰 표시를 포함하는 인가 토큰(312)을 생성할 수 있다. 신뢰 표시는 임의의 적합한 형식(예를 들어, 숫자, 텍스트, 문자열 등)을 포함할 수 있고 인가 토큰(312) 내에 포함되거나, 이에 첨부되거나, 이와 병합되거나, 또는 그렇지 않으면 이와 연관될 수 있다. 예를 들어, 신뢰 표시는 유사하게 인가 토큰(312)의 일부이거나 이와 통합된 태그, 식별자, 마킹, 플래그, 클레임, 메타데이터, 새로운 또는 수정된 범위 등을 포함할 수 있다. 인가 토큰(312)이 파일인 예에서, 신뢰 표시는 기존 필드에 기입되거나 또는 파일에 대한 새로운 엔트리로서 기입될 수 있다. 신뢰 표시를 포함 시킴으로써, 인가 토큰(312)은 "마킹된" 것으로 간주된다. 따라서, 구현에서, 인가 토큰(312)은 요청 엔티티가 안전하지 않을 수 있다고 표시하는 마킹된 토큰을 포함할 수 있다. 예에서, 토큰 생성기(316)는 (예를 들어, 네트워크를 통해) 신뢰 표시를 포함하는 인가 토큰(312)을 토큰 요청기(306)에게 전송(334)할 수 있다.

[0041] 단계(208)에서, 신뢰 표시를 포함하는 인가 토큰은 제 2 컴퓨팅 환경에서 실행되는 애플리케이션에 제공된다. 예를 들어, 도 3을 참조하면, 토큰 요청기(306)는 가상 머신(104) 상에서 실행되는 애플리케이션(302)에게 신뢰 표시를 포함하는 인가 토큰(312)을 제공(326)하도록 구성될 수 있다. 구현에서, 토큰 요청기(306)는 인가 토큰을 수정하지 않고 인가 토큰(312)을 애플리케이션(302)에 전달할 수 있다. 그 다음, 애플리케이션(302)은 인가 토큰(312)을 사용하여 보안된 리소스(116)(또는 컴퓨팅 디바이스(102)에 로컬로 저장될 수 있는 리소스)와 같은 리소스에 액세스할 수 있다. 예에서, 신뢰 표시는 인가 토큰(312)의 일부로서 포함되기 때문에, 애플리케이션(302)(또는 가상 머신(104)에서 실행될 수 있는 임의의 악성 코드)은 수신된 인가 토큰을 변경할 수 없다. 다시 말해, 인가 토큰이 잠재적으로 손상된 환경(예를 들어, 가상 머신(104))에서 발생하는 임의의 활동에 의해 변경되면, 변경된 인가 토큰은 리소스 제공자의 리소스에 액세스할 수 없게 되는데, 왜냐하면 리소스 제공자와 인가 서비스(예를 들어, 도 3의 예에 도시된 바와 같은 토큰 발행자(110) 및 리소스 관리자(114)) 사이에서 검증되지 않을 수 있기 때문이다. 결과적으로, 신뢰 표시는 수정될 수 없는 방식으로 인가 토큰에 내장되며, 그 때문에 인가 토큰의 무결성을 강화할 수 있다.

[0042] 아래에서 더 자세히 설명되는 바와 같이, 애플리케이션(302)이 수신된 인가 토큰을 적절한 리소스 제공자에게 전송(336)함으로써 리소스에 액세스하려고 시도할 때, 리소스 제공자는 인가 토큰으로부터 신뢰 표시를 추출(예를 들어, 판독 또는 복사)하고 리소스로의 액세스를 제공하기 전에 예방 조치가 수행해야 하는지를 결정하도록

구성될 수 있다. 예를 들어, 리소스 보호기(320)가 애플리케이션(302) 및/또는 가상 머신(104)이 안전하지 않을 수 있다고 표시하는 신뢰 표시를 추출하는 경우, 리소스 보호기(320)는 그러한 리소스로의 액세스(338)를 승인하기 전에 요청된 리소스의 백업을 생성함으로써 (예를 들어, 리소스 스냅샷(322)을 생성함으로써) 보안된 리소스(116)를 보호하도록 구성될 수 있다. 리소스를 보호하는 예방 조치의 수행을 도시는 예시적인 흐름도가 도 6과 관련하여 아래에서 더 자세히 설명될 것이다.

[0043] 위에서 설명한 바와 같이, 토큰 발행자(110)는 다양한 방식으로 신뢰 표시를 포함하는 인가 토큰을 생성하도록 구성될 수 있다. 예를 들어, 도 4는 예시적인 실시예에 따른, 신뢰 표시를 포함하는 인가 토큰을 생성하기 위한 방법의 흐름도(400)를 도시한다. 구현에서, 흐름도(400)의 방법은 아이덴티티 검증기(314) 및 토큰 생성기(316)에 의해 구현될 수 있다. 도 4는 도 3을 계속 참조하여 설명된다. 다른 구조적 및 동작적 구현은 흐름도(400) 및 도 3의 시스템(300)에 관한 다음의 논의에 기초하여 관련 기술(들)의 통상의 기술자에게 명백할 것이다.

[0044] 흐름도(400)는 단계(402)에서 시작한다. 단계(402)에서, 아이덴티티 정보 및 제 1 컴퓨팅 환경으로부터 적어도 부분적으로 격리된 제 2 컴퓨팅 환경의 애플리케이션에서 토큰 요청이 개시되었다는 표시를 포함하는 토큰 요청이 수신된다. 예를 들어, 도 3을 참조하면, 인가 서버(108)의 아이덴티티 검증기(314)는 아이덴티티 정보 및 연관된 신뢰 레벨을 표시하는 신뢰 레벨(310)을 포함하는 토큰 요청(308)을 수신하도록 구성될 수 있다. 예에서, 아이덴티티 정보는 사용자 로그인 자격증명(예를 들어, 사용자 이름 및/또는 비밀번호), 사용자 별칭, 계정 번호, 생체 인식 정보, 또는 아이덴티티 검증기(314)가 리소스(예를 들어, 보안된 리소스(116))로의 액세스를 허용할지를 결정하기 위해 검증할 수 있는 임의의 다른 정보 또는 자격증명 중 하나 이상을 포함할 수 있다. 앞서 설명된 바와 같이, 신뢰 레벨(310)은 토큰 요청(308)이 개시된 환경의 신뢰 레벨에 대응하는 정보를 포함할 수 있다. 예를 들어, 도 3을 참조하면, 신뢰 레벨(310)은 가상 머신(104)에서 실행되는 애플리케이션(302)과 연관된 신뢰 레벨을 표시할 수 있다. 다른 예에서, 신뢰 레벨(310)은 요청이 호스트 컴퓨팅 환경과 상이한 환경 또는 호스트 컴퓨팅 환경 내에서 실행되는 환경에서 개시되었다는 것을 표시하는 플래그 또는 다른 표시를 포함할 수 있다. 이러한 예는 예시일 뿐이며, 신뢰 레벨(310)은 토큰 요청(308)이 잠재적으로 신뢰성 없는 환경으로부터 유래되었을 수 있다고 표시하는 임의의 유형의 정보(예를 들어, 플래그, 마킹, 클레임, 메타데이터 등)를 포함할 수 있다.

[0045] 단계(404)에서, 아이덴티티 정보가 검증된다. 예를 들어, 도 3을 참조하면, 아이덴티티 검증기(314)는 토큰 요청(308)에서 수신된 아이덴티티 정보를 검증하여 요청 엔티티가 요청된 리소스에 액세스할 수 있게 하는 인가 토큰을 획득하도록 허용하는지를 결정하도록 구성될 수 있다. 아이덴티티 검증기(314)는 관련 기술 분야의 통상의 기술자에게 인식되는 바와 같이 다양한 방식으로, 이를테면 데이터베이스(예를 들어, 사용자 또는 계정 데이터베이스 또는 유사한 것)에서 아이덴티티 정보를 조회 및 비교하고, 검증을 위해 아이덴티티 정보를 다른 서버나 서비스에 제공하는 것 등을 수행함으로써 아이덴티티 정보를 검증할 수 있다. 예를 들어, 검증이 성공하지 못하면(예를 들어, 부정확한 사용자 자격증명이 수신되면), 아이덴티티 검증기(314)는 액세스가 허용되지 않아야 하고, 그래서 인가 토큰이 애플리케이션(302)에 제공되지 않을 것이라고 결정할 수 있다. 검증이 성공적일 때, 아이덴티티 검증기(314)는 토큰 생성기(316)가 요청된 리소스에 액세스할 애플리케이션(302)에 제공될 수 있는 적절한 인가 토큰을 생성하도록 할 수 있다.

[0046] 단계(406)에서, 신뢰 표시를 포함하는 인가 토큰이 생성된다. 예를 들어, 도 3을 참조하면, 토큰 생성기(316)는 토큰 요청이 개시된 컴퓨팅 환경의 신뢰 레벨을 나타내는 신뢰 표시를 포함하는 인가 토큰(312)을 생성하도록 구성될 수 있다. 예에서, 신뢰 표시는 이를테면 컴퓨팅 환경이 신뢰되지 않는다고 표시함으로써, 가상 머신(104) 및/또는 그 안에서 실행되는 애플리케이션(302)과 연관된 신뢰 레벨을 표시할 수 있다. 앞서 설명된 바와 같이, 신뢰 표시는 인가 토큰(312)에 내장될 수 있고, 인가 토큰이 신뢰성 없는 컴퓨팅 환경의 애플리케이션에 의해 사용될 수 있다는 것을 리소스 제공자(예를 들어, 리소스 서버(112))에게 표시할 수 있는 태그, 마킹, 플래그, 클레임 등을 비롯한 임의의 적합한 형태를 포함할 수 있다.

[0047] 일부 예시적인 구현에서, 신뢰 표시는 각각의 수신된 토큰 요청마다 상이할 수 있다. 예를 들어, 특정 유형의 격리된 환경(예를 들어, 그 안에서 실행되는 안전하지 않은 것으로 알려진 특정 애플리케이션 및/또는 운영 체제)은 다른 애플리케이션 또는 운영 체제보다 덜 신뢰할 수 있는 것으로 간주될 수 있으며, 그래서 이러한 덜 신뢰할 수 있는 애플리케이션 또는 운영 체제에 대한 신뢰 표시는 더 감소된 신뢰 레벨을 나타낼 수 있다. 다른 예에서, 신뢰 표시는 이를테면 애플리케이션이 (안전하지 않은 것으로 알려진 것과 대조적으로) 단지 잠재적으로 신뢰할 수 있는 것으로 간주될 수 있는 경우 상이한 유형의 표시를 포함할 수 있다. 이러한 방식으로, 토큰 생성기(316)는 신뢰성 없는 환경에서 애플리케이션의 신뢰 레벨을 나타내는 적절한 신뢰 표시로 인가 토큰

(312)을 마킹할 수 있고, 이에 의해 리소스 제공자가 내장된 신뢰 표시에 기초하여 상이한 예방 대책을 수행할 수 있게 한다.

[0048] 인가 토큰(312)은 컴퓨팅 엔티티(예를 들어, 애플리케이션, 서비스 등)가 리소스에 액세스할 수 있게 하는 임의의 유형의 토큰을 포함할 수 있다. 인가 토큰(312)의 예는 이것으로 제한되는 것은 아니지만, 웹 또는 다른 네트워크 액세스 가능한 리소스에 액세스할 수 있게 하는 웹 토큰, 액세스 토큰, 공개 인가(Open Authorization)(OAuth) 표준에 따라 생성된 토큰, 마이크로소프트® 윈도우즈 T 토큰 등을 포함한다. 인가 토큰(312)은 특정 요청 애플리케이션을 위해 또는 특정 리소스를 위해 생성될 수 있거나, 또는 복수의 이러한 애플리케이션과 연관된 단일 토큰을 포함할 수 있다.

[0049] 일부 예시적인 실시예에서, 토큰 생성기(316)는 또한 각각의 생성된 인가 토큰(312)을 적합한 저장 디바이스에(로컬로 또는 하나 이상의 클라우드 기반 저장소에) 저장하도록 구성될 수 있다. 따라서, 애플리케이션(302)이 인가 토큰(312)을 리소스 관리자(114)에게 제공함으로써 리소스에 액세스하려고 시도할 때, 리소스 보호기(320)는 요청된 리소스로의 액세스를 승인하기 전에 인가 서버(108)에 저장된 인가 토큰을 획득하여 애플리케이션(302)으로부터 수신된 토큰의 진위를 결정할 수 있다. 다른 예에서, 토큰 생성기(316)는 또한, 이를테면 토큰 생성기(316)가 애플리케이션(302)이 동일한 리소스에 액세스하기 위해 대응하는 인가 토큰을 이전에 생성했던 경우, 이전에 생성되고 만료되지 않은(신뢰 표시를 포함하는) 토큰을 토큰 요청기(306)에게 재전송하도록 구성될 수 있다.

[0050] 단계(408)에서, 신뢰 표시를 포함하는 인가 토큰이 제 2 컴퓨팅 환경에서 실행되는 애플리케이션에 제공된다. 예를 들어, 도 3을 참조하면, 토큰 생성기(316)는(예를 들어, 격리 경계를 통해 인가 토큰(302)을 전달함으로써) 및/또는 인가 토큰(312)을(예를 들어, 토큰을 중개자로서 토큰 요청기(306)에 전송하지 않고) 직접 애플리케이션(302)에 제공함으로써, 인가 토큰(312)을 토큰 요청기(306)에게 전송하여 애플리케이션(302)에 제공하도록 구성될 수 있다. 위에서 설명된 바와 같이, 애플리케이션(302)은 인가 토큰(312)을 사용하여 요청된 리소스에 액세스할 수 있다.

[0051] 본 명세서에서 설명된 바와 같이, 리소스 관리자(114)는 인가 토큰을 수신하는 것에 응답하여 보안된 리소스(116)를 보호하도록 구성될 수 있다. 예를 들어, 도 5는 예시적인 실시예에 따른, 리소스를 보호하는 예방 조치를 수행하기 위한 방법의 흐름도를 도시한다. 구현에서, 흐름도(500)의 방법은 리소스 액세스 제공기(318) 및 리소스 보호기(320)에 의해 구현될 수 있다. 도 5는 도 3을 계속 참조하여 설명된다. 다른 구조적 및 동작적 구현은 흐름도(500) 및 도 3의 시스템(300)에 관한 다음의 논의에 기초하여 관련 기술(들)의 통상의 기술자에게 명백할 것이다.

[0052] 흐름도(500)는 단계(502)에서 시작한다. 단계(502)에서, 인가 토큰이 컴퓨팅 환경에서 실행되는 애플리케이션으로부터 수신된다. 예를 들어, 도 3을 참조하면, 리소스 보호기(320)는 네트워크(110)를 통해 가상 머신(104)에서 실행되는 애플리케이션(302)으로부터 인가 토큰(312)을 수신하도록 구성될 수 있다. 본 명세서에서 설명된 바와 같이, 인가 토큰(312)은 또한 인가 토큰(312)과 연관된 환경의 신뢰 레벨을 나타내는 신뢰 표시를 포함할 수 있다. 그러므로, 이 예에서, 신뢰 표시는 가상 머신(104) 및/또는 애플리케이션(302)이 실행될 수 있는 컴퓨팅 환경의 신뢰 레벨을 표시할 수 있다.

[0053] 그러나, 일부 다른 예시적인 실시예에서, 이를테면 토큰 요청이 신뢰성 있는 환경에서(예를 들어, 컴퓨팅 디바이스의 주요 운영 체제 상에서 실행되는 애플리케이션으로부터) 유래되는 경우, 인가 토큰(312)은 신뢰 표시를 포함하지 않을 수 있다. 예를 들어, 신뢰성 있는 애플리케이션(또는 신뢰성 있는 환경에서 실행되는 애플리케이션)이 인가 토큰을 요청하면, 생성된 인가에는 이러한 애플리케이션에 대한 신뢰 표시가 포함되지 않을 수 있다. 따라서, 일부 예에서, 리소스 보호기(320)는 또한 수신된 인가 토큰에서 신뢰 표시가 존재하는지를 결정하도록 구성될 수 있다.

[0054] 앞서 설명된 바와 같이, 애플리케이션(302)이 인가 토큰(312)을 획득한 후에, 애플리케이션(302)은 리소스 서버(112)와 같은 적절한 리소스 제공자와 상호작용함으로써 승인된 인가 토큰의 범위와 일치하는 리소스에 액세스하려고 시도할 수 있다. 예에서, 애플리케이션(302)은 또한 시도된 자원의 액세스와 함께 인가 토큰(312)을 자원 보호기(320)에 제공할 수 있다. 리소스 보호기(320)는, 이를테면 인가 서버(108)와 상호작용하여 애플리케이션(302)으로부터 수신된 인증 토큰이 유효한지 및/또는 만료되지 않았는지를 결정함으로써, 이전에 설명된 것과 유사한 방식으로 인가 토큰(312)의 진위를 검증할 수 있다.

[0055] 단계(504)에서, 인가 토큰으로부터 신뢰 표시가 추출된다. 예를 들어, 리소스 보호기(320)는 인가 토큰(312)을

파싱하여 그로부터 신뢰 표시를 추출하도록 구성될 수 있다. 예를 들어, 신뢰 표시가 인가 토큰(312)에서 식별자, 마킹, 플래그, 클레임, 메타데이터 등으로서 내장되어 있는 경우, 리소스 보호기(320)는 이러한 표시를 추출할 수 있다. 일부 구현에서, 리소스 보호기(320)는 또한 (예를 들어, 수신된 토큰의 진위가 확인될 때) 인가 서버(108)로부터 신뢰 표시를 획득할 수 있다.

[0056] 단계(506)에서, 리소스를 보호하기 위해 예방 조치가 수행되어야 한다고 결정된다. 예를 들어, 도 3을 참조하면, 리소스 보호기(320)는 인가 토큰을 수신하고 신뢰 표시를 추출하는 것에 응답하여, 리소스를 보호하기 위해 예방 조치가 수행되어야 한다고 결정하도록 구성될 수 있다. 예를 들어, 신뢰 표시가 인가 토큰(312)이 수신된 환경이 신뢰할 수 없다고 표시하는 경우, 리소스 보호기(320)는 보안된 리소스(116)를 보호하기 위해 하나 이상의 예방 조치가 수행되어야 한다고 결정할 수 있다. 예방 조치는 보안된 리소스(116)에 대한 잠재적인 악의적 변경을 (예를 들어, 선제적으로) 방지하거나 또는 경감하기 위해 수행되는 임의의 유형의 조치를 포함할 수 있다.

[0057] 예를 들어, 추출된 신뢰 표시가 인가 토큰(312)이 수신된 컴퓨팅 환경이 신뢰할 수 없다고 표시하는 경우, 리소스 보호기(320)는 사용자의 데이터가 훼손되고, 손상되고/되거나 또는 위반되는 것을 방지하는 특정 조치를 수행하도록 구성될 수 있다. 일부 예에서, 리소스 보호기(320)는 복수의 예방 조치가 수행되어야 한다고 결정할 수 있다. 일부 다른 경우에, 이를테면 인증 토큰이 리소스 서버(112)에 의해 신뢰성 있는 것으로 알려진 컴퓨팅 환경으로부터 수신되는 경우, 리소스 보호기(320)는 예방 조치가 수행될 필요가 없다고 결정할 수 있다. 또 다른 일부 예에서, 이를테면 리소스 보호기(320)가 동일한 인가 토큰을 수신하는 것에 응답하여 애플리케이션(302)에 제공된 이전 액세스에 기초하여 애플리케이션(302)이 악성이 아니라고 간주하는 경우, 리소스 보호기(320)는 또한 예방 조치를 수행하지 않기로 결정할 수 있다.

[0058] 단계(508)에서, 예방 조치는 인가 토큰을 수신하는 것에 응답하여 리소스를 보호하기 위해 수행된다. 예를 들어, 도 3을 참조하면, 리소스 보호기(320)는 애플리케이션(302)으로부터 인가 토큰(312)을 수신하는 것에 응답하여 보안된 리소스(116)를 보호하기 위해 하나 이상의 예방 조치를 수행하도록 구성될 수 있다. 예에서, 보안된 리소스(116)를 보호하기 위해 수행되는 예방 조치의 유형(또는 유형들)은 액세스되는 리소스의 유형, 액세스의 범위(예를 들어, 판독 전용 액세스, 리소스의 변경 등) 및/또는 인가 토큰(312)의 신뢰 표시에 의해 표시될 수 있는 신뢰 레벨을 비롯한 인자의 조합에 기초할 수 있다. 예를 들어, 액세스된 리소스가 민감한 및/또는 중요한 것으로 식별되면, 리소스 보호기(320)는 리소스를 보호하기 위해 하나 이상의 보안 대책을 수행하도록 구성될 수 있다. 다른 예에서, 추출된 신뢰 표시가 인가 토큰(312)이 수신된 컴퓨팅 환경(예를 들어, 애플리케이션(302))이 신뢰되지 않는 것으로 알려져 있다고 표시하면, 리소스 보호기(320)는 보안된 리소스(116)를 보호하기 위해 하나 이상의 고조된 보안 조치를 수행할 수 있다.

[0059] 하나의 예에서, 리소스 보호기(320)는 애플리케이션(302)이 신뢰되지 않는다고 표시하는 인가 토큰(312)을 수신하는 것에 응답하여 리소스 스냅샷(322)을 자동으로 생성하도록 구성될 수 있다. 리소스 스냅샷(322)은, 예를 들어 인가 토큰(312)이 있을지라도, 애플리케이션(302)에게 액세스 불가능한 보안된 리소스(116)의 백업 복사본을 포함할 수 있다. 일부 구현에서, 리소스 보호기(320)는 인가 토큰(312)의 전체 액세스 범위와 일치하는 스냅샷을 생성하는 것(예를 들어, 인가 토큰(312)이 광범위하다면 모든 사용자의 파일을 복사하는 것), 및/또는 파일별로 리소스를 복사하는 것(예를 들어, 애플리케이션(302)이 액세스하려고 시도하는 개별 파일만을 복사하는 것)을 비롯한 다양한 방식으로 보안된 리소스(116)의 리소스 스냅샷(322)을 생성할 수 있다.

[0060] 일부 예에서 리소스 스냅샷(322)은 보안된 리소스(116)에 로컬로 저장될 수 있지만, 리소스 스냅샷(322)은 애플리케이션(302) 및/또는 또는 임의의 다른 잠재적으로 신뢰성 없는 애플리케이션에게 액세스 가능하지 않은 방식으로 원격으로 (예를 들어, 다른 서버 상에) 저장될 수도 있다고 생각된다. 일부 구현에서, 리소스 보호기(320)는 리소스 스냅샷(322)을 암호화(또는 추가로 암호화)하여 잠재적인 손상의 경우에 무단 액세스를 방지함으로써 보안을 더 강화하도록 구성될 수 있다.

[0061] 보안된 리소스(116)의 백업 복사본의 생성은 리소스 보호기(320)가 리소스를 보호하기 위해 수행할 수 있는 예방 대책 중 하나의 예시적인 예일 뿐이다. 리소스 보호기(320)는 또한 리소스 스냅샷(322)을 생성하는 것 외에도 또는 그에 대한 대안으로서, 이것으로 제한되는 것은 아니지만, 인가 토큰(312)에서 표시된 범위보다 더 제한된 액세스의 범위(예를 들어, 저장 디바이스 상에서 액세스된 파일의 판독 전용 액세스, 금융 기관으로부터의 출금 방지 등)를 인가하는 것, 그 이후에는 액세스가 종료되는 일정 기간(예를 들어, 일, 시간, 분, 초 등) 동안만 액세스를 허용하는 것, (예를 들어, 보안된 리소스가 은행 또는 금융 정보와 같이 너무 민감하거나 중요하여, 임의의 잠재적으로 신뢰성 없는 액세스를 허용할 수 없는 경우) 액세스를 전적으로 거부하는 것 및/또는 하

나 이상의 추가 또는 대안적인 인가 절차를 요구하는 것을 비롯한 하나 이상의 다른 대책을 수행할 수 있다.

[0062] 일부 다른 경우에, 리소스 보호기(320)는 신뢰 표시를 포함하는 인가 토큰을 수신하는 것에 응답하여 강화된 아이덴티티 인증을 수행할 수 있다. 예를 들어, 리소스 보호기(320)는 보안된 리소스(116)로의 액세스를 승인하기 전에, 컴퓨팅 디바이스(102)의 사용자가 추가적 인증 절차를 수행하거나 또는 신뢰성 있는 환경으로부터(예를 들어, 신뢰성 있는 주요 운영 체제 내에서 실행되는 애플리케이션으로부터) 동일한 인증 절차를 재실행하는 것, 리소스로의 액세스를 승인하기 전에 인증 토큰(312)이 합법적인 애플리케이션에 의해 개시되었다는 것을 확인하기 위해 다중 절차(multi-factor procedure)(예를 들어, 이동 디바이스, 이메일 계정 등으로 전송되는 무작위로 생성된 코드를 확인하는 것)를 수행하는 것을 요구할 수 있다.

[0063] 일부 추가 구현에서, 리소스 보호기(320)는 또한 본 명세서에서 설명된 인증 토큰을 통해 비정상적인 활동을 검출하도록 구성될 수 있다. 예를 들어, 리소스 보호기(320)가 애플리케이션(302)으로부터 특정 인가 토큰(312)과 연관된 비정상적인 횟수의 액세스 요청(예를 들어, 임계값 초과 또는 특정 기간 내의 다수의 액세스 요청)을 수신하면, 리소스 보호기(320)는 애플리케이션(302)이 잠재적으로 악의적인 활동에 참여하고 있다고 추론할 수 있거나 또는 그렇지 않으면 손상될 수 있다고 추론할 수 있다. 그러한 예에서, 리소스 보호기(320)는 추가적인 예방 대책으로서, 애플리케이션(302)으로부터의 액세스 요청을 추가적인 예방 대책으로서 서비스하는 것을 중단할 것을 결정할 수 있다.

[0064] 일부 다른 경우에, 리소스 보호기(320)는 또한 인가 토큰(312)과 관련되지 않은 하나 이상의 리소스에 대해 예방 조치를 수행할 수 있다. 예를 들어, 리소스 보호기(320)가 잠재적으로 신뢰할 수 없는 컴퓨팅 환경으로부터 요청을 수신하면, 리소스 보호기(320)는 보안을 더 강화하기 위해 높아진 민감도 또는 중요도를 포함할 수 있는 관련 없는 파일을(예를 들어, 암호화, 잠금, 더 안전한 위치로 이동 등을 통해) 자동으로 보호하도록 구성될 수 있다. 이러한 방식으로, 특정 악성 코드가 보안된 리소스(116)를 손상시킬 수 있더라도, 리소스 보호기(320)는 악성 코드가 리소스 스냅샷(322)뿐만 아니라, 동일한 서버에 존재할 수 있거나 동일한 서버에 의해 액세스할 수 있는 다른 데이터에 액세스하는 것을 방지할 수 있기 때문에, 악성 코드의 움직임은 여전히 제한될 수 있다.

[0065] 단계(510)에서, 리소스로의 액세스는 컴퓨팅 환경에서 실행되는 애플리케이션에 의해 승인된다. 예를 들어, 도 3을 참조하면, 리소스 액세스 제공기(318)는 컴퓨팅 환경(즉, 잠재적으로 신뢰성 없는 환경)에서 실행되는 애플리케이션(302)에 의해 보안된 리소스(116)로의 액세스를 승인하도록 구성될 수 있다. 일부 예에서, 리소스 액세스 제공기(318)에 의해 승인된 액세스의 유형은 보안된 리소스(116)를 보호하기 위해 수행되는 예방 조치(들)에 기초할 수 있다. 예를 들어, 리소스 보호기(320)가 애플리케이션(302)에 의해 액세스 가능하지 않은 리소스 스냅샷(322)을 생성했다면, 리소스 액세스 제공기(318)는 보안된 리소스(116)로의 전체 관독/기입 액세스를 허용할 수 있다.

[0066] 다른 예에서, 백업 복사본이 생성되지 않으면, 리소스 액세스 제공기(318)는 보안된 리소스(116)가 잠재적으로 악의적인 활동에 의해 영향을 받는 것을 방지하기 위해 관독 전용 액세스와 같은 보다 제한된 액세스를 애플리케이션(302)에게 승인할 수 있다. 예를 들어, 리소스 액세스 제공기(318)는 토큰에 포함된 신뢰 표시에 기초하여, 애플리케이션(302)에게 액세스를 승인하여 애플리케이션(302)이 기존 콘텐츠를 수정하거나 삭제하는 것을 방지하면서, 사용자의 파일 공간에 있는 기존 콘텐츠를 열고/열거나 사용자의 파일 공간에 저장하기 위한 새로운 콘텐츠를 생성하도록 구성될 수 있다. 일부 다른 구현에서, 리소스 액세스 제공기(318)는 또한 애플리케이션(302)에 의해 생성된 임의의 새로운 콘텐츠에 대해 마킹 또는 태그를 구현하도록 구성되어 애플리케이션이 새로운 콘텐츠(콘텐츠의 각 항목은 마킹 또는 태그에 의해 식별됨)를 생성할 수 있도록 할 뿐만 아니라, 콘텐츠의 마킹된 항목에 기초하여 새로 생성된 콘텐츠를 수정하거나 삭제하도록 할 수 있다. 추가 구현에서, 이러한 마킹 또는 태그는 예를 들어 미리 결정된 기간의 경과 후에 또는 전면적 액세스 인가 토큰(예를 들어, 신뢰성 있는 환경에서 실행되는 애플리케이션에게 승인된 토큰)이 마킹된 콘텐츠에 액세스할 때 자동으로 지워질 수 있다.

[0067] 리소스 액세스 제공기(318)는 또한 애플리케이션(302)이 (애플리케이션(302)으로부터 보호될 수 있는 보안된 리소스(116) 대신) 리소스 스냅샷(322)에 액세스하는 것을 허용하도록 구성될 수 있다. 어느 경우든, 리소스 보호기(320)는 애플리케이션(302)에 의한 액세스가 악의적이지 않다는 결정에 따라 및/또는 미리 결정된 시간 경과에 따라 백업 복사본을 자동으로 삭제하도록 구성될 수 있다. 리소스 보호기(320)가 애플리케이션(302)이(예를 들어, 랜섬웨어 또는 유사한 것으로 인해) 보안된 리소스(116)를 악의적으로 변경했다는 통지를 받을 수 있는 경우와 같은 다른 예에서, 리소스 보호기(320)는 리소스 스냅샷(322)으로부터 보안된 리소스(116)를 복원

하도록 구성될 수 있다. 결과적으로, 신뢰성 없는 애플리케이션이 랜섬웨어를 주입하여 사용자의 파일을 암호화하거나 또는 그렇지 않고 변경하려고 시도하더라도, 파일의 백업이 쉽게 복원될 수 있으며, 이에 의해 이러한 악의적인 행위의 피해를 최소화할 수 있다.

[0068] 도 3에 설명된 배열은 단지 예시일 뿐이며, 구현은 인가 토큰 관리자(106), 토큰 발행자(110), 리소스 관리자(114), 보안된 리소스(116) 및 리소스 스냅샷(322) 중 하나 이상이 컴퓨팅 디바이스(102)에 로컬로 구현될 수 있는 배열을 비롯한, 다양한 다른 유형의 배열을 포함할 수 있다. 도 6은 예시적인 실시예에 따른, 보안된 방식으로 로컬 리소스로의 액세스를 제공하기 위한 시스템(600)의 블록도를 도시한다. 시스템(600)은 컴퓨팅 디바이스(602)를 포함한다. 컴퓨팅 디바이스(102)와 유사하게, 컴퓨팅 디바이스(602)는 복수의 컴퓨팅 환경을 포함할 수 있다. 예를 들어, 컴퓨팅 디바이스(602)는 데스크톱 및/또는 이동 운영 체제(예를 들어, 마이크로소프트® 윈도우즈, 애플® macOS, 애플® iOS, 구글® 안드로이드)를 포함하는 기본 운영 체제가 실행될 수 있는 컴퓨팅 환경을 포함할 수 있다. 컴퓨팅 디바이스(602)는 또한 가상 머신(104) 및 그 안에서 실행되는 애플리케이션(예를 들어, 애플리케이션(302))을 포함할 수 있는 격리된 환경과 같은, 본 명세서에서 설명된 바와 같은 하나 이상의 다른 컴퓨팅 환경을 포함할 수 있다.

[0069] 도 6의 예시적인 배열에서, 제 1 컴퓨팅 환경(예를 들어, 격리된 환경을 호스팅할 수 있는 컴퓨팅 환경)은 인가 토큰 관리자(106), 토큰 발행자(110), 리소스 관리자(114), 보안된 리소스(116) 및 리소스 스냅샷(322) 중 하나 이상을 포함할 수 있다. 예를 들어, 그러한 컴포넌트 중 하나 이상이 하나 이상의 네트워크 엔티티 상에서 구현되는 대신에, 그러한 컴포넌트는 컴퓨팅 디바이스(602)에 로컬로 구현될 수 있다. 예를 들어, 토큰 요청기(306)는 토큰 요청(예를 들어, NT 토큰 또는 유사한 것에 대한 요청)을 컴퓨팅 디바이스(602) 상에서의 로컬 활동에 필요한 인가 토큰을 관리하도록 구성된 아이덴티티 검증기(314)에게 제공할 수 있다. 일부 예시적인 구현에서, 아이덴티티 검증기(314) 및/또는 토큰 생성기(316)는 컴퓨팅 디바이스(602)의 기본 운영 체제, 파일 시스템 관리자의 일부로서 및/또는 그 위에서 실행되는 임의의 다른 애플리케이션으로서 구현될 수 있어, 로컬로 저장된 데이터(또는 로컬 상호작용을 통해, 이를테면 바로 가기 또는 유사한 것을 통해 액세스할 수 있는 원격으로 저장된 데이터)가 로컬 인가 토큰을 통해 관리될 수 있도록 할 수 있다. 다시 말해서, 토큰 생성기(316)는 컴퓨팅 디바이스(602) 상에서 실행되는 애플리케이션(격리된 환경에서 호스팅될 수 있는 임의의 애플리케이션을 포함함)이 보안된 리소스(116)와 같은 로컬 리소스에 액세스하도록 허용하는 인가 토큰을 생성하고 제공하도록 구성될 수 있다.

[0070] 따라서, 애플리케이션(302)이 토큰을 요청하고 토큰 요청기(306)가 토큰 요청(308) 및 할당된 신뢰 레벨(310)을 토큰 발행자(110)에게 제공할 때, 토큰 생성기(316)는 이전에 설명된 바와 유사한 방식으로 신뢰 레벨(310)을 나타내는 신뢰 표시를 포함하는 인가 토큰을 생성할 수 있다. 인가 토큰은, 예를 들어, 사용자 정보(예를 들어, 관리자, 게스트 등으로서의 사용자의 식별), 허가 레벨(예를 들어, 판독 전용, 판독/기입 액세스 등), 요청된 리소스의 식별 등과 같은 인가된 액세스와 연관된 정보를 포함할 수 있다. 토큰 요청기(306)는 신뢰 표시를 포함하는 인가 토큰(예를 들어, 마킹된 인가 토큰)을 애플리케이션(302)에게 제공하여, 애플리케이션이 가상 머신(104)의 외부에서 이용할 수 있는 로컬 리소스에 액세스하도록 허용할 수 있다.

[0071] 따라서, 애플리케이션(302)이 보안된 리소스(116)와 같은 격리된 컴퓨팅 환경 외부의 리소스에 액세스하거나 변경하려고 시도할 때, 리소스 액세스 제공기(318)는 애플리케이션(302)에 의해 제공되는 인가 토큰으로부터 신뢰 표시를 추출하고 애플리케이션(302)이 신뢰되지 않을 수 있다고 결정할 수 있다. 애플리케이션(302)이 신뢰되지 않을 수 있다고 표시하는 그러한 마킹된 인가 요청을 수신하는 것에 응답하여, 리소스 보호기(320)는 보안된 리소스(116)를 보호하기 위해 기본 운영 체제를 포함하는 컴퓨팅 환경에서 하나 이상의 예방 조치, 이를테면 보안된 리소스(116)로의 액세스를 허용하기 전에 보안된 리소스(116)의 백업 복사본을 포함하는 리소스 스냅샷(322)의 생성을 수행할 수 있다. 앞서 설명된 바와 같이, 리소스 보호기(320)는 리소스 스냅샷(322)을 생성하는 것에 추가하여 또는 이에 대한 대안으로서, 이것으로 제한되는 것은 아니지만, 보안된 리소스(116)로의 제한된 액세스(예를 들어, 판독 전용 액세스)를 허용하는 것, 보안된 리소스(116)가 암호화되는 것(또는 추가로 암호화되는 것)을 방지하는 것, 강화된 인가를 요구하는 것, 또는 관련 기술분야의 통상의 기술자에 의해 인식되는 바와 같은 임의의 다른 예방 조치를 비롯한, 임의의 다른 유형의 예방 조치를 포함할 수 있다.

[0072] 격리된 환경은 도 3 및 도 6과 관련하여 설명된 바와 같은 가상 머신(104)을 포함할 필요가 없다는 것을 유의하고 이해한다. 예를 들어, 애플리케이션(302)은 또한 부분적 또는 완전한 격리 경계를 포함할 수 있는 호스트 컴퓨팅 환경 상에서 실행되는 임의의 유형의 애플리케이션(예를 들어, 웹 브라우저)을 포함할 수 있다. 따라서, 격리된 환경이 로컬로 또는 원격으로 저장된 리소스에 액세스할 수 있는 다른 애플리케이션을 포함하는 경우일지라도, 구현은 이러한 액세스에 사용되는 인가 토큰을 본 명세서에서 설명된 바와 같은 액세스하는 환경

의 신뢰 정보로 마킹함으로써 이러한 리소스가 여전히 보다 안전한 방식으로 (예를 들어, 백업 복사본을 생성함으로써, 액세스를 제한함으로써 등) 액세스될 수 있게 할 수 있다.

[0073] III. 예시적인 이동 및 고정 디바이스 실시예

[0074] 컴퓨팅 디바이스(102), 가상 머신(104), 인가 토큰 관리자(106), 인가 서버(108), 토큰 발행자(110), 리소스 서버(112), 리소스 관리자(114), 보안된 리소스(116), 신뢰 레벨 할당기(304), 토큰 요청기(306), 아이덴티티 검증기(314), 토큰 생성기(316), 리소스 액세스 제공기(318), 리소스 보호기(320), 리소스 스냅샷(322), 흐름도(200), 흐름도(400) 및/또는 흐름도(500)는 이블테면 물리적/하드웨어 기반 컴퓨터 판독 가능 저장 매체에 저장되고 하나 이상의 프로세서 상에서 실행되도록 구성된 컴퓨터 프로그램 코드/명령어로서 구현되는 또는 하드웨어 로직/전기 회로(예를 들어, 트랜지스터, 로직 게이트, 연산 증폭기, 하나 이상의 주문형 집적 회로(Application Specific Integrated Circuit)(ASIC), 하나 이상의 필드 프로그램 가능 게이트 어레이(Field Programmable Gate Array)(FPGA)로 구성된 전기 회로)로서 구현되는 하드웨어 또는 소프트웨어 및/또는 펌웨어와 연결된 하드웨어로 구현될 수 있다. 예를 들어, 컴퓨팅 디바이스(102), 가상 머신(104), 인가 토큰 관리자(106), 인가 서버(108), 토큰 발행자(110), 리소스 서버(112), 리소스 관리자(114), 보안된 리소스(116), 신뢰 레벨 할당기(304), 토큰 요청기(306), 아이덴티티 검증기(314), 토큰 생성기(316), 리소스 액세스 제공기(318), 리소스 보호기(320), 리소스 스냅샷(322), 흐름도(200), 흐름도(400), 및/또는 흐름도(500)는 SoC에서 개별적으로 또는 함께 구현될 수 있다. SoC는 프로세서(예를 들어, 중앙 프로세싱 유닛(CPU), 마이크로컨트롤러, 마이크로프로세서, 디지털 신호 프로세서(digital signal processor)(DSP) 등), 메모리, 하나 이상의 통신 인터페이스 및 /또는 추가 회로 중 하나 이상을 포함하는 집적 회로 칩을 포함할 수 있으며, 선택적으로는 수신된 프로그램 코드를 실행하고/하거나 내장된 펌웨어를 포함하여 기능을 수행할 수 있다.

[0075] 도 7은 예시적인 실시예가 구현될 수 있는 컴퓨팅 디바이스(700)의 예시적인 구현을 도시한다. 예를 들어, 컴퓨팅 디바이스(102), 가상 머신(104), 인가 토큰 관리자(106), 인가 서버(108), 토큰 발행자(110), 리소스 서버(112), 리소스 관리자(114), 보안된 리소스(116), 신뢰 레벨 할당기(304), 토큰 요청기(306), 아이덴티티 검증기(314), 토큰 생성기(316), 리소스 액세스 제공기(318), 리소스 보호기(320) 및/또는 리소스 스냅샷(322) 중 임의의 것은 컴퓨팅 디바이스(700)의 하나 이상의 특징 및/또는 대안적인 특징을 포함하는, 고정 또는 이동 컴퓨터 실시예에서의 컴퓨팅 디바이스(700)와 유사한 하나 이상의 컴퓨팅 디바이스에서 구현될 수 있다. 본 명세서에서 제공된 컴퓨팅 디바이스(700)의 설명은 예시를 위해 제공되며 제한하려는 의도가 아니다. 예시적인 실시예는 관련 기술(들)의 통상의 기술자에게 알려진 바와 같이 추가 유형의 컴퓨터 시스템에서 구현될 수 있다.

[0076] 도 7에 도시된 바와 같이, 컴퓨팅 디바이스(700)는 프로세서 회로(702)로 지칭되는 하나 이상의 프로세서, 시스템 메모리(704) 및 시스템 메모리(704)를 포함하는 비롯한 다양한 시스템 컴포넌트를 프로세서 회로(702)에 연결하는 버스(706)를 포함한다. 프로세서 회로(702)는 하나 이상의 물리적 하드웨어 전기 회로 디바이스 요소 및/또는 중앙 프로세싱 유닛(CPU), 마이크로컨트롤러, 마이크로프로세서 및/또는 다른 물리적 하드웨어 프로세서 회로로서의 집적 회로 디바이스(반도체 재료 칩 또는 다이)에서 구현된 전기 및/또는 광학 회로이다. 프로세서 회로(702)는 운영 체제(730)의 프로그램 코드, 애플리케이션 프로그램(732), 다른 프로그램(734) 등과 같이 컴퓨터 판독 가능 매체에 저장된 프로그램 코드를 실행할 수 있다. 버스(706)는 메모리 버스 또는 메모리 제어기, 주변 기기 버스, 가속 그래픽 포트 및 임의의 다양한 버스 아키텍처를 사용하는 프로세서 또는 로컬 버스를 비롯한, 임의의 여러 유형의 버스 구조 중 하나 이상을 나타낸다. 시스템 메모리(704)는 판독 전용 메모리(read only memory)(ROM)(708) 및 랜덤 액세스 메모리(random-access memory)(RAM)(710)를 포함한다. 기본 입/출력 시스템(basic input/output system)(BIOS)(712)은 ROM(708)에 저장된다.

[0077] 컴퓨팅 디바이스(700)는 또한 다음과 같은 드라이브: 하드 디스크로부터 판독하고 하드 디스크에 기입하기 위한 하드 디스크 드라이브(714), 착탈식 자기 디스크(718)로부터 판독하거나 착탈식 자기 디스크에 기입하기 위한 자기 디스크 드라이브(716) 및 CD ROM, DVD ROM 또는 다른 광학 매체와 같은 착탈식 광학 디스크(722)로부터 판독하거나 착탈식 광학 디스크에 기입하기 위한 광학 디스크 드라이브(720) 중 하나 이상을 갖는다. 하드 디스크 드라이브(714), 자기 디스크 드라이브(716) 및 광학 디스크 드라이브(720)는 각기 하드 디스크 드라이브 인터페이스(724), 자기 디스크 드라이브 인터페이스(726) 및 광학 드라이브 인터페이스(728)에 의해 버스(706)에 연결된다. 드라이브 및 이와 연관된 컴퓨터 판독 가능 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 컴퓨터에 필요한 다른 데이터의 비휘발성 저장을 제공한다. 하드 디스크, 착탈식 자기 디스크 및 착탈식 광학 디스크가 설명되지만, 플래시 메모리 카드, 디지털 비디오 디스크, RAM, ROM 및 다른 하드웨어 저장 매체와 같은 다른 유형의 하드웨어 기반 컴퓨터 판독 가능 저장 매체가 데이터를 사용하는 데 사용될 수 있

다.

- [0078] 다수의 프로그램 모듈은 하드 디스크, 자기 디스크, 광학 디스크, ROM 또는 RAM 상에 저장될 수 있다. 이러한 프로그램은 운영 체제(730), 하나 이상의 애플리케이션 프로그램(732), 다른 프로그램(734) 및 프로그램 데이터(736)를 포함한다. 애플리케이션 프로그램(732) 또는 다른 프로그램(734)은, 예를 들어, 컴퓨팅 디바이스(102), 가상 머신(104), 인가 토큰 관리자(106), 인가 서버(108), 토큰 발행자(110), 리소스 서버(112), 리소스 관리자(114), 보안된 리소스(116), 신뢰 레벨 할당기(304), 토큰 요청기(306), 아이덴티티 검증기(314), 토큰 생성기(316), 리소스 액세스 제공기(318), 리소스 보호기(320), 리소스 스냅샷(322), (호름도(200, 400 또는 500)의 임의의 적합한 단계를 포함하는) 호름도(200), 호름도(400) 및/또는 호름도(500), 및/또는 본 명세서에서 설명된 추가의 예시적인 실시예를 구현하기 위한 컴퓨터프로그램 로직(예를 들어, 컴퓨터 프로그램 코드 또는 명령어)을 포함할 수 있다.
- [0079] 사용자는 키보드(738) 및 포인팅 디바이스(740)와 같은 입력 디바이스를 통해 컴퓨팅 디바이스(700)에 명령어 및 정보를 입력할 수 있다. 다른 입력 디바이스(도시되지 않음)는 마이크론, 조이스틱, 게임 패드, 위성 접시, 스캐너, 터치 스크린 및/또는 터치 패드, 음성 입력을 수신하는 음성 인식 시스템, 제스처 입력을 수신하는 제스처 인식 시스템 또는 이와 유사한 것을 포함할 수 있다. 이러한 입력 디바이스 및 다른 입력 디바이스는 종종 버스(706)에 연결된 직렬 포트 인터페이스(742)를 통해 프로세서 회로(702)에 연결되지만, 병렬 포트, 게임 포트 또는 범용 직렬 버스(universal serial bus)(USB)와 같은 다른 인터페이스에 의해 연결될 수 있다.
- [0080] 디스플레이 스크린(744)은 또한 비디오 어댑터(746)와 같은 인터페이스를 통해 버스(706)에 연결된다. 디스플레이 스크린(744)은 컴퓨팅 디바이스(700) 외부에 있거나 컴퓨팅 디바이스에 통합될 수 있다. 디스플레이 스크린(744)은 정보를 디스플레이할 수 있을 뿐만 아니라, (예를 들어, 터치, 손가락 제스처, 가상 키보드 등에 의해) 사용자 명령어 및/또는 다른 정보를 수신하기 위한 사용자 인터페이스일 수 있다. 디스플레이 스크린(744) 이외에, 컴퓨팅 디바이스(700)는 스피커 및 프린터와 같은 다른 주변 기기 출력 디바이스(도시되지 않음)를 포함할 수 있다.
- [0081] 컴퓨팅 디바이스(700)는 어댑터 또는 네트워크 인터페이스(750), 모뎀(752) 또는 네트워크를 통한 통신을 설정하기 위한 다른 수단을 통해 네트워크(748)(예를 들어, 인터넷)에 연결된다. 내부 또는 외부에 있을 수 있는 모뎀(752)은 도 7에 도시된 바와 같이 직렬 포트 인터페이스(742)를 통해 버스(706)에 연결될 수 있거나, 또는 병렬 인터페이스를 비롯한 다른 인터페이스 유형을 사용하여 버스(706)에 연결될 수 있다.
- [0082] 본 명세서에서 사용된 바와 같이, "컴퓨터 프로그램 매체", "컴퓨터 판독가능 매체" 및 "컴퓨터 판독가능 저장 매체"라는 용어는 하드 디스크 드라이브(714)와 연관된 하드 디스크, 착탈식 자기 디스크(718), 착탈식 광학 디스크(722), RAM, ROM, 플래시 메모리 카드, 디지털 비디오 디스크, zip 디스크, MEM, 나노기술 기반 저장 디바이스와 같은 다른 물리적 하드웨어 매체, 및 추가 유형의 물리적/유형의 하드웨어 저장 매체를 지칭하는 데 사용된다. 이러한 판독 가능 저장 매체는 통신 매체와 구별되며 중첩되지 않는다(통신 매체는 포함하지 않음). 통신 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 반송파와 같은 변조된 데이터 신호의 다른 데이터를 구현한다. "변조된 데이터 신호"라는 용어는 신호의 정보를 인코딩하는 방식으로 설정되거나 변경된 특성 중 하나 이상을 갖는 신호를 의미한다. 예로서, 제한되는 것은 아니지만, 통신 매체는 음향, RF, 적외선 및 다른 무선 매체뿐만 아니라, 유선 매체와 같은 무선 매체를 포함한다. 예시적인 실시예는 또한 컴퓨터 판독가능 저장 매체에 관한 실시예와 별개이고 중첩되지 않는 그러한 통신 매체에 관한 것이다.
- [0083] 위에서 언급한 바와 같이, (애플리케이션 프로그램(732) 및 다른 프로그램(734)을 비롯한) 컴퓨터 프로그램 및 모듈은 하드 디스크, 자기 디스크, 광학 디스크, ROM, RAM 또는 다른 하드웨어 저장 매체 상에 저장될 수 있다. 그러한 컴퓨터 프로그램은 또한 네트워크 인터페이스(750), 직렬 포트 인터페이스(742), 또는 임의의 다른 인터페이스 유형을 통해 수신될 수 있다. 이러한 컴퓨터 프로그램은 애플리케이션에 의해 실행되거나 로드될 때 컴퓨팅 디바이스(700)가 본 명세서에서 설명된 예시적인 실시예의 특징을 구현할 수 있게 한다. 따라서, 이러한 컴퓨터 프로그램은 컴퓨팅 디바이스(700)의 제어기를 대변한다.
- [0084] 예시적인 실시예는 또한 임의의 컴퓨터 판독가능 매체 상에 저장된 컴퓨터 코드 또는 명령어를 포함하는 컴퓨터 프로그램 제품에 관한 것이다. 이러한 컴퓨터 프로그램 제품은 하드 디스크 드라이브, 광학 디스크 드라이브, 메모리 디바이스 패키지, 휴대용 메모리 스틱, 메모리 카드 및 다른 유형의 물리적 저장 하드웨어를 포함한다.
- [0085] IV. 예시적인 실시예
- [0086] 인가 토큰을 신뢰 표시와 함께 제공하기 위한 컴퓨팅 디바이스의 시스템이 여기에서 설명된다. 시스템은, 하나

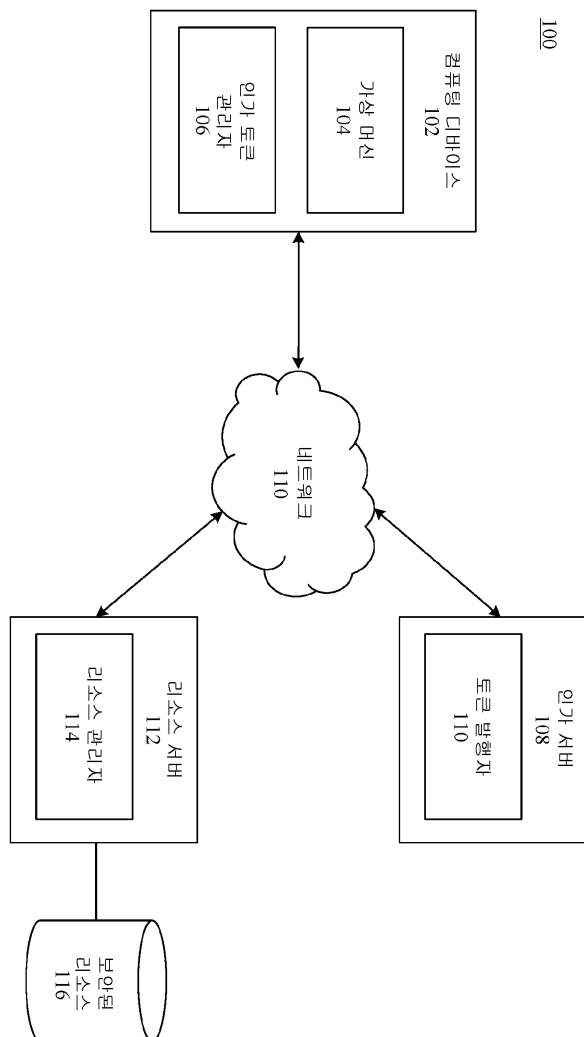
이상의 프로세서와, 하나 이상의 프로세서에 의해 실행되도록 구성된 프로그램 코드를 저장하는 하나 이상의 메모리 디바이스를 포함하고, 프로그램 코드는, 제 1 컴퓨팅 환경의 인가 토큰 관리자로부터, 식별 정보 및 제 1 컴퓨팅 환경으로부터 적어도 부분적으로 격리된 제 2 컴퓨팅 환경에서 실행되는 애플리케이션에서 토큰 요청이 개시되었다는 표시를 포함하는 표시를 포함하는 토큰 요청을 수신하고; 아이덴티티 정보를 검증하도록 구성된 아이덴티티 검증기와, 제 2 컴퓨팅 환경의 신뢰 레벨을 나타내는 신뢰 표시를 포함하는 인가 토큰을 생성하고; 신뢰 표시를 포함하는 인가 토큰을 제 1 컴퓨팅 환경으로 전송하도록 구성된 토큰 생성기를 포함한다.

- [0087] 전술한 시스템의 하나의 구현에서, 신뢰 표시는 제 2 컴퓨팅 환경에서 실행되는 애플리케이션이 신뢰되지 않는다는 표시를 포함한다.
- [0088] 전술한 시스템의 다른 구현에서, 제 2 컴퓨팅 환경은 제 1 컴퓨팅 환경에서 호스팅되는 가상 머신을 포함한다.
- [0089] 전술한 시스템의 다른 구현에서, 인가 토큰은 제 2 컴퓨팅 환경에서 실행되는 애플리케이션이 제 1 컴퓨팅 환경의 보안된 리소스에 액세스하는 것을 허용하도록 구성된다.
- [0090] 전술한 시스템의 다른 구현에서, 인가 토큰은 제 2 컴퓨팅 환경에서 실행되는 애플리케이션이 네트워크를 통해 보안된 리소스에 액세스하는 것을 허용하도록 구성된다.
- [0091] 전술한 시스템의 다른 구현에서, 제 2 컴퓨팅 환경에서 실행되는 애플리케이션에 의한 보안된 리소스의 액세스는 보안된 리소스의 판독 전용 액세스를 포함한다.
- [0092] 보안된 방식으로 리소스에 액세스할 수 있게 하기 위한 방법이 여기에서 개시된다. 방법은, 리소스에 액세스하기 위해 제 1 컴퓨팅 환경으로부터 적어도 부분적으로 격리된 제 2 컴퓨팅 환경에서 실행되는 애플리케이션으로부터 토큰 요청을 수신하는 단계와, 토큰 요청에 신뢰 레벨을 할당하는 단계와, 신뢰 표시를 포함하는 인가 토큰을 획득하는 단계 - 신뢰 표시는 토큰 요청의 신뢰 레벨에 대응함 - 와, 신뢰 표시를 포함하는 인가 토큰을 제 2 컴퓨팅 환경에서 실행되는 애플리케이션에 제공하는 단계를 포함한다.
- [0093] 전술한 방법의 하나의 구현에서, 인가 토큰을 획득하는 단계는, 토큰 요청 및 할당된 신뢰 레벨을 토큰 발행자에게 전송하는 단계와, 토큰 발행자로부터 신뢰 레벨에 대응하는 신뢰 표시를 포함하는 인가 토큰을 수신하는 단계를 포함한다.
- [0094] 전술한 시스템의 다른 구현에서, 신뢰 표시는 제 2 컴퓨팅 환경에서 실행되는 애플리케이션이 신뢰되지 않는다는 표시를 포함한다.
- [0095] 전술한 방법의 다른 구현에서, 리소스는 제 1 컴퓨팅 환경에 저장되어 있고, 방법은, 제 2 컴퓨팅 환경에서 실행되는 애플리케이션으로부터 인가 토큰을 수신하는 단계와, 인가 토큰을 수신하는 것에 응답하여 리소스를 보호하기 위해 제 1 컴퓨팅 환경에서 예방 조치를 수행하는 단계를 더 포함한다.
- [0096] 전술한 방법의 다른 구현에서, 예방 조치는 인가 토큰을 수신하는 것에 응답하여 리소스의 백업의 생성을 포함한다.
- [0097] 전술한 방법의 다른 구현에서, 방법은, 인가 토큰을 수신하는 것에 응답하여 제 1 컴퓨팅 환경에 의한 리소스로의 판독 전용 액세스를 승인하는 단계를 더 포함한다.
- [0098] 전술한 방법의 다른 구현에서, 리소스는 인가 토큰을 수신하고, 인가 토큰으로부터 신뢰 표시를 추출하고, 추출된 신뢰 표시에 기초하여 예방 조치가 수행되어야 한다고 결정하는 것에 응답하여 예방 조치를 수행하도록 구성되는 서버에 저장된다.
- [0099] 전술한 방법의 다른 구현에서, 제 2 컴퓨팅 환경은 제 1 컴퓨팅 환경에서 호스팅되는 가상 머신을 포함한다.
- [0100] 리소스로의 액세스를 승인하기 위한 시스템이 여기에서 설명된다. 시스템은, 하나 이상의 프로세서와, 하나 이상의 프로세서에 의해 실행되도록 구성된 프로그램 코드를 저장하는 하나 이상의 메모리 디바이스를 포함하고, 프로그램 코드는, 컴퓨팅 환경에서 실행되는 애플리케이션으로부터 리소스에 액세스하는 인가 토큰을 수신 - 인가 토큰은 애플리케이션의 신뢰 레벨을 나타내는 신뢰 표시를 포함함 - 하고; 신뢰 표시를 포함하는 인가 토큰을 수신하는 것에 응답하여 리소스를 보호하는 예방 조치를 수행하도록 구성된 리소스 보호기와, 컴퓨팅 환경에서 실행되는 애플리케이션에 의한 리소스로의 액세스를 승인하도록 구성된 리소스 액세스 공급자를 포함한다.
- [0101] 전술한 시스템의 하나의 구현에서, 신뢰 표시는 컴퓨팅 환경에서 실행되는 애플리케이션이 신뢰되지 않는다는 표시를 포함한다.

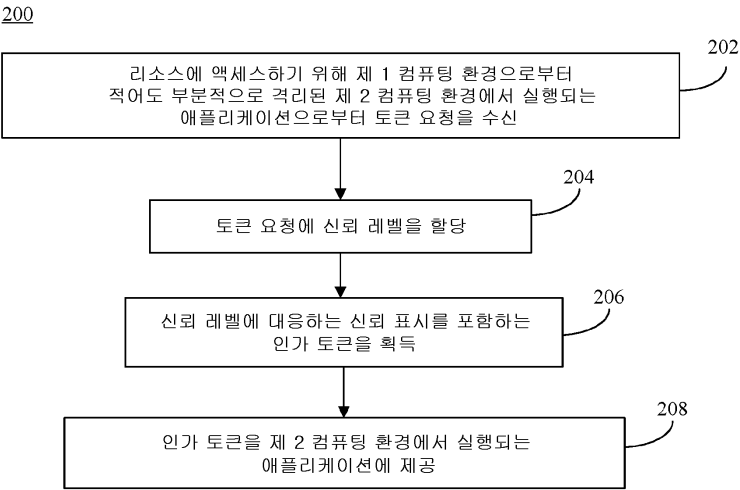
- [0102] 전술한 시스템의 다른 구현에서, 컴퓨팅 환경은 다른 컴퓨팅 환경에서 호스팅되는 가상 머신을 포함한다.
- [0103] 전술한 시스템의 다른 구현에서, 리소스 보호기에 의해 수행되는 예방 조치는 인가 토큰을 수신하는 것에 응답하여 리소스의 백업의 생성을 포함한다.
- [0104] 전술한 시스템의 다른 구현에서, 리소스 액세스 제공기는 인가 토큰을 수신하는 것에 응답하여 컴퓨팅 환경에서 실행되는 애플리케이션에 의한 리소스로의 제한된 액세스를 승인하도록 구성된다.
- [0105] 전술한 시스템의 다른 구현에서, 리소스 보호기는 인가 토큰을 수신하는 것에 응답하여 강화된 아이덴티티 인증을 수행하도록 구성되고, 리소스 액세스 제공기는 강화된 아이덴티티 인증을 수행하는 것에 응답하여 리소스로의 액세스를 승인하도록 구성된다.
- [0106] V. 결론
- [0107] 본 발명의 다양한 실시예가 위에서 설명되었지만, 다양한 실시예는 단지 예로서 제시되었으며 제한이 아니라는 것을 이해해야 한다. 관련 기술분야(들)의 통상의 기술자에 의해, 첨부된 청구범위에서 정의된 바와 같은 본 발명의 사상 및 범위를 벗어나지 않으면서 형태 및 세부사항에서 다양한 변경이 이루어질 수 있다는 것이 이해될 것이다. 따라서, 본 발명의 폭 및 범위는 위에서 설명한 예시적인 실시예 중 어떠한 실시예에 의해서도 제한되지 않아야 하며, 다음의 청구범위 및 그 균등물에 따라서만 정의되어야 한다.

도면

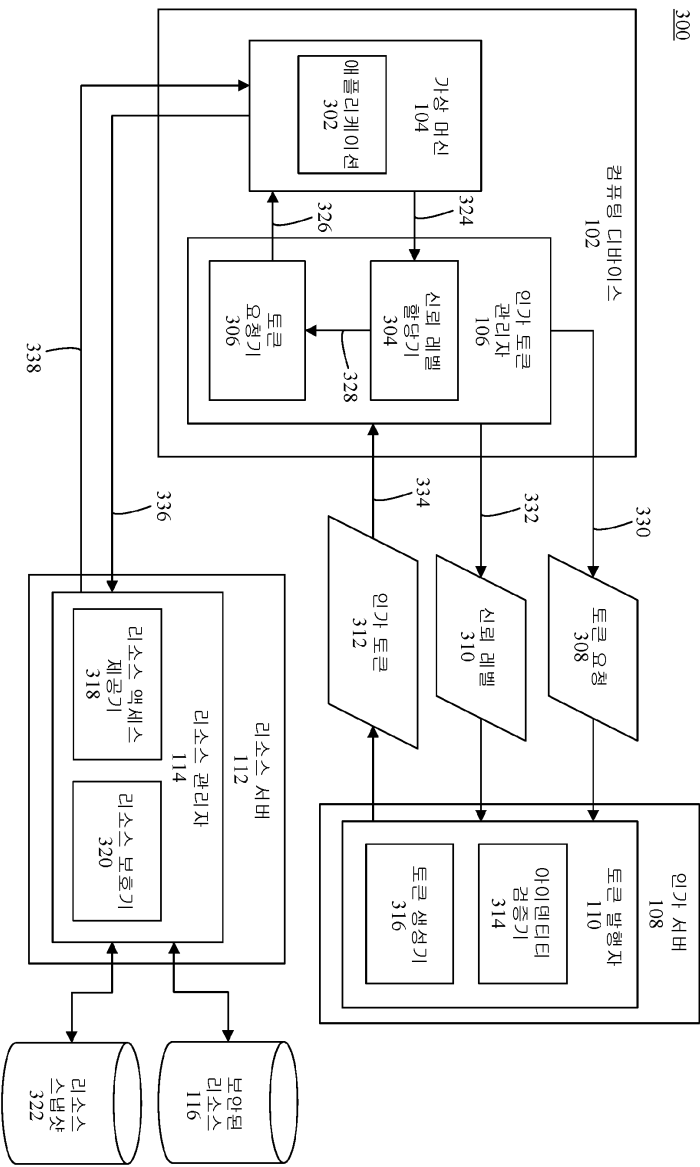
도면1



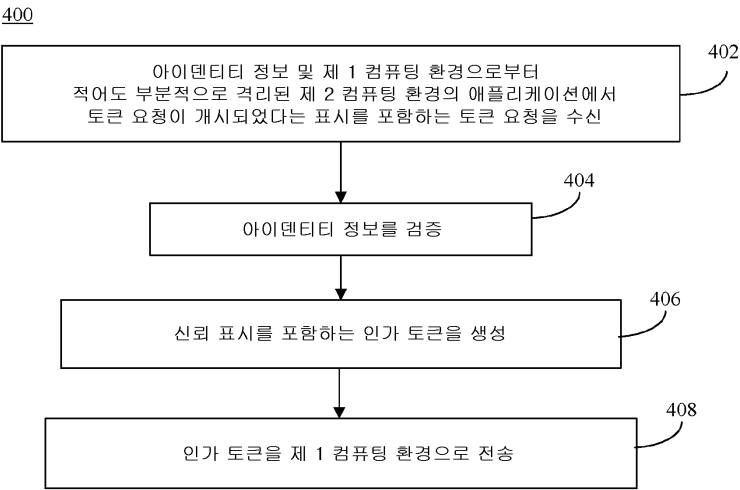
도면2



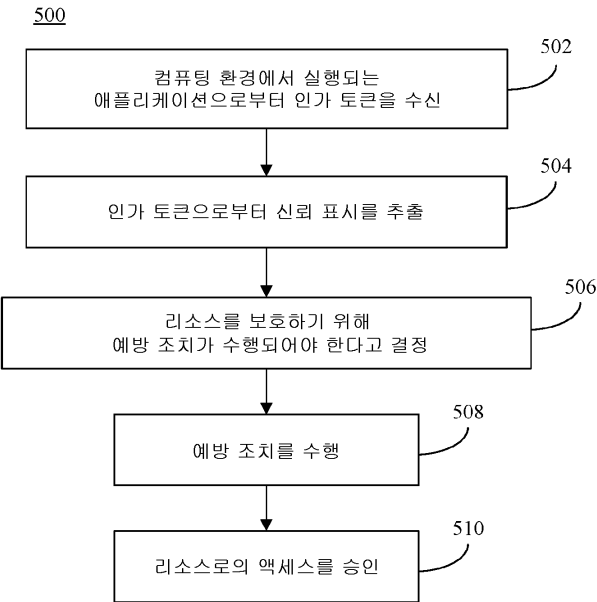
도면3



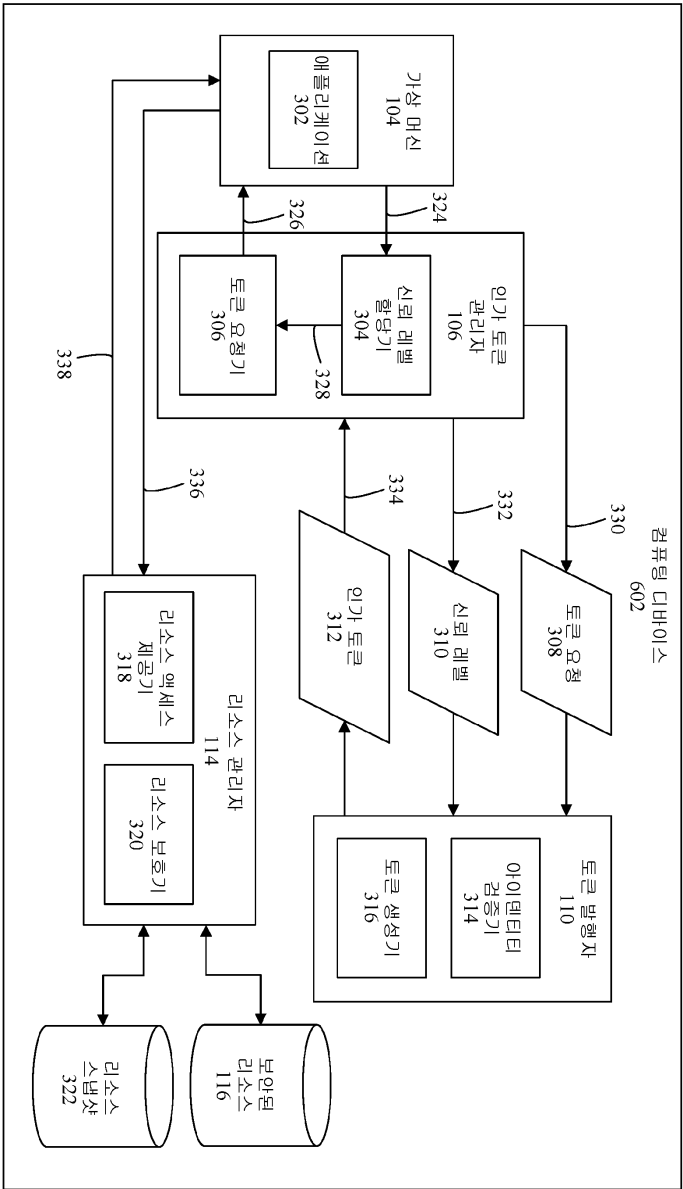
도면4



도면5



도면6



600

도면7

