(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월12일
(11) 등록번호 10-1429434
(24) 등록일자 2014년08월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/53 (2013.01) *G06F 21/44* (2013.01)
(21) 출원번호 10-2013-0026746
(22) 출원일자 2013년03월13일
심사청구일자 2013년03월13일
(56) 선행기술조사문헌
KR1020130007373 A
KR1020110051028 A
KR1020120056300 A
KR1020120061249 A

(73) 특허권자
한국과학기술원
대전광역시 유성구 대학로 291(구성동)
(72) 발명자
맹승렬
대전 유성구 대학로 291, 전산학과 (구성동, 한국과학기술원)
최재원
대전 유성구 대학로 291, 전산학과 4414호 (구성동, 한국과학기술원)
진성욱
대전 유성구 대학로 291, (구성동, 한국과학기술원)
(74) 대리인
특허법인충현

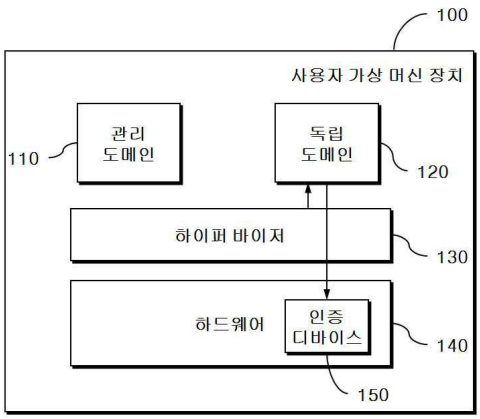
전체 청구항 수 : 총 13 항 심사관 : 구본재

(54) 발명의 명칭 **클라우드 컴퓨팅 환경에서 사용자 가상 머신 실행환경의 신뢰성 향상 장치 및 방법**

(57) 요 약

본 발명은 클라우드 컴퓨팅 환경에서의 사용자 가상 머신 장치에 관한 것으로서 가상 머신을 생성하고 관리하는 관리 도메인, 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스, 상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 상기 인증 디바이스를 격리시키는 하이퍼바이저, 및 상기 인증 디바이스에 전용 접근하는 독립 도메인을 포함함으로써, 신뢰성이 향상된 클라우드 서비스를 제공할 수 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	KI002090
부처명	지식경제부
연구사업명	지식경제기술혁신사업
연구과제명	신뢰성 컴퓨팅 기반 기술 개발
기 여 율	1/1
주관기관	한국과학기술원
연구기간	2012.03.01 ~ 2013.02.28

특허청구의 범위

청구항 1

클라우드 컴퓨팅 환경에서의 사용자 가상 머신 장치에 있어서,

가상 머신을 생성하고 관리하는 관리 도메인;

상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스;

상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 상기 인증 디바이스를 격리시키는 하이퍼바이저; 및

상기 인증 디바이스에 전용 접근하는 독립 도메인을 포함하고,

상기 하이퍼바이저는,

입출력 메모리 관리장치(IOMMU)의 입출력 페이지 테이블을 이용하여 상기 독립 도메인만 상기 인증 디바이스에 접근할 수 있도록 하는 것을 특징으로 하는 장치.

청구항 2

제 1 항에 있어서,

상기 인증 디바이스는 영구적으로 데이터를 저장하고 암호 연산들을 지원하는 하드웨어 디바이스이거나, 영구적으로 데이터를 저장하는 PCI 디바이스인 것을 특징으로 하는 장치.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 하이퍼바이저는,

상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값을 비교하고,

상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 관리 도메인으로부터 수신한 독립 도메인의 커널 이미지를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행시키는 것을 특징으로 하는 장치.

청구항 5

제 1 항에 있어서,

상기 독립 도메인은 상기 가상 머신의 인증을 위해 인증기관과 통신하는 인증 프로토콜을 포함하는 장치.

청구항 6

제 5 항에 있어서,

상기 관리 도메인은,

사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신하면, 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께

상기 선택된 노드에 전송하며,

상기 인증 프로토콜은,

상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 상기 가상 머신을 인증하기 위하여 인증기관에 전송하고,

상기 가상 머신은,

상기 가상 머신의 커널 이미지의 해시 값이 상기 인증기관이 저장하고 있는 가상 머신의 커널 이미지 해시 값 리스트 중 하나와 일치하는 경우 인증되는 것을 특징으로 하는 장치.

청구항 7

클라우드 컴퓨팅 환경에서의 사용자 가상 머신 시스템에 있어서,

가상 머신을 생성하고 관리하는 관리 도메인;

상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스;

상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 상기 인증 디바이스를 격리시키는 하이퍼바이저;

상기 인증 디바이스에 전용 접근하고, 상기 가상 머신의 인증을 위해 인증기관과 통신하는 인증 프로토콜을 포함하는 독립 도메인; 및

상기 인증 프로토콜과 통신을 통해 수신한 상기 가상 머신의 커널 이미지의 해시 값을 이용하여 상기 가상 머신을 인증하는 인증기관을 포함하고,

상기 하이퍼바이저는,

입출력 메모리 관리장치(IOMMU)의 입출력 페이지 테이블을 이용하여 상기 독립 도메인만 상기 인증 디바이스에 접근할 수 있도록 하는 것을 특징으로 하는 시스템.

청구항 8

제 7 항에 있어서,

상기 하이퍼바이저는,

상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값을 비교하고,

상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 관리 도메인으로부터 수신한 독립 도메인의 커널 이미지를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행시키는 것을 특징으로 하는 시스템.

청구항 9

제 7 항에 있어서,

사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신하면, 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송하며,

상기 인증 프로토콜은,

상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 상기 가상 머신을 인증하기 위하여 인증기관에 전송하고,

상기 인증기관은 상기 인증 프로토콜로부터 수신한 상기 가상 머신의 커널 이미지의 해시 값을 미리 저장하고 있는 해시 값 리스트와 비교함으로써 상기 가상 머신을 인증하고, 상기 수신한 난스와 시큐어셸 호스트 키를 상

기 인증기관의 키를 이용하여 서명한 후 상기 사용자에게 송신하는 것을 특징으로 하는 시스템.

청구항 10

클라우드 컴퓨팅 환경에서의 사용자 가상 머신의 신뢰성 향상 방법에 있어서,

관리 도메인의 디스크 드라이버를 이용하여 관리 도메인의 메모리에 독립 도메인의 커널 이미지를 저장하는 단계;

상기 관리 도메인이 저장하고 있는 상기 독립 도메인의 커널 이미지를 하이퍼바이저로 전달하는 단계;

상기 하이퍼바이저가 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값과 일치하는지 판단하는 단계;

상기 판단결과, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 하이퍼바이저가 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행시키는 단계를 포함하고,

상기 독립 도메인은 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스를 전용 접근하며,

상기 하이퍼바이저는,

입출력 메모리 관리장치(IOMMU)의 입출력 페이지 테이블을 이용하여 상기 독립 도메인만 상기 인증 디바이스에 접근할 수 있도록 하는 것을 특징으로 하는 것을 특징으로 하는 방법.

청구항 11

제 10 항에 있어서,

상기 인증 디바이스는 영구적으로 데이터를 저장하고 암호 연산들을 지원하는 하드웨어 디바이스이거나, 영구적으로 데이터를 저장하는 PCI 디바이스인 것을 특징으로 하는 방법.

청구항 12

제 10 항에 있어서,

상기 하이퍼바이저는,

입출력 메모리 관리장치(IOMMU)의 입출력 페이지 테이블을 이용하여 상기 독립 도메인만 상기 인증 디바이스에 접근할 수 있도록 하는 것을 특징으로 하는 방법.

청구항 13

클라우드 컴퓨팅 환경에서의 사용자 가상 머신의 신뢰성 향상 방법에 있어서,

관리 도메인이 사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신하는 단계;

상기 관리 도메인이 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송하는 단계;

상기 노드가 상기 가상 머신의 커널 이미지의 해시 값을 산출하고, 상기 가상 머신을 실행시키는 단계; 및

독립 도메인의 인증 프로토콜이 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 인증기관에 전송하여 상기 가상 머신에 대한 인증을 받는 단계를 포함하고,

상기 독립 도메인은,

상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스를 전용 접근하고,

상기 가상 머신은,

상기 인증기관이 수신한 상기 가상 머신의 커널 이미지의 해시 값과 상기 인증기관이 저장하고 있는 가상 머신의 커널 이미지의 해시 값 리스트 중 하나와 일치하는 경우, 상기 수신한 가상 머신의 커널 이미지는 악의적인 관리자에 의해 변경되지 않은 것으로 판단하고, 상기 수신한 난스와 시큐어셀 호스트 키를 상기 인증기관의 키를 이용하여 서명한 후, 사용자에게 전달함으로써 인증되는 것을 특징으로 하는 방법.

청구항 14

제 10 항 내지 제 13 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 사용자 가상 머신 장치에 관한 것으로서, 보다 상세하게는 독립된 독립 도메인을 이용하여 가상 머신을 인증함으로써, 관리 도메인이 악의적일지라도 가상 머신의 신뢰성을 보장해줄 수 있는 장치에 관한 것이다.

배 경 기 술

[0002] 클라우드 컴퓨팅은 컴퓨팅 자원을 효율적으로 관리 및 활용하여 비용을 절감할 수 있는 컴퓨팅 모델로써 최근 많은 관심을 받고 있다. 클라우드 서비스 제공자(Cloud Service Provider, CSP)는 컴퓨팅 자원을 관리하여 클라우드 사용자(Cloud Customer)의 요구에 따라 자원을 배분하고, 클라우드 사용자는 자원을 필요에 따라 클라우드 서비스 제공에게 요청함으로써 실제 물리적 컴퓨팅 환경을 구축할 필요 없이 원하는 만큼의 컴퓨팅 자원을 사용하고, 사용량에 따라 클라우드 제공자에게 비용을 지불하게 된다. 클라우드 컴퓨팅은 제공하는 서비스에 따라 여러 가지 모델로 구분할 수 있는데, 그 중 사용자에게 가상 머신 단위로 서비스를 제공하는 IaaS (Infrastructure as a Service) 모델에서 사용자는 클라우드 서비스 제공자가 제공하는 가상 머신을 자신의 물리적 머신과 같이 사용하게 된다. 클라우드 서비스 제공자는 클라우드 사용자에게 가상 머신을 제공하기 위해 가상화(Virtualization)라는 기술을 통하여 서비스를 제공한다. 가상화는 하나의 물리적 머신의 자원을 관리하여 여러 개의 가상 머신이 공유할 수 있도록 제어하는 기술이며, 주로 하이퍼바이저(Hypervisor)와 관리 도메인(Management domain)으로 구성된다. 하이퍼바이저는 CPU와 메모리를 관리하며, 관리 도메인은 나머지 모든 하드웨어 장치를 가상 머신이 공유할 수 있도록 제어하는 역할을 한다.

발명의 내용

해결하려는 과제

[0003] 본 발명이 해결하고자 하는 첫 번째 과제는 관리 도메인과 독립된 독립 도메인을 이용하여 가상 머신을 인증함으로써, 가상 머신의 신뢰성을 향상시키는 사용자 가상 머신 장치를 제공하는 것이다.

[0004] 본 발명이 해결하고자 하는 두 번째 과제는 관리 도메인과 독립된 독립 도메인을 이용하여 가상 머신을 인증함으로써, 가상 머신의 신뢰성을 향상시키는 사용자 가상 머신 시스템을 제공하는 것이다.

[0005] 본 발명이 해결하고자 하는 세 번째 과제는 관리 도메인과 독립된 독립 도메인을 이용하여 가상 머신을 인증함으로써, 가상 머신의 신뢰성을 향상시키는 사용자 가상 머신의 신뢰성을 향상시키는 방법을 제공하는 것이다.

과제의 해결 수단

[0006] 본 발명은 상기 첫 번째 과제를 해결하기 위하여, 클라우드 컴퓨팅 환경에서의 사용자 가상 머신 장치에 있어서, 가상 머신을 생성하고 관리하는 관리 도메인; 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는

인증 디바이스; 상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 상기 인증 디바이스를 격리시키는 하이퍼바이저; 및 상기 인증 디바이스에 전용 접근하는 독립 도메인을 포함하는 장치를 제공한다.

[0007] 본 발명의 일 실시예에 따르면, 상기 인증 디바이스는 영구적으로 데이터를 저장하고 암호 연산들을 지원하는 하드웨어 디바이스이거나, 영구적으로 데이터를 저장하는 PCI 디바이스인 것을 특징으로 하는 장치일 수 있고, 상기 하이퍼바이저는, 입출력 메모리 관리장치(IOMMU)의 입출력 페이지 테이블을 이용하여 상기 독립 도메인만 상기 인증 디바이스에 접근할 수 있도록 하는 것을 특징으로 하는 장치일 수 있다.

[0008] 본 발명의 다른 실시예에 따르면, 상기 하이퍼바이저는, 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값을 비교하고, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 관리 도메인으로부터 수신한 독립 도메인의 커널 이미지를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행시키는 장치일 수 있다.

[0009] 본 발명의 다른 실시예에 따르면, 상기 독립 도메인은 상기 가상 머신의 인증을 위해 인증기관과 통신하는 인증 프로토콜을 포함할 수 있고, 상기 관리 도메인은, 사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신하면, 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송하며, 상기 인증 프로토콜은, 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 상기 가상 머신을 인증하기 위하여 인증기관에 전송하고, 상기 가상 머신은, 상기 가상 머신의 커널 이미지의 해시 값이 상기 인증기관이 저장하고 있는 가상 머신의 커널 이미지 해시 값 리스트 중 하나와 일치하는 경우 인증되는 것을 특징으로 하는 장치일 수 있다.

[0010] 본 발명은 상기 두 번째 과제를 해결하기 위하여, 클라우드 컴퓨팅 환경에서의 사용자 가상 머신 시스템에 있어서, 가상 머신을 생성하고 관리하는 관리 도메인; 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스; 상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 상기 인증 디바이스를 격리시키는 하이퍼바이저; 상기 인증 디바이스에 전용 접근하고, 상기 가상 머신의 인증을 위해 인증기관과 통신하는 인증 프로토콜을 포함하는 독립 도메인; 및 상기 인증 프로토콜과 통신을 통해 수신한 상기 가상 머신의 커널 이미지의 해시 값을 이용하여 상기 가상 머신을 인증하는 인증기관을 포함하는 시스템을 제공한다.

[0011] 본 발명은 상기 세 번째 과제를 해결하기 위하여, 클라우드 컴퓨팅 환경에서의 사용자 가상 머신의 신뢰성 향상 방법에 있어서, 관리 도메인의 디스크 드라이버를 이용하여 관리 도메인의 메모리에 상기 독립 도메인의 커널 이미지를 저장하는 단계; 상기 관리 도메인이 저장하고 있는 상기 독립 도메인의 커널 이미지를 하이퍼바이저로 전달하는 단계; 상기 하이퍼바이저는 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값과 일치하는지 판단하는 단계; 상기 판단결과, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 하이퍼바이저가 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행시키는 단계를 포함하고, 상기 독립 도메인은 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스를 전용 접근하는 것을 특징으로 하는 방법을 제공한다.

발명의 효과

[0012] 본 발명에 따르면, 하드웨어를 가상 머신이 공유할 수 있도록 제어하는 관리 도메인으로부터 독립된 도메인과 디바이스를 사용하여, 독립된 도메인에서 관리 도메인을 거치지 않고 디바이스를 직접 접근함으로써 인증기관의 인증서를 안전하게 접근할 수 있다. 따라서 악의적인 관리자는 독립된 도메인이 하드웨어 디바이스로부터 읽으려는 데이터에 대한 접근을 하지 못함으로써 프로토콜이 안전하게 수행할 수 있도록 보장할 수 있다. 이를 통해 클라우드 사용자의 가상 머신은 관리 도메인으로부터 메모리를 보호하는 신뢰성 하이퍼바이저에서만 수행할 수 있도록 보장한다. 또한 독립된 도메인을 사용하여 관리 도메인을 통하지 않고 하드웨어를 접근함으로써 클라우드 서비스 제공자는 서비스 측면에서 보았을 때 사용자에게 더욱 높은 신뢰성 서비스를 제공하기 위해 데이터 보호에 필요한 키를 안전하게 저장하고 사용할 수 있다. 나아가, 클라우드 사용자는 클라우드 서비스 제공자를 더욱 신뢰하여 사용할 수 있고, 클라우드 서비스 제공자 역시 신뢰성 있는 서비스를 제공함으로써 클라우드 컴퓨팅의 확산에 일조할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일 실시예에 따른 사용자 가상 머신 장치의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 사용자 가상 머신 시스템의 블록도이다.

도 3 내지 4는 본 발명의 실시예에 따른 사용자 가상 머신 장치이다.

도 5는 본 발명의 실시예에 따른 사용자 가상 머신 장치의 독립 도메인을 실행시키는 것을 도시한 것이다.

도 6은 본 발명의 실시예에 따른 사용자 가상 머신 장치의 가상 머신을 인증하는 방법을 도시한 것이다.

도 7은 본 발명의 일 실시예에 따른 사용자 가상 머신의 신뢰성을 향상시키는 방법의 흐름도이다.

도 8은 본 발명의 실시예에 따른 사용자 가상 머신의 신뢰성을 향상시키는 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 혹은 기술적 사상의 핵심을 우선 제시한다.

[0015] 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 사용자 가상 머신 장치는 가상 머신을 생성하고 관리하는 관리 도메인, 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스, 상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 상기 인증 디바이스를 격리시키는 하이퍼바이저, 및 상기 인증 디바이스에 전용 접근하는 독립 도메인을 포함한다.

[0016] 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 실시 예를 상세히 설명한다. 그러나 이들 실시예는 본 발명을 보다 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 의하여 제한되지 않는다는 것은 당업계의 통상의 지식을 가진 자에게 자명할 것이다.

[0017] 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세하게 설명함에 있어 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0018] 클라우드 컴퓨팅의 많은 장점에도 불구하고 가장 중요시되고 있는 문제점은 바로 클라우드 서비스 제공자의 신뢰성 문제이다. 클라우드 컴퓨팅 환경에서 모든 사용자의 데이터와 그에 대한 연산은 클라우드 사용자의 머신이 아니라 클라우드 서비스 제공자에 의해 관리되는 머신에서 처리되고 관리된다. 이러한 환경에서 클라우드 관리자는 관리 도메인을 통하여 악의적으로 시스템의 권한을 사용하여 클라우드 사용자 가상 머신의 메모리에 접근함으로써 사용자 가상 머신의 데이터를 볼 수 있다. 이를 해결하기 위해 하이퍼바이저를 수정하여 관리 도메인으로부터 사용자 가상 머신을 보호하려는 신뢰성 하이퍼바이저의 구현이 필요하다. 하지만 클라우드 컴퓨팅 환경에서 사용자 가상 머신은 클라우드 서비스 제공자가 관리하는 데이터센터의 어느 물리머신에서 실행될지 알 수 없고, 가상 머신 실행 중에도 마이그레이션을 통해 다른 물리머신으로 실행이 옮겨질 수 있다. 따라서 이러한 가상 머신 관리 연산을 제대로 제어하지 못하면 클라우드 사용자 가상 머신을 보호할 수 없게 된다. 이를 위해 제 3의 인증기관 (Certificate Authority)을 통하여 인증받은 물리머신만 사용자 가상 머신을 실행할 수 있도록 제한하는 프로토콜이 제안되었으나, 이를 실제 현재의 가상화 환경에 실현할 때 하드웨어를 관리 도메인이 직접 관리하기 때문에 프로토콜 동작에 필요한 인증기관의 인증서를 관리 도메인을 통하여 읽어와야만 한다. 따라서 이 과정에서 악의적인 관리자는 관리 도메인의 권한을 통해 하드웨어 접근을 마음대로 조정할 수 있으며, 따라서 인증기관의 인증서를 변경할 수 있다. 이러한 환경에서 더 이상 프로토콜은 안전하게 수행된다고 보장할 수 없으며 따라서 클라우드 사용자의 가상 머신을 안전하지 보호하지 못하게 된다.

[0019] 또한 프로토콜은 인증을 하기 위해 여러 암호 함수와 라이브러리들을 요구하게 된다. 이것은 프로토콜의 코드 양을 증가시키게 되고, 결국 프로토콜 자체가 취약성을 내포하게 된다는 것을 뜻한다. 이러한 프로토콜이 시스템에서 가장 높은 권한으로 동작하는 하이퍼바이저에서 수행한다는 것은 하이퍼바이저의 복잡도를 높이게 되고 전체 시스템의 신뢰성을 떨어뜨리는 원인이 된다. 따라서 프로토콜을 하이퍼바이저에서 실행시키는 것이 아니라 보다 낮은 권한을 가진 곳에서 실행될 수 있도록 하여 시스템의 신뢰성을 향상시킬 필요가 있다.

[0020] 본 발명에서는 독립된 도메인을 사용하여, 관리 도메인을 사용하지 않고서도 하드웨어를 접근함으로써 악의적인 관리자가 인증기관의 인증서를 변경하지 못하도록 하고자 한다. 가상화 기술은 기본적으로 하드웨어 자원을 가상 머신이 공유할 수 있도록 제어를 하기위해 관리 도메인에서 관리하도록 한다. 따라서 관리 도메인이 모든 하드웨어 접근을 위한 디바이스 드라이버를 가지며, 하이퍼바이저는 메모리와 CPU만 관리함으로써 하이퍼바이저의 복잡도를 낮춰 신뢰성을 향상시킨다. 하지만 성능이나 보안 등의 특수한 목적으로 물리 가상 머신에 설치된 디바이스를 가상 머신 전용으로 사용할 수 있게 한다. 가상 머신이 하드웨어를 직접 접근하여 사용할 경우 다른 가상 머신과 하드웨어 장치를 공유하여 사용할 수 없는 단점이 있지만, 이를 통해 가상 머신이 하드웨어를 접근함으로써 관리 도메인을 거치지 않으므로 입출력 성능 향상과 신뢰성을 향상시킬 수 있다. 본 발명에서는 가상 머신간의 공유를 필요로 하지 않는 하드웨어를 사용하여 독립된 도메인이 직접 접근하여 사용하도록 함으로써 인증기관을 인증서를 관리 도메인을 거치지 않고 안전하게 접근하도록 한다. 따라서 악의적인 관리자는 독립된 도메인이 하드웨어 접근을 하더라도 중간에 개입할 수가 없다. 이하, 이를 구현하기 위한 본 발명의 실시예에 따른 사용자 가상 머신 장치에 대해 자세히 설명하도록 한다.

[0021] 도 1은 본 발명의 일 실시예에 따른 사용자 가상 머신 장치의 블록도이다.

[0022] 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서 사용자 가상 머신 장치(100)는 관리 도메인(110), 독립 도메인(120), 하이퍼바이저(130), 및 인증 디바이스(150)로 구성된다.

[0023] 관리 도메인(110)은 가상 머신을 생성하고 관리한다.

[0024] 보다 구체적으로, 관리 도메인(110)은 가상 머신을 생성하는데 필요한 각종 드라이버를 포함하고 있다. 하지만, 인증 디바이(150)스에 대한 접근 권한이 제한되는바, 악의적인 관리자가 관리 도메인(110)을 통해 사용자의 인증 디바이스(150)에 접근하는 것이 불가능하다.

[0025] 독립 도메인(120)은 인증 디바이스(150)에 전용 접근한다.

[0026] 보다 구체적으로, 관리 도메인(110)이 아닌, 관리 도메인(110)과 독립된 별도의 독립 도메인(120)을 생성하고, 인증 디바이스(150)는 오직 독립 도메인(120)을 통해서만 접근이 가능하도록 한다. 독립 도메인(120)만이 인증 디바이스(150)에 전용 접근할 수 있고, 관리 도메인(110)은 인증 디바이스(150)로의 접근이 제한된다.

[0027] 인증 디바이스(150)는 상기 가상 머신을 인증하기 위한 인증 데이터를 저장한다.

[0028] 보다 구체적으로, 인증 디바이스(150)는 인증서 저장용도로 사용된다. 인증 디바이스(150)를 인증 데이터를 저장하는데 사용하기 위하여, 인증 디바이스(150)는 영구적으로 데이터를 저장하고 암호 연산들을 지원하는 하드웨어 디바이스이거나, 영구적으로 데이터를 저장하는 PCI 디바이스일 수 있다. 인증서의 신뢰성을 높이기 위하여, 독립 도메인(120) 이외의 관리 도메인(110) 또는 다른 가상 머신의 접근을 제한하도록 하이퍼바이저(130)에 의해 격리된다.

[0029] 하이퍼바이저(130)는 상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 인증 디바이스(150)를 격리시킨다.

[0030] 보다 구체적으로, 하이퍼바이저(130)는 하나 이상의 가상 머신들이 하드웨어를 공유하며 실행되기 위한 가상 플랫폼이며, 독립 도메인(120)이 전용 접근할 수 있도록 인증 디바이스(150)를 격리시킨다. 이를 위하여, 하이퍼바이저(130)는 입출력 메모리 관리장치(IOMMU, I/O Memory Managemaent Unit)의 입출력 페이지 테이블을 이용하여 독립 도메인(120)만 상기 인증 디바이스에 접근할 수 있도록 한다. 상기 입출력 메모리 관리장치는 가상화 환경에서 안전한 DMA(Direct Memory Access)를 지원하기 위하여 사용된다. 상기 입출력 메모리 관리장치에서 사용되는 입출력 페이지 테이블을 관리하여 독립 도메인(120)만 인증 디바이스(150)에 접근할 수 있도록 하고, 관리 도메인(110)이나 다른 가상 머신에서 인증 디바이스(150)에 접근할 수 없도록 한다.

[0031] 독립 도메인(120) 역시 하나의 가상 머신으로써 기본적으로 관리 도메인(110)에 의해 생성되고 관리된다. 따라서, 독립 도메인(120)의 생성과정에서 관리 도메인(110)이 악의적으로 독립 도메인(120)의 커널 이미지를 변경한다면 독립 도메인(120)의 실행환경이 안전하다고 할 수 없다. 독립 도메인(120)의 커널 이미지를 관리 도메인(110)이 변경하지 못하도록 막기 위하여, 하이퍼바이저(130)가 직접 독립 도메인(120)의 커널 이미지 정보를 메모리에 저장함으로써 독립 도메인(120)의 커널 이미지를 보호할 수 있다.

[0032] 이를 구현하기 위하여, 하이퍼바이저(130)는 관리 도메인(110)으로부터 수신한 독립 도메인(120)의 커널이미지

로부터 제 1 해시 값을 생성한 뒤, 하이퍼바이저(130)가 저장하고 있는 독립 도메인(120)의 커널 이미지의 제 2 해시 값을 상기 제 1 해시 값과 비교하고, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 관리 도메인(110)으로부터 수신한 독립 도메인(120)의 커널 이미지를 독립 도메인(120)에 로드함으로써 독립 도메인(120)을 실행시킬 수 있다.

[0033] 일반적인 가상 머신 생성과정에서 관리 도메인(110)은 디스크 드라이버를 사용하여 하드웨어(140)로부터 생성할 가상 머신의 커널 이미지를 관리 도메인(110)의 메모리에 저장한다. 그 후 관리 도메인(110)은 직접 새로운 가상 머신의 메모리에 상기 가상 머신의 커널 이미지를 로드한다. 이 과정에서 관리 도메인(110)은 새로운 가상 머신의 커널 이미지를 변경할 수 있다. 따라서, 독립 도메인(120)은 하나의 가상 머신인바, 독립 도메인(120)를 생성함에 있어서, 독립 도메인(120)의 커널 이미지를 관리 도메인(110)으로부터 보호할 필요가 있다. 관리 도메인(110)의 디스크 드라이버를 통하여 독립 도메인(120)의 커널 이미지를 관리 도메인(110)의 메모리에 저장하는 과정은 동일하다. 그 후 관리 도메인(110)은 독립 도메인(120)의 커널 이미지를 하이퍼바이저(130)로 전달하고, 하이퍼바이저(130)는 해시 검사를 통해 상기 수신한 독립 도메인(120)의 커널 이미지의 제 1 해시 값을 산출하고, 상기 제 1 해시 값과 하이퍼바이저(130)가 저장하고 있는 제 2 해시 값이 일치하는 경우에만 상기 관리 도메인(110)으로부터 수신한 독립 도메인(120)의 커널 이미지를 독립 도메인(120)의 메모리로 로드함으로써 독립 도메인(120)을 실행시킨다. 상기 해시 검사는 독립 도메인(120)의 커널 이미지가 관리 도메인(110)에 의해 변경되었는지 확인을 하기 위해 사용하며, 이때 비교되는 제 2 해시 값은 하이퍼바이저(130)가 부팅할 때부터 가지고 있게 되고, 따라서 관리 도메인(110)은 하이퍼바이저(130)의 메모리에 저장되어 있는 제 2 해시 값을 변경할 수가 없고, 최종적으로 독립 도메인(120)의 커널 이미지 역시 변경할 수 없게 된다. 만약 악의적인 관리자가 독립 도메인(120)의 커널 이미지를 변경하였다면 하이퍼바이저(130)는 상기 해시 검사를 통해 변경을 감지할 수 있다.

[0034] 독립 도메인(120)은 상기 가상 머신의 인증을 위해 인증기관과 통신하는 인증 프로토콜을 포함할 수 있다. 가상 머신에 대한 신뢰성을 확보하기 위하여, 외부의 인증기관을 통해 상기 가상 머신의 인증을 수행하기 위하여, 상기 인증기관과 통신하는 프로토콜을 독립 도메인(120)이 포함할 수 있다. 상기 인증 프로토콜은 하이퍼바이저(130)에 포함될 수도 있다.

[0035] 인증 절차를 구현하는 인증 프로토콜이 인증기관과 통신을 통해 가상 머신에 대한 인증을 수행하기 위해서는 여러 암호함수와 라이브러리들을 필요로 한다. 따라서 인증 프로토콜의 코드 사이즈가 커지고 그에 따라 취약성을 내포할 수 있게 된다. 이러한 인증 프로토콜이 시스템에서 가장 높은 권한으로 동작하는 하이퍼바이저(130)에서 동작하는 것은 시스템의 신뢰성을 떨어뜨리는 원인이 될 수 있다. 따라서, 상기 인증 프로토콜을 하이퍼바이저(130) 보다 낮은 권한으로 동작하는 독립 도메인(120)에서 수행하도록 하여 시스템의 신뢰성을 향상시킬 수 있다. 독립 도메인(120)은 하드웨어 디바이스에 악의적인 관리 도메인(110)을 거치지 않고 접근함과 동시에 인증 프로토콜도 수행할 수 있다. 독립 도메인(120)은 가상 머신의 한 종류로써 하이퍼바이저(130)가 제공해주는 가상의 플랫폼위에서 동작하게 되므로 하이퍼바이저(130) 보다 낮은 권한으로 동작하게 된다. 만약 프로토콜이 취약하게 되어 독립 도메인(120)이 제대로 동작하지 않더라도, 하이퍼바이저(130)는 이에 영향을 받지 않게 되고 따라서 클라우드 사용자의 가상 머신은 아무런 영향을 받지 않고 실행을 계속 유지할 수 있는 장점이 있다.

[0036] 관리 도메인(110)은 사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신하면, 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송하며, 상기 인증 프로토콜은 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 상기 가상 머신을 인증하기 위하여 인증기관에 전송하고, 상기 가상 머신은 상기 가상 머신의 커널 이미지의 해시 값이 상기 인증기관이 저장하고 있는 가상 머신의 커널 이미지 해시 값 리스트 중 하나와 일치하는 경우 인증될 수 있다.

[0037] 독립 도메인(120)을 생성한 후, 사용자로부터 가상 머신 생성 요청을 받는 경우, 상기 가상 머신을 인증하기 위하여 외부의 인증기관의 인증을 이용할 수 있다. 물리 머신에서 가상 머신을 생성해서 실행할 경우에는 해당 가상 머신이 안전한 물리 머신 위에서 생성되고 실행되는지 확인해야 하며, 해당 가상 머신에서 수행 중인 OS가 악의적으로 변경되지 않았다는 것을 인증해야 한다. 클라우드 사용자로부터 가상 머신 생성 요청을 수신한다. 이때, 세션 재사용 공격(Replay Attack)을 방지하기 위해 사용자는 무작위 난수인 난스(nonce)를 함께 보낼 수 있다. 클라우드 서비스 제공자는 데이터 센터의 노드 가운데 하나를 선택하여 사용자의 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하고 가상 머신 명령을 전송할 수 있다. 요청을 받은 노드는 독립 도메인(120)에서 동작하는 인증 프로토콜을 이용하여 생성할 사용자의 가상 머신의 커널 이미지의 해시 값을

산출하고, 가상 머신을 실행시킬 수 있다. 그리고 가상 머신 부팅 과정에서 시큐어셸 호스트 키(ssh host key)를 생성하게 되는데, 인증 프로토콜은 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 상기 시큐어셸 호스트 키를 노드 등록과정에서 생성한 키를 사용하여 서명하고, 이를 인증기관에 전송할 수 있다. 인증기관은 신뢰할 수 있는 사용자 가상 머신의 커널 이미지에 대한 해시 값들을 리스트로 관리하고, 노드로부터 받은 가상 머신의 커널 이미지의 해시 값과 비교하여 일치할 경우 악의적인 관리자로부터 변경되지 않았다는 것으로 판단하고, 난스와 시큐어셸 호스트 키를 인증기관의 키를 이용하여 서명하여 사용자에게 전달할 수 있다. 최종적으로 사용자는 인증기관의 서명을 확인하고, 사용자가 전달한 난스와 일치하는지 확인 후, 인증된 가상 머신을 안전하게 사용할 수 있다. 이때 시큐어셸 호스트 키를 통하여 사용자는 자신이 사용하는 가상 머신이 신뢰성 하이퍼바이저(130) 위에서 동작하고 인증기관에 올바르게 인증받은 것임을 확인할 수 있는바, 상기 가상 머신에 대한 신뢰를 가지고 상기 가상 머신을 사용할 수 있게 된다.

[0038] 도 2는 본 발명의 일 실시예에 따른 사용자 가상 머신 시스템의 블록도이다.

[0039] 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 사용자 가상 머신 시스템(200)은 가상 머신을 생성하고 관리하는 관리 도메인(110), 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스(150), 상기 가상 머신을 실행하기 위한 가상 플랫폼이며, 인증 디바이스(150)를 격리시키는 하이퍼바이저(130), 인증 디바이스(150)에 전용 접근하고, 상기 가상 머신의 인증을 위해 인증기관(210)과 통신하는 인증 프로토콜을 포함하는 독립 도메인(120), 및 인증 프로토콜(121)과 통신을 통해 수신한 상기 가상 머신의 커널 이미지의 해시 값을 이용하여 상기 가상 머신을 인증하는 인증기관(210)을 포함한다.

[0040] 도 1의 사용자 가상 머신 장치(100)와 인증기관(210)를 포함함으로써, 사용자의 사용자 가상 머신 장치(100)에 대한 신뢰성을 확보할 수 있다. 인증기관(210)을 더 포함하는 것 이외에는 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명과 동일하다.

[0041] 즉, 하이퍼바이저(130)는 관리 도메인(110)으로부터 수신한 상기 독립 도메인(120)의 커널 이미지로부터 생성한 제 1 해시 값과 하이퍼바이저(130)가 저장하고 있는 독립 도메인(120)의 커널 이미지의 제 2 해시 값을 비교하고, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 관리 도메인(110)으로부터 수신한 독립 도메인(120)의 커널 이미지를 독립 도메인(120)에 로드함으로써 독립 도메인(120)을 실행시킬 수 있다.

[0042] 또한, 사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신하면, 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송하며, 인증 프로토콜(121)은 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 상기 가상 머신을 인증하기 위하여 인증기관(210)에 전송한다.

[0043] 인증기관(210)은 인증 프로토콜(121)과 통신을 통해 수신한 상기 가상 머신의 커널 이미지의 해시 값을 이용하여 상기 가상 머신을 인증한다.

[0044] 보다 구체적으로, 인증 프로토콜(121)로부터 수신한 상기 가상 머신의 커널 이미지의 해시 값을 미리 저장하고 있는 해시 값 리스트와 비교함으로써 상기 가상 머신을 인증하고, 상기 수신한 난스와 시큐어셸 호스트 키를 인증기관(210)의 키를 이용하여 서명한 후 상기 사용자에게 송신함으로써 상기 가상 머신을 인증할 수 있다. 인증 프로토콜(121)로부터 수신한 가상 머신의 커널 이미지의 해시 값이 신뢰할 수 있는 가상 머신의 커널이미지의 해시 값 리스트 중 하나와 일치하는지를 판단함으로써 상기 가상 머신을 인증한다. 상기 가상 머신의 커널 이미지의 해시 값 리스트는 미리 설정되어 있거나, 클라우드 서비스 제공자로부터 제공받은 신뢰할 수 있는 가상 머신의 커널 이미지의 해시 값들로 설정될 수 있다.

[0045] 상기 가상 머신을 인증한 후, 인증여부를 사용자에게 제공하기 위하여, 인증 프로토콜(121)로부터 수신한 난스와 시큐어셸 호스트 키를 인증기관(210)의 키를 이용하여 서명한 후 상기 사용자에게 송신한다. 사용자는 인증기관(210)으로부터 수신한 난스가 자신이 가상 머신 인증요청시 함께 전송한 난스와 동일한지 판단함으로써, 상기 난스가 동일한 경우, 상기 가상 머신에 대해 신뢰를 갖고 이용할 수 있다.

[0046] 도 3 내지 4는 본 발명의 실시예에 따른 사용자 가상 머신 장치이다.

[0047] 사용자 가상 머신 장치는 관리 도메인(Management domain), 독립 도메인인 미니 도메인(Mini-domain), 신뢰할

수 있는 하이퍼바이저(Trusted Hypervisor), 및 하드웨어(Hardware)로 구성될 수 있다. 관리 도메인은 각종 드라이버(driver)를 포함하고, 가상 머신을 관리(VM manage)하며, 사용자 프로세스(user process)를 수행한다. 독립 도메인인 미니 도메인은 관리 도메인으로부터 생성되는 별도의 도메인인바, 미니 도메인이라 할 수 있다. 인증을 위한 프로토콜은 도 3과 같이, 하이퍼바이저에 위치하거나, 도 4와 같이, 독립 도메인인 미니 도메인에 위치할 수 있다. 도 3과 같이, 인증 프로토콜이 하이퍼바이저에 위치하는 경우보다 도 4와 같이, 하이퍼바이저보다 낮은 권한으로 동작하는 미니 도메인에 위치하는 것이 시스템의 신뢰성을 향상시킬 수 있다. 인증 데이터는 독립 도메인인 미니 도메인이 전용으로 접근하는 신뢰성 플랫폼 보드(TPB, Trusted Platform Board)에 저장될 수 있다. 상기 신뢰성 플랫 보드뿐만 아니라, 영구적인 데이터를 저장할 수 있는 PCI 디바이스에 저장될 수도 있다.

[0048] 도 5는 본 발명의 실시예에 따른 사용자 가상 머신 장치의 독립 도메인을 실행시키는 것을 도시한 것이다.

[0049] 독립 도메인인 미니 도메인을 생성하기 위하여, 우선 관리 도메인이 디스크 드라이버를 이용하여 하드웨어로부터 커널 이미지를 저장한다. 관리 도메인에 의해 상기 커널 이미지가 변형될 수 있는바, 관리 도메인으로부터 바로 커널 이미지를 미니 도메인에 로드하지 않고, 신뢰할 수 있는 하이퍼바이저를 경유하도록 한다. 관리 도메인이 저장하고 있는 커널 이미지로부터 생성된 해시 값을 하이퍼바이저가 저장하고 있는 해시 값과 비교하여, 두 해시 값이 동일한 경우에만 해당 커널 이미지를 미니 도메인에 로드함으로써 미니 도메인을 실행시킬 수 있다. 이를 통해, 악의적인 관리자에 의한 미니 도메인의 커널 이미지 변경을 방지할 수 있다.

[0050] 도 6은 본 발명의 실시예에 따른 사용자 가상 머신 장치의 가상 머신을 인증하는 방법을 도시한 것이다.

[0051] 사용자가 난스(nonce)를 포함하는 가상 머신 생성 요청을 클라우드 관리자(Cloud Manager)에게 전송하면, 클라우드 관리자는 가상 머신을 생성할 노드를 선택하고, 커널 이미지를 복사하여 상기 난스와 함께 해당 노드에 전송한다. 노드는 노드 아이디, 커널 이미지의 해시 값, 난스, 및 시큐어셀 호스트 키를 서명한 후 인증기관(Certificate Authority)로 전송한다. 인증기관은 커널 이미지의 해시 값을 이용하여 가상 머신을 인증하고, 난스 및 시큐어셀 호스트 키를 서명한 후 사용자에게 전송하여 가상 머신이 인증되었음을 알린다. 사용자는 인증기관으로부터 상기 가상 머신이 인증되었음을 확인하고, 상기 가상 머신을 안전하게 이용할 수 있다.

[0052] 도 7은 본 발명의 일 실시예에 따른 사용자 가상 머신의 신뢰성을 향상시키는 방법의 흐름도이다.

[0053] 사용자 가상 머신의 신뢰성을 향상시키기 위하여, 관리 도메인과 독립된 독립 도메인을 이용하여 인증을 수행할 수 있다. 여기서, 독립 도메인은 상기 가상 머신을 인증하기 위한 인증 데이터를 저장하는 인증 디바이스를 전용 접근할 수 있는 도메인이다. 상기 인증 디바이스는 영구적으로 데이터를 저장하고 암호 연산들을 지원하는 하드웨어 디바이스이거나, 영구적으로 데이터를 저장하는 PCI 디바이스일 수 있으며, 하이퍼바이저가 입출력 메모리 관리장치(IOMMU)의 입출력 페이지 테이블을 이용하여 상기 독립 도메인만 상기 인증 디바이스에 접근할 수 있도록 할 수 있다. 독립 도메인은 하나의 가상 머신인바, 상기 독립 도메인이 안전한 환경에서 실행될 수 있도록 도 7의 방법을 수행한다.

[0054] 710단계는 관리 도메인의 디스크 드라이버를 이용하여 관리 도메인의 메모리에 상기 독립 도메인의 커널 이미지를 저장하는 단계이다.

[0055] 보다 구체적으로, 독립 도메인의 커널 이미지를 저장하는 단계로 이는 다른 가상 머신의 커널 이미지를 생성하는 것과 동일하다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로 대신한다.

[0056] 720단계는 상기 관리 도메인이 저장하고 있는 상기 독립 도메인의 커널 이미지를 하이퍼바이저로 전달하는 단계이다.

[0057] 보다 구체적으로, 독립 도메인의 안전한 실행 환경을 위하여, 관리 도메인으로부터 독립 도메인의 커널 이미지를 바로 독립 도메인에 로드하지 않고, 하이퍼바이저를 경유하기 위하여, 상기 관리 도메인이 저장하고 있는 상기 독립 도메인의 커널 이미지를 하이퍼바이저로 전달한다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로

대신한다.

[0058] 730단계는 상기 하이퍼바이저가 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값과 일치하는지 판단하는 단계이다.

[0059] 보다 구체적으로, 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지가 악의적인 관리자에 의해 변경되었는지 확인하기 위하여, 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값과 일치하는지 판단한다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로 대신한다.

[0060] 740단계는 상기 판단결과, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 하이퍼바이저가 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행시키는 단계이다.

[0061] 보다 구체적으로, 730단계의 판단 결과, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지가 악의적인 관리자에 의해 변경되지 않은 것인바, 이를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행시킨다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로 대신한다.

[0062] 도 8은 본 발명의 실시예에 따른 사용자 가상 머신의 신뢰성을 향상시키는 방법의 흐름도이다.

[0063] 사용자 가상 머신의 신뢰성을 향상시키기 위하여, 사용자가 사용하려는 가상 머신에 대한 인증을 수행할 수 있다. 상기 가상 머신의 인증을 위하여 인증기관을 이용할 수 있으며, 상기 인증기관과 통신할 수 있는 인증 프로토콜을 이용할 수 있다. 상기 가상 머신을 인증하기 위하여 도 8의 방법을 수행한다.

[0064] 810단계는 관리 도메인이 사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신하는 단계이다.

[0065] 보다 구체적으로, 사용자로부터 가상 머신 생성 요청을 수시할 때, 세션 재사용 공격을 방지하기 위하여 무작위 난수인 난스를 함께 수신한다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로 대신한다.

[0066] 820단계는 상기 관리 도메인이 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송하는 단계이다.

[0067] 보다 구체적으로, 새로 생성할 가상 머신이 할당될 하드웨어의 노드를 선택하고, 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송한다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로 대신한다.

[0068] 830단계는 상기 노드가 상기 가상 머신의 커널 이미지의 해시 값을 산출하고, 상기 가상 머신을 실행시키는 단계이다.

[0069] 보다 구체적으로, 인증기관의 인증에 필요한 가상 머신의 커널 이미지의 해시 값을 산출하고, 상기 가상 머신을 실행시킨다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로 대신한다.

[0070] 840단계는 독립 도메인의 인증 프로토콜이 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 인증기관에 전송하여 상기 가상 머신에 대한 인증을 받는 단계이다.

[0071] 보다 구체적으로, 인증기관과 통신하는 인증 프로토콜이 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셸 호스트 키(ssh host key)를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 인증기관에 전송한다. 상기 인증기관으로부터 가상 머신에 대한 인증은 다음과 같이 이루어진다. 상기 인증기관이 수신한 상기

가상 머신의 커널 이미지의 해시 값과 상기 인증기관이 저장하고 있는 가상 머신의 커널 이미지의 해시 값 리스트 중 하나와 일치하는 경우, 상기 수신한 가상 머신의 커널 이미지는 악의적인 관리자에 의해 변경되지 않은 것으로 판단하고, 상기 수신한 난스와 시큐어셀 호스트 키를 상기 인증기관의 키를 이용하여 서명한 후, 사용자에게 전달함으로써 인증될 수 있다. 상기 인증기관으로부터 난스와 시큐어셀 호스트 키를 수신한 사용자는 810 단계에서 가상 머신 생성 요청과 함께 전송한 난스와 상기 수신한 난스를 확인하여, 동일한 난스인경우, 해당 가상 머신을 신뢰하고, 안전하게 상기 가상 머신을 이용할 수 있다. 본 단계에 대한 상세한 설명은 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명에 대응하는바, 도 1의 사용자 가상 머신 장치(100)에 대한 상세한 설명으로 대신한다.

[0072] 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체 (magnetic media), CD-ROM, DVD와 같은 광기록 매체 (optical media), 플롭티컬 디스크 (floptical disk)와 같은 자기-광 매체 (magneto-optical media), 및 롬 (ROM), 램 (RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0073] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0074] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0075] 100: 사용자 가상 머신 장치

110: 관리 도메인

120: 독립 도메인

121: 인증 프로토콜

130: 하이퍼바이저

140: 하드웨어

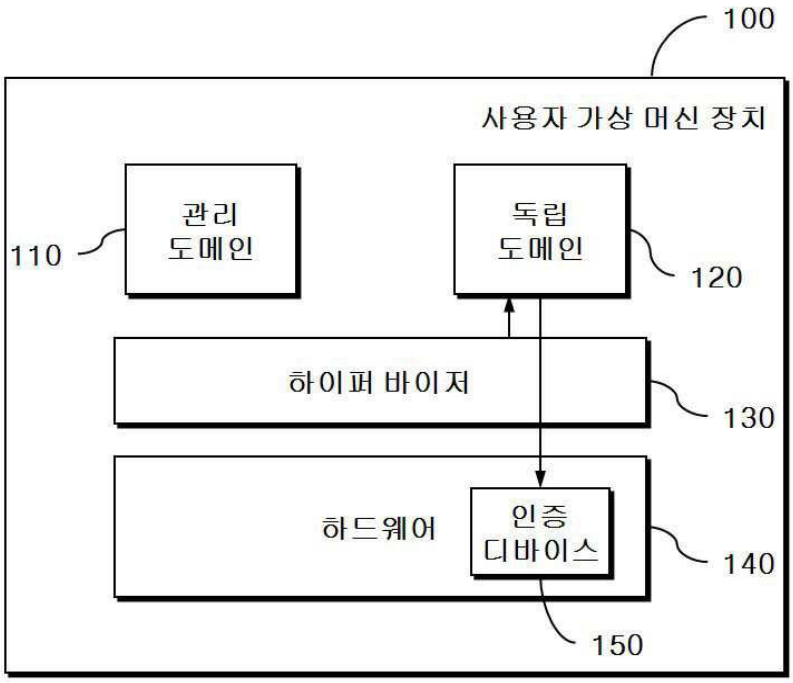
150: 인증디바이스

200: 사용자 가상 머신 시스템

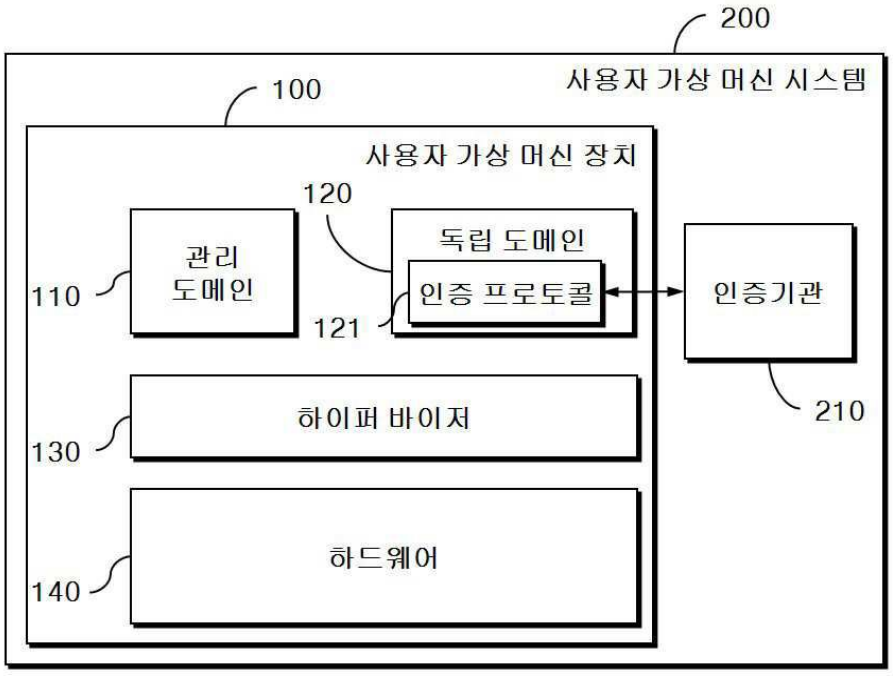
210: 인증기관

도면

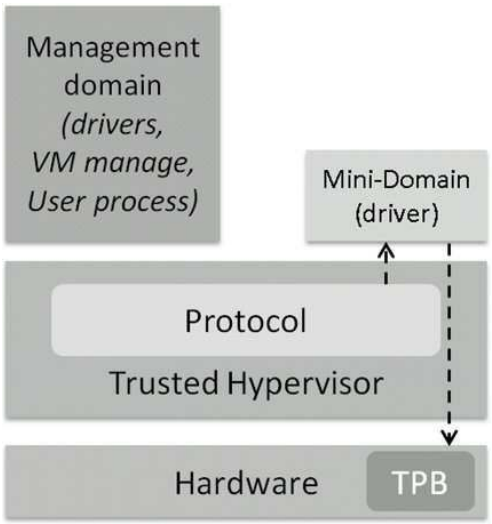
도면1


100
사용자 가상 머신 장치
관리
도메인
110
독립
도메인
120
하이퍼 바이저
130
하드웨어
인증
디바이스
140
150

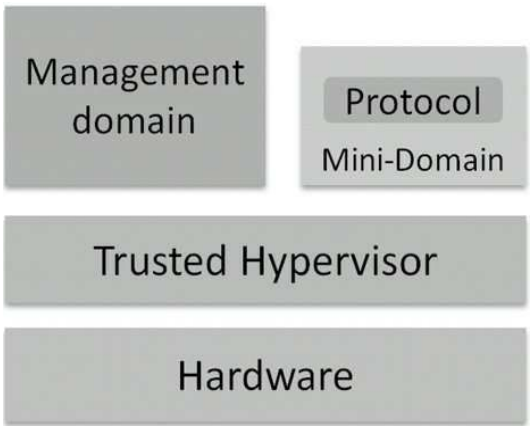
도면2


200
사용자 가상 머신 시스템
100
사용자 가상 머신 장치
120
독립 도메인
관리
도메인
110
인증 프로토콜
121
인증기관
210
하이퍼 바이저
130
하드웨어
140

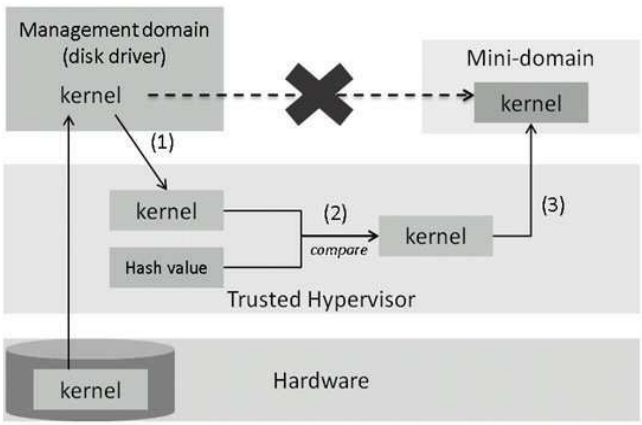
도면3


Management domain (drivers, VM manage, User process)
Mini-Domain (driver)
Protocol
Trusted Hypervisor
Hardware
TPB

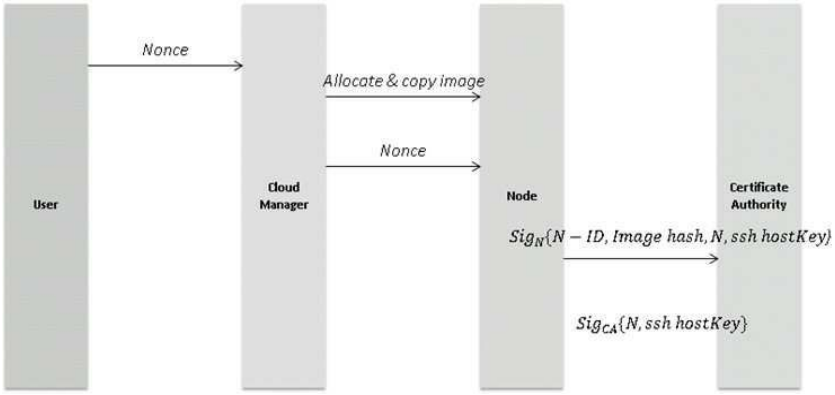
도면4


Management domain
Protocol
Mini-Domain
Trusted Hypervisor
Hardware

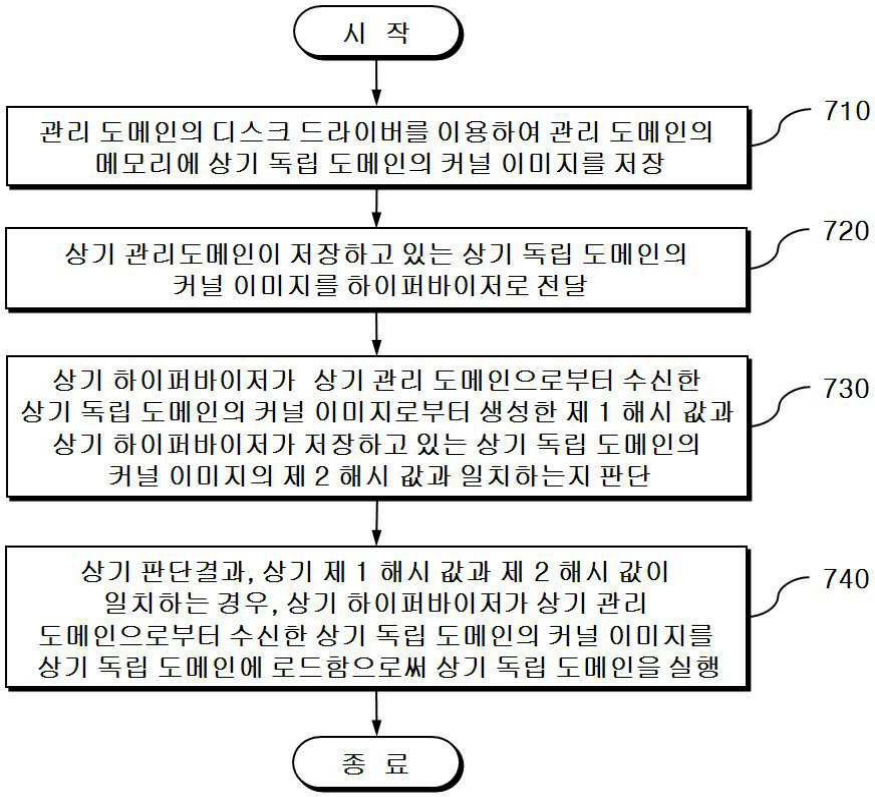
도면5


Management domain (disk driver)
kernel
(1)
Mini-domain
kernel
kernel
(2)
compare
kernel
(3)
Hash value
Trusted Hypervisor
kernel
Hardware

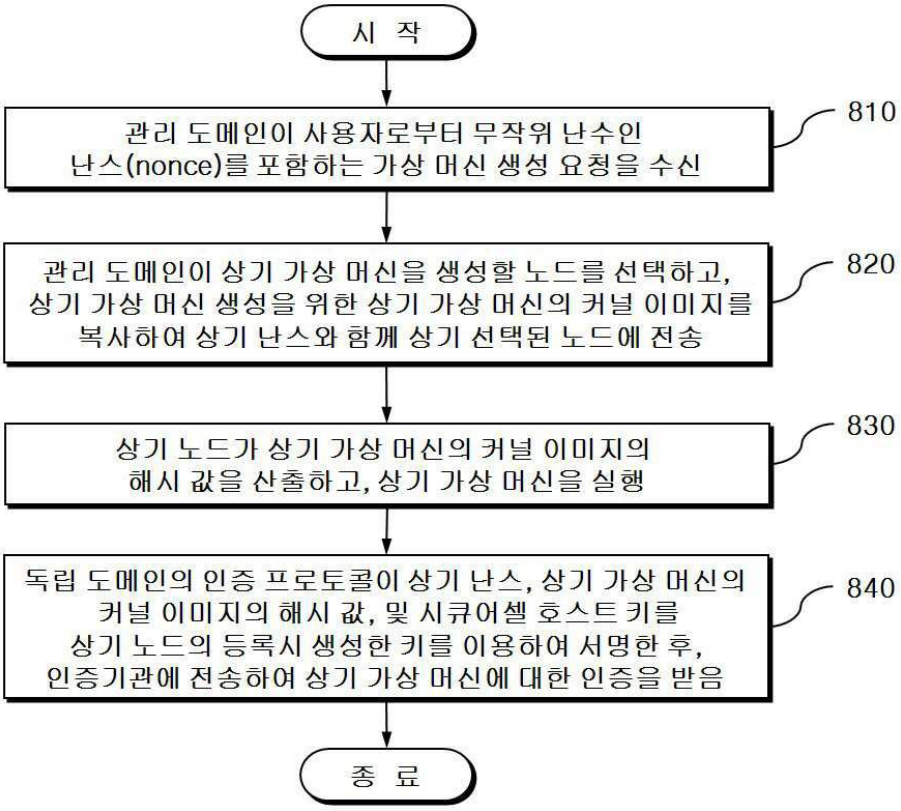
도면6


User
Nonce
Cloud Manager
Allocate & copy image
Nonce
Node
Certificate Authority
$Sig_N\{N-ID, Image\ hash, N, ssh\ hostKey\}$
$Sig_{CA}\{N, ssh\ hostKey\}$

도면7


시 작
관리 도메인의 디스크 드라이버를 이용하여 관리 도메인의 메모리에 상기 독립 도메인의 커널 이미지를 저장
710
상기 관리도메인이 저장하고 있는 상기 독립 도메인의 커널 이미지를 하이퍼바이저로 전달
720
상기 하이퍼바이저가 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지로부터 생성한 제 1 해시 값과 상기 하이퍼바이저가 저장하고 있는 상기 독립 도메인의 커널 이미지의 제 2 해시 값과 일치하는지 판단
730
상기 판단결과, 상기 제 1 해시 값과 제 2 해시 값이 일치하는 경우, 상기 하이퍼바이저가 상기 관리 도메인으로부터 수신한 상기 독립 도메인의 커널 이미지를 상기 독립 도메인에 로드함으로써 상기 독립 도메인을 실행
740
종 료

도면8


시 작
관리 도메인이 사용자로부터 무작위 난수인 난스(nonce)를 포함하는 가상 머신 생성 요청을 수신
810
관리 도메인이 상기 가상 머신을 생성할 노드를 선택하고, 상기 가상 머신 생성을 위한 상기 가상 머신의 커널 이미지를 복사하여 상기 난스와 함께 상기 선택된 노드에 전송
820
상기 노드가 상기 가상 머신의 커널 이미지의 해시 값을 산출하고, 상기 가상 머신을 실행
830
독립 도메인의 인증 프로토콜이 상기 난스, 상기 가상 머신의 커널 이미지의 해시 값, 및 시큐어셀 호스트 키를 상기 노드의 등록시 생성한 키를 이용하여 서명한 후, 인증기관에 전송하여 상기 가상 머신에 대한 인증을 받음
840
종 료