(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0124048
(43) 공개일자 2018년11월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 12/14* (2006.01)
G06F 21/62 (2013.01) *G06F 21/79* (2013.01)
G06F 9/455 (2018.01)
(52) CPC특허분류
G06F 21/602 (2013.01)
G06F 12/1433 (2013.01)
(21) 출원번호 10-2018-7027284
(22) 출원일자(국제) 2017년02월24일
심사청구일자 없음
(85) 번역문제출일자 2018년09월19일
(86) 국제출원번호 PCT/US2017/019396
(87) 국제공개번호 WO 2017/165073
국제공개일자 2017년09월28일
(30) 우선권주장
15/076,936 2016년03월22일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
크리스토도레스쿠 미하이
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
두르자티 디나카르
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
이슬람 나임
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

전체 청구항 수 : 총 28 항

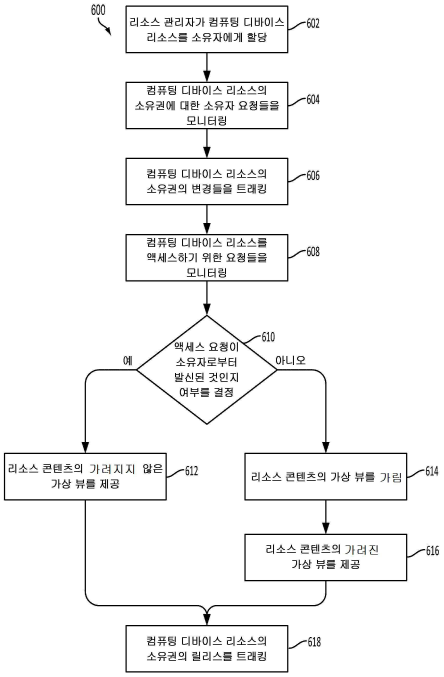
(54) 발명의 명칭 **가상 리소스 뷰들을 이용한 데이터 보호**

(57) 요 약

실시형태들은 리소스 콘텐츠들의 가상 뷰들을 이용하여 데이터를 보호하기 위한 컴퓨팅 디바이스들, 시스템들, 및 방법들을 포함한다. 가상화 인터페이스 모니터는 제 1 요청 엔터티에 의한 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청을 모니터링하고, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정할

(뒷면에 계속)

대 표 도 - 도6



수도 있다. 데이터 보호 시스템은, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 것에 응답하여, 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려지지 않은 가상 뷰를 제 1 요청 엔터티에 제공할 수도 있다. 리소스 콘텐츠 암호화 디바이스는, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가상 뷰를 가릴 수도 있다. 데이터 보호 시스템은, 컴퓨팅 디바이스 리소스의 리소스 콘텐츠의 가려진 가상 뷰를 제 1 요청 엔터티에 제공할 수도 있다.

(52) CPC특허분류
G06F 21/6218 (2013.01)
G06F 21/79 (2013.01)
G06F 9/45558 (2013.01)

명 세 서

청구범위

청구항 1

리소스 콘텐츠들의 가상 뷰들을 이용하여 데이터를 보호하는 방법으로서,

컴퓨팅 디바이스의 가상화 인터페이스 모니터에 의해, 제 1 요청 엔터티에 의한 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청을 모니터링하는 단계;

상기 가상화 인터페이스 모니터에 의해, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 단계;

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려지지 않은 (unobscured) 가상 뷰를 상기 컴퓨팅 디바이스의 데이터 보호 시스템에 의해 상기 제 1 요청 엔터티에 제공하는 단계; 및

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 가려진 (obscured) 가상 뷰를 상기 데이터 보호 시스템에 의해 상기 제 1 요청 엔터티에 제공하는 단계를 포함하는, 데이터를 보호하는 방법.

청구항 2

제 1 항에 있어서,

리소스 콘텐츠 암호화 디바이스에 의해, 상기 제 1 요청 엔터티가 인증된 기능을 갖는지 여부를 결정하는 단계;

상기 리소스 콘텐츠 암호화 디바이스에 의해, 상기 제 1 요청 엔터티가 인증된 기능을 갖는다고 결정하는 것에 응답하여, 상기 제 1 요청 엔터티에 대해 액세스 타입을 결정하는 단계; 및

상기 컴퓨팅 디바이스의 리소스 콘텐츠 암호화 디바이스에 의해, 상기 액세스 타입에 기초한 가림 레벨을 이용하여, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 가리는 단계를 더 포함하는, 데이터를 보호하는 방법.

청구항 3

제 2 항에 있어서,

상기 액세스 타입은 부분적 가려짐 및 가려짐을 포함하고,

상기 액세스 타입에 기초한 가림 레벨을 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 가리는 단계는,

상기 리소스 콘텐츠 암호화 디바이스에 의해, 상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 부분적 가려짐이라고 결정하는 것에 응답하여 호모모픽 암호화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 암호화하는 단계; 및

상기 리소스 콘텐츠 암호화 디바이스에 의해, 상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 가려짐이라고 결정하는 것에 응답하여 강력한 암호화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 암호화하는 단계를 포함하는, 데이터를 보호하는 방법.

청구항 4

제 1 항에 있어서,

상기 가상화 인터페이스 모니터에 의해, 상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경들에 대해 가상화 인터페이스를 모니터링하는 단계; 및

상기 가상화 인터페이스 모니터에 의해, 상기 제 1 요청 엔터티에 대해 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 상기 제 1 요청 엔터티의 제 1 소유자 식별자를 저장하는 단계를 더 포함하고,

상기 제 1 소유자 식별자는, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유권을 승인받는 것 및 상기 가상 리소스 식별자가 상기 컴퓨팅 디바이스 리소스의 물리적 리소스 식별자에 맵핑되는 것을 나타내는, 데이터를 보호하는 방법.

청구항 5

제 4 항에 있어서,

상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경에 대해 가상화 인터페이스를 모니터링하는 단계는, 제 2 요청 엔터티에 의한 상기 컴퓨팅 디바이스 리소스의 소유권에 대한 요청에 대해 모니터링하는 단계를 포함하는, 데이터를 보호하는 방법.

청구항 6

제 1 항에 있어서,

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 단계는,

상기 가상화 인터페이스 모니터에 의해, 상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 가상 리소스 식별자를, 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 저장된 소유자 식별자와 비교하는 단계; 및

상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 상기 가상 리소스 식별자 및 상기 컴퓨팅 디바이스 리소스의 상기 가상 리소스 식별자가 매칭될 때, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 단계를 포함하는, 데이터를 보호하는 방법.

청구항 7

제 1 항에 있어서,

상기 컴퓨팅 디바이스 리소스의 상기 소유자는 애플리케이션이고; 그리고

상기 컴퓨팅 디바이스 리소스의 상기 비-소유자는 오퍼레이팅 시스템 커널, 하이퍼바이저, 및 트러스트존 중 하나를 포함하는 리소스 관리자인, 데이터를 보호하는 방법.

청구항 8

컴퓨팅 디바이스로서,

가상화 인터페이스 모니터 및 리소스 콘텐츠 암호화 디바이스를 포함하는 데이터 보호 시스템을 포함하고,

상기 가상화 인터페이스 모니터는,

제 1 요청 엔터티에 의한 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청을 모니터링하는 동작; 및

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 동작

을 포함하는 동작들을 수행하도록 가상화 인터페이스 모니터 실행가능 명령들로 구성되고, 그리고

상기 데이터 보호 시스템은,

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려지지 않은 가상 뷰를 상기 제 1 요청 엔터티에 제공하는 동작; 및

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 가려진 가상 뷰를 상기 제 1 요청 엔터티에 제공하는 동작

을 포함하는 동작들을 수행하도록 데이터 보호 시스템 실행가능 명령들로 구성되는, 컴퓨팅 디바이스.

청구항 9

제 8 항에 있어서,

상기 리소스 콘텐츠 암호화 디바이스는,

상기 제 1 요청 엔터티가 인증된 기능을 갖는지 여부를 결정하는 동작;

상기 제 1 요청 엔터티가 인증된 기능을 갖는다고 결정하는 것에 응답하여, 상기 제 1 요청 엔터티에 대해 액세스 타입을 결정하는 동작; 및

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 가상 뷰를 가리는 동작

을 더 포함하는 동작들을 수행하도록 리소스 콘텐츠 암호화 디바이스 실행가능 명령들로 구성되는, 컴퓨팅 디바이스.

청구항 10

제 9 항에 있어서,

상기 액세스 타입은 부분적 가려짐 및 가려짐을 포함하고,

상기 리소스 콘텐츠 암호화 디바이스는,

상기 액세스 타입에 기초한 가림 레벨을 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰를 가리는 동작이,

상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 부분적 가려짐이라고 결정하는 것에 응답하여 호모모픽 암호화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰를 암호화하는 동작; 및

상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 가려짐이라고 결정하는 것에 응답하여 강력한 암호화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 암호화하는 동작

을 포함하도록 하는 동작들을 수행하도록 리소스 콘텐츠 암호화 디바이스 실행가능 명령들로 구성되는, 컴퓨팅 디바이스.

청구항 11

제 8 항에 있어서,

상기 가상화 인터페이스 모니터는,

상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경들에 대해 가상화 인터페이스를 모니터링하는 동작; 및

상기 제 1 요청 엔터티에 대해 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 상기 제 1 요청 엔터티의 제 1 소유자 식별자를 저장하는 동작

을 더 포함하는 동작들을 수행하도록 가상화 인터페이스 모니터 실행가능 명령들로 구성되며,

상기 제 1 소유자 식별자는, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유권을 승인받는 것 및 상기 가상 리소스 식별자가 상기 컴퓨팅 디바이스 리소스의 물리적 리소스 식별자에 맵핑되는 것을 나타내는, 컴퓨팅 디바이스.

청구항 12

제 11 항에 있어서,

상기 가상화 인터페이스 모니터는, 상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경에 대해 가상화 인터페이스를 모니터링하는 동작이, 제 2 요청 엔터티에 의한 상기 컴퓨팅 디바이스 리소스의 소유권에 대한 요청에 대해 모니터링하는 동작을 포함하도록 하는 동작들을 수행하도록 가상화 인터페이스 모니터 실행가능 명령들로 구성되는, 컴퓨팅 디바이스.

청구항 13

제 8 항에 있어서,

상기 가상화 인터페이스 모니터는,

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 동작이,

상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 가상 리소스 식별자를, 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 저장된 소유자 식별자와 비교하는 동작; 및

상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 상기 가상 리소스 식별자 및 상기 컴퓨팅 디바이스 리소스의 상기 가상 리소스 식별자가 매칭될 때, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 동작

을 포함하도록 하는 동작들을 수행하도록 가상화 인터페이스 모니터 실행가능 명령들로 구성되는, 컴퓨팅 디바이스.

청구항 14

제 8 항에 있어서,

상기 데이터 보호 시스템에 통신가능하게 접속된 복수의 프로세서들을 더 포함하고,

상기 컴퓨팅 디바이스 리소스의 상기 소유자는 상기 복수의 프로세서들의 제 1 프로세서 상에서 실행되는 애플리케이션이고; 그리고

상기 컴퓨팅 디바이스 리소스의 상기 비-소유자는 상기 복수의 프로세서들의 제 2 프로세서 상에서 실행되는 오퍼레이팅 시스템 커널, 하이퍼바이저, 및 트러스트존 중 하나를 포함하는 리소스 관리자인, 컴퓨팅 디바이스.

청구항 15

리소스 콘텐츠들의 가상 뷰들을 이용하여 데이터를 보호하도록 구성된 컴퓨팅 디바이스로서,

제 1 요청 엔터티에 의한 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청을 모니터링하는 수단;

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 수단;

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려지지 않은 가상 뷰를 상기 제 1 요청 엔터티에 제공하는 수단; 및

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 가려진 가상 뷰를 상기 제 1 요청 엔터티에 제공하는 수단을 포함하는, 컴퓨팅 디바이스.

청구항 16

제 15 항에 있어서,

상기 제 1 요청 엔터티가 인증된 기능을 갖는지 여부를 결정하는 수단; 및

상기 제 1 요청 엔터티가 인증된 기능을 갖는다고 결정하는 것에 응답하여, 상기 제 1 요청 엔터티에 대해 액세스 타입을 결정하는 수단; 및

상기 액세스 타입에 기초한 가림 레벨을 이용하여, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 가리는 수단을 더 포함하는, 컴퓨팅 디바이스.

청구항 17

제 16 항에 있어서,

상기 액세스 타입은 부분적 가려짐 및 가려짐을 포함하고,

상기 액세스 타입에 기초한 가림 레벨을 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 가리는 수단은,

상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 부분적 가려짐이라고 결정하는 것에 응답하여 호모모픽 암호

화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 암호화하는 수단; 및

상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 가려짐이라고 결정하는 것에 응답하여 강력한 암호화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 암호화하는 수단을 포함하는, 컴퓨팅 디바이스.

청구항 18

제 15 항에 있어서,

상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경들에 대해 가상화 인터페이스를 모니터링하는 수단; 및

상기 제 1 요청 엔터티에 대해 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 상기 제 1 요청 엔터티의 제 1 소유자 식별자를 저장하는 수단을 더 포함하고,

상기 제 1 소유자 식별자는, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유권을 승인받는 것 및 상기 가상 리소스 식별자가 상기 컴퓨팅 디바이스 리소스의 물리적 리소스 식별자에 맵핑되는 것을 나타내는, 컴퓨팅 디바이스.

청구항 19

제 18 항에 있어서,

상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경에 대해 가상화 인터페이스를 모니터링하는 수단은, 제 2 요청 엔터티에 의한 상기 컴퓨팅 디바이스 리소스의 소유권에 대한 요청에 대해 모니터링하는 수단을 포함하는, 컴퓨팅 디바이스.

청구항 20

제 15 항에 있어서,

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 수단은,

상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 가상 리소스 식별자를, 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 저장된 소유자 식별자와 비교하는 수단; 및

상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 상기 가상 리소스 식별자 및 상기 컴퓨팅 디바이스 리소스의 상기 가상 리소스 식별자가 매칭될 때, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 수단을 포함하는, 컴퓨팅 디바이스.

청구항 21

제 15 항에 있어서,

상기 컴퓨팅 디바이스 리소스의 상기 소유자는 애플리케이션이고; 그리고

상기 컴퓨팅 디바이스 리소스의 상기 비-소유자는 오퍼레이팅 시스템 커널, 하이퍼바이저, 및 트러스트존 중 하나를 포함하는 리소스 관리자인, 컴퓨팅 디바이스.

청구항 22

프로세서 실행가능 명령들을 저장한 비-일시적 프로세서 판독가능 저장 매체로서,

상기 명령들은 컴퓨팅 디바이스의 프로세서로 하여금,

제 1 요청 엔터티에 의한 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청을 모니터링하는 동작;

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 동작

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려지지 않은 가상 뷰를 상기 제 1 요청 엔터티에 제공하는 동작; 및

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려진 가상 뷰를 상기 제 1 요청 엔터티에 제공하는 동작

을 포함하는 동작들을 수행하게 하도록 구성되는, 비-일시적 프로세서 판독가능 저장 매체.

청구항 23

제 22 항에 있어서,

저장된 상기 프로세서 실행가능 명령들은 상기 프로세서로 하여금,

상기 제 1 요청 엔터티가 인증된 기능을 갖는지 여부를 결정하는 동작;

상기 제 1 요청 엔터티가 인증된 기능을 갖는다고 결정하는 것에 응답하여, 상기 제 1 요청 엔터티에 대해 액세스 타입을 결정하는 동작; 및

상기 액세스 타입에 기초한 가림 레벨을 이용하여, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 비-소유자라고 결정하는 것에 응답하여, 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 가상 뷰를 가리는 동작

을 더 포함하는 동작들을 수행하게 하도록 구성되는, 비-일시적 프로세서 판독가능 저장 매체.

청구항 24

제 23 항에 있어서,

상기 액세스 타입은 부분적 가려짐 및 가려짐을 포함하고,

저장된 상기 프로세서 실행가능 명령들은 상기 프로세서로 하여금,

상기 액세스 타입에 기초한 가림 레벨을 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰를 가리는 동작이,

상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 부분적 가려짐이라고 결정하는 것에 응답하여 호모모픽 암호화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰를 암호화하는 동작; 및

상기 제 1 요청 엔터티에 대한 상기 액세스 타입이 가려짐이라고 결정하는 것에 응답하여 강력한 암호화를 이용하여 상기 컴퓨팅 디바이스 리소스의 상기 리소스 콘텐츠들의 상기 가상 뷰들을 암호화하는 동작

을 포함하도록 하는 동작들을 수행게 하도록 구성되는, 비-일시적 프로세서 판독가능 저장 매체.

청구항 25

제 22 항에 있어서,

저장된 상기 프로세서 실행가능 명령들은 상기 프로세서로 하여금,

상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경들에 대해 가상화 인터페이스를 모니터링하는 동작; 및

상기 제 1 요청 엔터티에 대해 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 상기 제 1 요청 엔터티의 제 1 소유자 식별자를 저장하는 동작

을 더 포함하는 동작들을 수행하게 하도록 구성되고,

상기 제 1 소유자 식별자는, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유권을 승인받는 것 및 상기 가상 리소스 식별자가 상기 컴퓨팅 디바이스 리소스의 물리적 리소스 식별자에 맵핑되는 것을 나타내는, 비-일시적 프로세서 판독가능 저장 매체.

청구항 26

제 25 항에 있어서,

저장된 상기 프로세서 실행가능 명령들은 상기 프로세서로 하여금, 상기 컴퓨팅 디바이스 리소스의 소유권에서의 변경에 대해 가상화 인터페이스를 모니터링하는 동작이, 제 2 요청 엔터티에 의한 상기 컴퓨팅 디바이스 리소스의 소유권에 대한 요청에 대해 모니터링하는 동작을 포함하도록 하는 동작들을 수행하게 하도록 구성되는, 비-일시적 프로세서 판독가능 저장 매체.

청구항 27

제 22 항에 있어서,

저장된 상기 프로세서 실행가능 명령들은 상기 프로세서로 하여금,

상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정하는 동작이,

상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 가상 리소스 식별자를, 상기 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 저장된 소유자 식별자와 비교하는 동작; 및

상기 컴퓨팅 디바이스 리소스를 액세스하기 위한 상기 요청의 상기 가상 리소스 식별자 및 상기 컴퓨팅 디바이스 리소스의 상기 가상 리소스 식별자가 매칭될 때, 상기 제 1 요청 엔터티가 상기 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 동작

을 포함하도록 하는 동작들을 수행하게 하도록 구성되는, 비-일시적 프로세서 판독가능 저장 매체.

청구항 28

제 22 항에 있어서,

상기 컴퓨팅 디바이스 리소스의 상기 소유자는 애플리케이션이고; 그리고

상기 컴퓨팅 디바이스 리소스의 상기 비-소유자는 오퍼레이팅 시스템 커널, 하이퍼바이저, 및 트러스트존 중 하나를 포함하는 리소스 관리자인, 비-일시적 프로세서 판독가능 저장 매체.

발명의 설명

기 술 분 야

배 경 기 술

[0001] 하나 이상의 프로세서들 및 하나 이상의 주변장치들을 갖는 임의의 컴퓨터 시스템에서, 리소스 관리 소프트웨어는 높은 특권을 가지고 실행된다. 일 예로서 보호 링 모델을 이용하여, 오퍼레이팅 시스템은 모든 하드웨어에 대한 완전한 액세스로 링-0 에서 실행되고, 하이퍼바이저는 모든 하드웨어에 대한 완전한 액세스로 링-0 아래에서 실행된다. 리소스 관리자가 태스크에 리소스를 할당할 때, 예를 들어 오퍼레이팅 시스템이 프로세스에 메모리 페이지를 할당할 때, 리소스 관리자는 그 리소스에 대한 완전한 액세스를 유지한다. 리소스에 대해 완전한 액세스를 유지하는 것은 리소스 관리자로 하여금 태스크를 대신하여 리소스를 관리하는 것을 가능하게 한다. 리소스 관리자는 또한 리소스에 대한 판독/기입 액세스를 가질 수 있고, 이는 리소스로 하여금 리소스 관리를 구현하는 것을 가능하게 할 수도 있다. 예를 들어, 오퍼레이팅 시스템은 메모리 페이지를 재할당하거나 메모리 밖으로 프로세스를 스왑핑하기 위해 프로세스에 할당된 메모리 페이지를 판독한다.

[0002] 오퍼레이팅 시스템들, 하이퍼바이저들, 및 트러스트존들을 포함하는 리소스 관리자들은 소프트웨어의 취약한 부분들이다. 그것들의 선천적인 복잡성으로 인해, 모든 버그들의 제거는 불가능에 가깝다. 리소스 관리자에서의 취약성을 이용하는 공격은 컴퓨터 시스템의 고장을 초래할 수 있다. 리소스 관리자의 높은 특권 때문에, 공격자는 컴퓨터 시스템에 대한 완전한 액세스를 가질 수 있다. 따라서, 공격자들은 리소스 관리자들에서의 결점들을 발견하고 이용하도록 장려된다.

발명의 내용

[0003] 다양한 실시형태들의 방법들 및 장치들은 리소스 콘텐츠들 (resource contents) 의 가상 뷰들 (virtual views) 을 이용하여 데이터를 보호하는 장치 및 방법들을 제공한다. 다양한 실시형태들은, 제 1 요청 엔터티 (entity) 에 의한 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청을 모니터링하는 컴퓨팅 디바이스의 가상화 인터페이스 모니터 (virtualization interface monitor) 를 포함할 수도 있다. 가상화 인터페이스 모니터는, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유자 (owner) 인지 여부를 결정할 수도 있다. 제 1 요청 엔터티에 대한 컴퓨팅 디바이스의 데이터 보호 시스템은, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유자라고 결정하는 것에 응답하여, 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려지지 않은 (unobscured)

가상 뷰를 제공할 수도 있다. 데이터 보호 시스템은, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 비-소유자 (non-owner) 라고 결정하는 것에 응답하여, 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가려진 (obscured) 가상 뷰를 제 1 요청 엔터티에 제공할 수도 있다.

[0004] 일부 실시형태들에서, 리소스 콘텐츠 암호화 디바이스 (resource content cryptographic device) 는, 제 1 요청 엔터티가 인증된 기능 (certified function) 을 갖는지 여부를 결정하고, 제 1 요청 엔터티가 인증된 기능을 갖는다고 결정하는 것에 응답하여, 제 1 요청 엔터티에 대해 액세스 타입 (access type) 을 결정할 수도 있다. 리소스 콘텐츠 암호화 디바이스는, 그 액세스 타입에 기초한 가림 레벨 (obscuring level) 을 이용하여, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 비-소유자 라고 결정하는 것에 응답하여, 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가상 뷰를 가릴 수도 있다.

[0005] 일부 실시형태들에서, 액세스 타입은 부분적 가려짐 (partially obscured) 및 가려짐 (obscured) 을 포함할 수도 있다. 리소스 콘텐츠 암호화 디바이스는, 제 1 요청 엔터티에 대한 액세스 타입이 부분적 가려짐이라고 결정하는 것에 응답하여 호모모픽 암호화 (homomorphic encryption) 를 이용하여 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가상 뷰들을 암호화함으로써, 액세스 타입에 기초한 가림 레벨을 이용하여 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가상 뷰들을 가릴 수도 있다. 리소스 콘텐츠 암호화 디바이스는, 제 1 요청 엔터티에 대한 액세스 타입이 가려짐이라고 결정하는 것에 응답하여, 강력한 암호화 (encryption) 를 이용하여 컴퓨팅 디바이스 리소스의 리소스 콘텐츠들의 가상 뷰를 암호화할 수도 있다.

[0006] 일부 실시형태들에서, 가상화 인터페이스 모니터는, 컴퓨팅 디바이스 리소스의 소유권 (ownership) 에서의 변경들에 대해 가상화 인터페이스를 모니터링하고, 제 1 요청 엔터티에 대해 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 제 1 요청 엔터티의 제 1 소유자 식별자를 저장할 수도 있다. 이러한 실시형태들에서, 제 1 소유자 식별자는, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유권을 승인받는 것 및 가상 리소스 식별자가 컴퓨팅 디바이스 리소스의 물리적 리소스 식별자에 맵핑되는 것을 나타낼 수도 있다.

[0007] 일부 실시형태들에서, 컴퓨팅 디바이스 리소스의 소유권에서의 변경에 대해 가상화 인터페이스를 모니터링하는 것은, 제 2 요청 엔터티에 의한 컴퓨팅 디바이스 리소스의 소유권에 대한 요청에 대해 모니터링하는 것을 포함할 수도 있다.

[0008] 일부 실시형태들에서, 가상화 인터페이스 모니터는, 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청의 가상 리소스 식별자를, 컴퓨팅 디바이스 리소스의 가상 리소스 식별자와 상관된 저장된 소유자 식별자와 비교함으로써, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유자인지 여부를 결정할 수도 있다. 가상화 인터페이스 모니터는, 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청의 가상 리소스 식별자 및 컴퓨팅 디바이스 리소스의 가상 리소스 식별자가 매칭될 때, 제 1 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유자라고 결정할 수도 있다.

[0009] 일부 실시형태들에서, 컴퓨팅 디바이스 리소스의 소유자는 애플리케이션을 포함할 수도 있고, 컴퓨팅 디바이스 리소스의 비-소유자는 오퍼레이팅 시스템 커널 (operating system kernel), 하이퍼바이저 (hypervisor), 및 트러스트존 (TrustZone) 중 하나를 포함하는 리소스 관리자를 포함할 수도 있다.

[0010] 다양한 실시형태들은, 리소스 콘텐츠들의 가상 뷰들을 이용하여 데이터를 보호하도록 구성된 컴퓨팅 디바이스를 포함할 수도 있다. 컴퓨팅 디바이스는, 가상화 인터페이스 모니터 및 리소스 콘텐츠 암호화 디바이스를 포함하는 데이터 보호 시스템을 포함할 수도 있다. 컴퓨팅 디바이스의 하나 이상의 프로세서들은, 상기 요약된 실시형태 방법들의 하나 이상의 동작들을 수행하기 위해, 데이터 보호 시스템 실행가능 명령들, 가상화 인터페이스 모니터 실행가능 명령들, 및 리소스 콘텐츠 암호화 디바이스 실행가능 명령들로 구성될 수도 있다.

[0011] 다양한 실시형태들은, 상기 요약된 실시형태 방법들 중 하나 이상의 실시형태 방법들의 기능들을 수행하기 위한 수단을 갖는, 리소스 콘텐츠들의 가상 뷰들을 이용하여 데이터를 보호하도록 구성된 컴퓨팅 디바이스를 포함할 수도 있다.

[0012] 다양한 실시형태들은, 컴퓨팅 디바이스의 하나 이상의 프로세서들로 하여금, 상기 요약된 실시형태 방법들 중 하나 이상의 실시형태 방법들의 동작들을 수행하게 하도록 구성된 프로세서-실행가능 명령들을 그 위에 저장한 비-일시적 프로세서-판독가능 저장 매체를 포함할 수도 있다.

도면의 간단한 설명

[0013] 본 명세서에 통합되고 그 일부를 구성하는 첨부하는 도면들은, 다양한 실시형태들의 예시적인 실시형태들을 예시하고, 상기 주어진 일반적인 설명 및 아래에 주어지는 상세한 설명과 함께, 청구항들의 피처들을 설명하도록

기능한다.

도 1 은 일 실시형태를 구현하기에 적합한 컴퓨팅 디바이스를 예시하는 컴포넌트 블록도이다.

도 2 는 일 실시형태를 구현하기에 적합한 일 예의 멀티-코어 프로세서를 예시하는 컴포넌트 블록도이다.

도 3 은 일 실시형태를 구현하기에 적합한 데이터 보호 시스템을 예시하는 컴포넌트 블록도이다.

도 4 는 일 실시형태에 따른 리소스 소유권 테이블이다.

도 5 는 일 실시형태에 따른 액세스 요청 인증 테이블이다.

도 6 은 가상 리소스 뷰들을 이용하여 데이터를 보호하기 위한 일 실시형태 방법을 나타내는 프로세스 흐름도이다.

도 7 은 컴퓨팅 디바이스 리소스들의 소유권을 트래킹하기 위한 일 실시형태 방법을 예시하는 프로세스 흐름도이다.

도 8 은 리소스 콘텐츠의 가상 뷰들에 암호화를 적용하기 위해 인증서들을 이용하기 위한 일 실시형태 방법을 예시하는 프로세스 흐름도이다.

도 9 는 다양한 실시형태들과 함께 사용하기에 적합한 일 예시적인 모바일 컴퓨팅 디바이스를 예시하는 컴포넌트 블록도이다.

도 10 은 다양한 실시형태들과 함께 사용하기에 적합한 일 예시적인 모바일 컴퓨팅 디바이스를 예시하는 컴포넌트 블록도이다.

도 11 은 다양한 실시형태들과 함께 사용하기에 적합한 일 예시적인 서버를 예시하는 컴포넌트 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 다양한 실시형태들이 첨부하는 도면들을 참조하여 상세히 설명될 것이다. 가능하면 언제나, 동일한 참조 부호들이 동일하거나 또는 유사한 부분들을 지칭하기 위해 도면들 전반에 걸쳐 사용될 것이다. 예시를 목적으로 특정한 예들 및 구현들이 참조되며, 청구항들의 범위를 제한하도록 의도되지 않는다.

[0015] 용어들 "컴퓨팅 디바이스" 및 "모바일 컴퓨팅 디바이스" 는 셀룰러 전화기들, 스마트폰들, 개인 또는 모바일 멀티-미디어 플레이어들, 개인 휴대 정보 단말기들 (PDA들), 랩톱 컴퓨터들, 태블릿 컴퓨터들, 컨버터블 랩톱들/태블릿들 (2-인-1 컴퓨터들), 스마트북들, 울트라북들, 넷북들, 팜톱 컴퓨터들, 무선 전자 메일 수신기들, 멀티미디어 인터넷 가능 셀룰러 전화기들, 모바일 게이밍 콘솔들, 무선 게이밍 제어기들, 및 메모리, 및 멀티-코어 프로그래밍가능 프로세서를 포함하는 유사한 개인 전자 디바이스들 중 임의의 하나 또는 전부를 지칭하기 위해 본 명세서에서 상호교환가능하게 사용된다. 용어 "컴퓨팅 디바이스" 는 개인 컴퓨터들, 데스크톱 컴퓨터들, 올-인-원 컴퓨터들, 워크 스테이션들, 수퍼 컴퓨터들, 메인프레임 컴퓨터들, 임베디드 컴퓨터들, 서버들, 홈 씨어터 컴퓨터들, 및 게임 콘솔들을 포함하는 정지식 컴퓨팅 디바이스들을 추가로 지칭할 수도 있다. 다양한 실시형태들은 제한된 메모리 및 배터리 리소스들을 갖는 스마트폰들과 같은 모바일 컴퓨팅 디바이스들에 대해 특히 유용하다. 하지만, 본 실시형태들은 일반적으로는, 프로세서들의 전력 소비를 감소시키는 것이 모바일 컴퓨팅 디바이스의 배터리-동작 시간을 연장시킬 수 있는 제한된 전력 버짓 (limited power budget) 및 복수의 메모리 디바이스들을 구현하는 임의의 전자 디바이스에 있어서 유용하다.

[0016] 실시형태들은, 오퍼레이팅 시스템 커널을 포함하는 오퍼레이팅 시스템들, 하이퍼바이저들, 및/또는 트러스트존들과 같은 리소스 관리자들의 고-특권 액세스 허가들로부터 리소스 관리 태스크들을 분리하기 위한 방법들, 시스템들, 및 디바이스들을 포함할 수도 있다. 다양한 리소스들에 대한 액세스 요청들을 번역 (translate) 하기 위해 사용되는 가상화 인터페이스들의 모니터링은 리소스에 대한 소유자 애플리케이션 액세스들 및 리소스 관리자 액세스들을 구별하기 위해 사용될 수도 있다. 동일한 리소스의 상이한 뷰들은 소유자 애플리케이션 및 리소스 관리에게 제공될 수도 있다. 액세스 요청에 관련된 리소스 콘텐츠의 보호의 상이한 레벨들은 리소스의 액세서 (accessor) 및 리소스 데이터의 민감도 (sensitivity) 에 의해 계획된 동작에 기초하여 제공될 수도 있다.

[0017] 리소스들은, 애플리케이션들이 다양한 프로세스들을 구현하기 위해 리소스 콘텐츠에 대해 액세스할 필요가 있는 동안, 리소스 데이터와 같은 그것들의 콘텐츠에 대한 액세스를 가짐이 없이 리소스 관리자에 의해 관리 (예컨대, 이동, 카피 등) 될 수 있다. 가상화 인터페이스들은, 리소스 관리자로 하여금 관리 기능을 구현하

도록 허용하면서, 그리고 리소스 소유 애플리케이션이 프로세스들을 구현하기 위해 리소스 콘텐츠를 액세스하도록 허용하면서, 리소스 관리자로부터 리소스 콘텐츠를 마스킹할지 여부를 결정하기 위해 모니터링될 수도 있다.

가상화 인터페이스 모니터들 및 리소스 콘텐츠 암호화 디바이스들은 리소스에 대한 소유자 애플리케이션 액세스들 및 리소스 관리자 액세스들을 구별하도록 그리고 리소스 관리자에 의한 리소스 콘텐츠의 액세스를 제한하도록 구성된 하드웨어로 구현될 수도 있다.

[0018] 가상화 인터페이스 모니터는 컴퓨팅 디바이스 시스템의 리소스들의 소유권을 저장 및 업데이트하도록 구성된 리소스 소유권 트래커 (tracker) 를 포함할 수도 있다. 가상화 인터페이스 모니터는, 리소스에 대한 액세스 요청이 컴퓨팅 디바이스 시스템의 리소스 관리자 또는 리소스의 소유자 애플리케이션에 의해 발행되는지 여부를 결정하도록 구성될 수도 있다. 리소스 콘텐츠 암호화 디바이스는, 액세스 요청이 리소스 관리자에 의해 발행된 것이라는 결정에 응답하여, 리소스의 콘텐츠를 암호화할 수도 있다. 리소스 콘텐츠 암호화 디바이스는, 액세스 요청이 소유자 애플리케이션에 의해 발행된 것이라는 결정에 응답하여, 암호화되지 않은 형태로 리소스의 콘텐츠를 제공할 수도 있다.

[0019] 리소스 관리자는 애플리케이션에 리소스를 할당할 수도 있다. 애플리케이션은 리소스의 소유권을 요청할 수도 있고, 가상화 인터페이스 모니터는 리소스의 소유자를 업데이트할 수도 있다.

[0020] 리소스의 소유자 애플리케이션 및 리소스 관리자는 리소스의 상이한 가상적 표현들을 제공받을 수도 있다. 리소스의 각각의 가상적 표현들은 리소스의 물리적 메모리 어드레스들에 대한 가상적 메모리 어드레스들의 상이한 맵핑들을 포함할 수도 있다.

[0021] 가상화 인터페이스 모니터는 소유된 리소스를 액세스하기 위한 요청을 수신, 검출, 또는 차단할 수도 있다. 가상화 인터페이스 모니터는, 액세스 요청의 가상 메모리 어드레스에 의해 요청 엔터티가 리소스 관리자인지 또는 리소스 소유자인지 여부를 식별할 수도 있다. 요청 엔터티가 리소스 소유자 애플리케이션이라고 결정하는 것에 응답하여, 리소스 콘텐츠 암호화 디바이스는 리소스 콘텐츠의 암호화되지 않은 가상 표현에 대해 소유자 애플리케이션 액세스를 제공할 수도 있다. 요청 엔터티가 리소스 관리자라고 결정하는 것에 응답하여, 리소스 콘텐츠 암호화 디바이스는 리소스의 콘텐츠의 가상적 표현을 암호화하고, 암호화된 가상적 표현에 대해 리소스 관리자 액세스를 제공할 수도 있다.

[0022] 일부 구현들에서, 리소스 콘텐츠 암호화 디바이스는 리소스 콘텐츠의 민감도 및 요청 엔터티에 의해 계획된 동작에 기초하여 리소스 콘텐츠의 보호를 변화시킬 수도 있다. 리소스 콘텐츠 암호화 디바이스는 강력한 암호화 및 서명 요건들, 또는 부분적 호모모픽 암호화와 같은, 상이한 타입들의 암호화를 지원할 수도 있다.

[0023] 인증 디바이스는, 컴파일러가 어떤 동작들이 특정 소프트웨어 컴포넌트에 의해 수행되는 것을 보장하는 것을 진술하는, 애플리케이션들 및 리소스 관리자들에 대한 컴파일러 인증서들을 저장 및 업데이트할 수도 있다. 컴파일러 인증서들은 지정된 타입의 암호화와 상관될 수도 있다. 리소스 콘텐츠 암호화 디바이스는, 다양한 리소스 소유자 애플리케이션들, 비-소유자 애플리케이션들, 및 리소스 관리자들에 대해 인증 디바이스에 의해 유지되는 상관들 및 요청 엔터티의 결정에 기초하여 상이한 타입들의 암호화를 실시할 수도 있다.

[0024] 도 1 은 다양한 실시형태들에의 이용에 적합한 원격 컴퓨팅 디바이스 (50) 와 통신하고 있는 컴퓨팅 디바이스 (10) 를 포함하는 시스템을 예시한다. 컴퓨팅 디바이스 (10) 는 프로세서 (14), 메모리 (16), 통신 인터페이스 (18), 및 저장 메모리 인터페이스 (20) 를 가진 시스템-온-칩 (SoC) (12) 을 포함할 수도 있다. 컴퓨팅 디바이스 (10) 는 통신 컴포넌트 (22), 이를 테면 유선 또는 무선 모뎀, 저장 메모리 (24), 무선 네트워크 (30) 에 대한 무선 접속 (32) 을 확립하기 위한 안테나 (26), 및/또는 인터넷 (40) 에 대한 유선 접속 (44) 에 접속하기 위한 네트워크 인터페이스 (28) 를 더 포함할 수도 있다. 프로세서 (14) 는 다양한 하드웨어 코어들, 예를 들어, 다수의 프로세서 코어들 중 임의의 것을 포함할 수도 있다.

[0025] 용어 "시스템-온-칩" (SoC) 은 하드웨어 코어, 메모리, 및 통신 인터페이스를 통상적으로 포함하지만, 배타적으로 포함하지는 않는 상호접속된 전자 회로들의 세트를 지칭하기 위해 본 명세서에서 사용된다. 하드웨어 코어는 다양한 상이한 타입들의 프로세서들, 이를 테면 범용 프로세서, 중앙 프로세싱 유닛 (CPU), 디지털 신호 프로세서 (DSP), 그래픽스 프로세싱 유닛 (GPU), APU (accelerated processing unit), 보조 프로세서, 단일-코어 프로세서, 및 멀티-코어 프로세서를 포함할 수도 있다. 하드웨어 코어는 다른 하드웨어 및 하드웨어 조합들, 이를 테면 필드 프로그래밍가능 게이트 어레이 (FPGA), 주문형 집적 회로 (ASIC), 다른 프로그래밍가능 로직 디바이스, 이산 게이트 로직, 트랜지스터 로직, 성능 모니터링 하드웨어, 와치독 하드웨어, 및 타임 레퍼런스들을 더 구현할 수도 있다. 집적 회로들은 집적 회로의 컴포넌트들이 실리콘과 같은, 반도체 재료의 단

일 피스 상에 상주하도록 구성될 수도 있다. SoC (12) 는 하나 이상의 프로세서들 (14) 을 포함할 수도 있다. 컴퓨팅 디바이스 (10) 는 1 초과의 SoC들 (12) 을 포함할 수도 있고, 이로써 프로세서들 (14) 및 프로세서 코어들의 수를 증가시킬 수도 있다. 컴퓨팅 디바이스 (10) 는 또한, SoC (12) 와 연관되지 않은 프로세서들 (14) 을 포함할 수도 있다. 개개의 프로세서들 (14) 은 도 2 를 참조하여 아래에 설명한 바와 같은 멀티-코어 프로세서들일 수도 있다. 프로세서들 (14) 은 컴퓨팅 디바이스 (10) 의 다른 프로세서들 (14) 과 동일하거나 또는 상이할 수도 있는 특정 목적들을 위해 각각 구성될 수도 있다. 동일한 또는 상이한 구성들의 프로세서들 (14) 및 프로세서 코어들 중 하나 이상은 함께 그룹화될 수도 있다. 프로세서들 (14) 또는 프로세서 코어들의 그룹은 멀티-프로세서 클러스터로 지칭될 수도 있다.

[0026] SoC (12) 의 메모리 (16) 는 프로세서 (14) 에 의한 액세스를 위해 데이터 및 프로세서 실행가능 코드를 저장하기 위해 구성된 휘발성 또는 비휘발성 메모리일 수도 있다. 컴퓨팅 디바이스 (10) 및/또는 SoC (12) 는 다양한 목적들을 위해 구성된 하나 이상의 메모리들 (16) 을 포함할 수도 있다. 실시형태에서, 하나 이상의 메모리들 (16) 은 휘발성 메모리들, 이를 테면 랜덤 액세스 메모리 (RAM) 또는 메인 메모리, 또는 캐시 메모리를 포함할 수도 있다. 이들 메모리들 (16) 은 데이터 센서 또는 서브시스템으로부터 수신된 제한된 양의 데이터를 일시적으로 보유하도록 구성될 수도 있다. 이들 메모리들 (16) 은 다양한 팩터들에 기초하여 미래의 액세스를 예상하고 비휘발성 메모리로부터 메모리들 (16) 로 로드된, 비휘발성 메모리로부터 요청되는 데이터 및/또는 프로세서 실행가능 코드 명령들을 일시적으로 보유하도록 구성될 수도 있다. 이들 메모리들 (16) 은 프로세서 (14) 에 의해 생성되고 비휘발성 메모리에 저장되지 않고 미래의 빠른 액세스를 위해 일시적으로 저장된 중간의 프로세싱 데이터 및/또는 프로세서 실행가능 코드 명령들을 일시적으로 보유하도록 구성될 수도 있다.

[0027] 메모리 (16) 는 프로세서들 (14) 중 하나 이상의 프로세서들에 의한 액세스를 위해, 다른 메모리 디바이스, 이를 테면 다른 메모리 (16) 또는 저장 메모리 (24) 로부터 메모리 (16) 로 로드되는, 데이터 및 프로세서 실행가능 코드를 적어도 일시적으로 저장하도록 구성될 수도 있다. 메모리 (16) 로 로드된 데이터 또는 프로세서 실행가능 코드는 프로세서 (14) 에 의한 기능의 실행에 응답하여 로드될 수도 있다. 기능의 실행에 응답하여 메모리 (16) 로 데이터 또는 프로세서 실행가능 코드를 로드하는 것은, 요청된 데이터 또는 프로세서 실행가능 코드가 메모리 (16) 에 로케이트되지 않기 때문에, 성공적이지 않거나, 또는 미스 (miss) 인, 메모리 (16) 로의 메모리 액세스 요청으로부터 발생할 수도 있다. 미스에 응답하여, 다른 메모리 (16) 또는 저장 메모리 (24) 로의 메모리 액세스 요청은 요청된 데이터 또는 프로세서 실행가능 코드를 다른 메모리 (16) 또는 저장 메모리 (24) 로부터 메모리 (16) 로 로드시킬 수도 있다. 기능의 실행에 응답하여 메모리 (16) 로 데이터 또는 프로세서 실행가능 코드를 로드하는 것은 다른 메모리 (16) 또는 저장 메모리 (24) 로의 메모리 액세스 요청으로부터 발생할 수도 있고, 데이터 또는 프로세서 실행가능 코드는 추후의 액세스를 위해 메모리 (16) 로 로드될 수도 있다.

[0028] 통신 인터페이스 (18), 통신 컴포넌트 (22), 안테나 (26), 및/또는 네트워크 인터페이스 (28) 는 컴퓨팅 디바이스 (10) 가 무선 접속 (32) 을 경유하여 무선 네트워크 (30) 를 통해, 및/또는 유선 네트워크 (44) 를 통해 원격 컴퓨팅 디바이스 (50) 와 통신하는 것을 가능하게 하기 위해 협심하여 작동할 수도 있다. 무선 네트워크 (30) 는 원격 컴퓨팅 디바이스 (50) 와 데이터를 교환할 수도 있는 인터넷 (40) 에의 접속을 컴퓨팅 디바이스 (10) 에 제공하기 위해, 예를 들어, 무선 통신을 위해 이용되는 무선 주파수 스펙트럼을 포함하는, 다양한 무선 통신 기술들을 이용하여 구현될 수도 있다.

[0029] 저장 메모리 인터페이스 (20) 및 저장 메모리 (24) 는 컴퓨팅 디바이스 (10) 가 비휘발성 저장 매체 상에 데이터 및 프로세서 실행가능 코드를 저장하는 것을 허용하기 위해 협심하여 작동할 수도 있다. 저장 메모리 (24) 는 저장 메모리 (24) 가 프로세서들 (14) 중 하나 이상의 프로세서에 의한 액세스를 위해 데이터 또는 프로세서 실행가능 코드를 저장할 수도 있는 메모리 (16) 의 실시형태와 매우 유사하게 구성될 수도 있다. 비휘발성인 저장 메모리 (24) 는 컴퓨팅 디바이스 (10) 의 전력이 셧 오프된 후라도 정보를 유지할 수도 있다. 전력이 다시 턴 온되고 컴퓨팅 디바이스 (10) 가 리부팅되는 경우, 저장 메모리 (24) 상에 저장된 정보는 컴퓨팅 디바이스 (10) 에 이용가능할 수도 있다. 저장 메모리 인터페이스 (20) 는 저장 메모리 (24) 에 대한 액세스를 제어하고 프로세서 (14) 가 저장 메모리 (24) 로부터 데이터를 판독하고 저장 메모리 (24) 에 데이터를 기록하는 것을 허용할 수도 있다.

[0030] 컴퓨팅 디바이스 (10) 의 컴포넌트들의 일부 또는 전부는 필요한 기능들을 여전히 서빙하면서 상이하게 배열 및/또는 결합될 수도 있다. 더욱이, 컴퓨팅 디바이스 (10) 는 컴포넌트들의 각각의 하나에 제한되지 않을 수

도 있고, 각각의 컴포넌트의 다수의 인스턴스들이 컴퓨팅 디바이스 (10) 의 다양한 구성들에 포함될 수도 있다.

[0031] 도 2 는 실시형태를 구현하기에 적합한 멀티-코어 프로세서 (14) 를 예시한다. 멀티-코어 프로세서 (14) 는 복수의 동종 또는 이종의 프로세서 코어들 (200, 201, 202, 203) 을 가질 수도 있다. 프로세서 코어들 (200, 201, 202, 203) 은, 단일 프로세서 (14) 의 프로세서 코어들 (200, 201, 202, 203) 이 동일한 목적을 위해 구성되고 동일하거나 또는 유사한 성능 특성들을 가질 수도 있다는 점에서 동종일 수도 있다. 예를 들어, 프로세서 (14) 는 범용 프로세서일 수도 있고, 프로세서 코어들 (200, 201, 202, 203) 은 동종의 범용 프로세서 코어들일 수도 있다. 대안적으로, 프로세서 (14) 는 그래픽스 프로세싱 유닛 또는 디지털 신호 프로세서일 수도 있고, 프로세서 코어들 (200, 201, 202, 203) 은 각각 동종의 그래픽스 프로세서 코어들 또는 디지털 신호 프로세서 코어들일 수도 있다. 참조의 용이함을 위해, 용어들 "프로세서" 및 "프로세서 코어" 는 본 명세서에서 상호교환가능하게 사용될 수도 있다.

[0032] 프로세서 코어들 (200, 201, 202, 203) 은, 단일 프로세서 (14) 의 프로세서 코어들 (200, 201, 202, 203) 이 상이한 목적들을 위해 구성되고 및/또는 상이한 성능 특성들을 가질 수도 있다는 점에서 이종일 수도 있다. 이러한 이종의 프로세서 코어들의 이종성 (heterogeneity) 은 상이한 명령 세트 아키텍처, 파이프라인들, 동작 주파수들 등을 포함할 수도 있다. 이러한 이종의 프로세서 코어들의 일 예는, 더 느린, 저전력 프로세서 코어들이 보다 강력하고 전력 소모적인 프로세서 코어들과 커플링될 수도 있는 "big.LITTLE" 아키텍처들로 알려져 있는 것을 포함할 수도 있다. 유사한 실시형태들에서, SoC (12) 는 다수의 동종 또는 이종의 프로세서들 (14) 을 포함할 수도 있다.

[0033] 도 2 에 예시된 예에서, 멀티-코어 프로세서 (14) 는 4 개의 프로세서 코어들 (200, 201, 202, 203) (즉, 프로세서 코어 0, 프로세서 코어 1, 프로세서 코어 2, 및 프로세서 코어 3) 을 포함한다. 설명의 용이함을 위해, 본 명세서의 예들은 도 2 에 예시된 4 개의 프로세서 코어들 (200, 201, 202, 203) 을 참조할 수도 있다. 그러나, 도 2 에 예시되고 본 명세서에서 설명된 4 개의 프로세서 코어들 (200, 201, 202, 203) 은 단지 일 예로서 제공될 뿐이며, 결코 다양한 실시형태들을 4-코어 프로세서 시스템으로 제한하려는 의도는 없다. 컴퓨팅 디바이스 (10), SoC (12), 또는 멀티-코어 프로세서 (14) 는 본 명세서에서 예시 및 설명된 4 개의 프로세서 코어들 (200, 201, 202, 203) 보다 더 적거나 또는 더 많은 프로세서 코어들을 개별로 또는 조합하여 포함할 수도 있다.

[0034] 도 3 은 일 실시형태에 따른 데이터 보호 시스템을 예시한다. 데이터 보호 시스템 (300) 은, 컴퓨팅 디바이스 리소스에 대해 가상화 인터페이스를 모니터링하고, 리소스 콘텐츠들의 일부를 암호화하고 리소스의 사용 또는 리소스에 대한 액세스를 요청하는 컴퓨팅 디바이스 (10) 의 상이한 컴포넌트들 ("요청 컴포넌트들") 에 대해 리소스 콘텐츠의 상이한 암호화된 및 암호화되지 않은 가상 뷰들을 제공함으로써 리소스 콘텐츠를 보호하도록 구성될 수도 있다. 데이터 보호 시스템 (300) 은 가상화 인터페이스 모니터 (302) 및 리소스 콘텐츠 암호화 디바이스 (304) 를 포함할 수도 있다.

[0035] 가상화 인터페이스 모니터 (302) 는, 메모리 (16) 의 어드레스 로케이션, 저장 메모리 (24) 의 디스크 블록들, 및 통신 컴포넌트 (22) 의 네트워크 카드 큐 식별자들과 같은 컴퓨팅 디바이스 리소스들의 소유권을 트래킹하도록 구성될 수도 있다. 리소스들의 소유권은 컴퓨팅 디바이스 (10) 상에서 실행되는 애플리케이션 (312), 오퍼레이팅 시스템 (306), 하이퍼바이저 (308), 및/또는 트러스트존 (310) 에 기인할 수도 있다.

[0036] 컴퓨팅 디바이스 리소스의 소유권의 속성은 다수의 데이터를 링크 및/또는 배열하도록 구성된 데이터 구조 또는 테이블에서 가상화 인터페이스 모니터 (302) 에 의해 저장될 수도 있다. 본 개시를 제한함이 없이, 설명의 용이함을 위해, 본원에서의 언급은 가상화 인터페이스 모니터 (302) 에 의해 저장된 그리고 도 4 를 참조하여 본원에서 추가로 설명되는 소유권 테이블 (미도시) 에 대해 이루어진다. 소유권 테이블은 오퍼레이팅 시스템 (306), 하이퍼바이저 (308), 트러스트존 (310), 및/또는 애플리케이션 (312) 중 하나를 표시하도록 구성된 소유자 식별자들 (ID) 을, 소유된 컴퓨팅 디바이스 리소스의, 가상 어드레스와 같은, 가상 리소스 식별자와 상관시킬 수도 있다.

[0037] 컴퓨팅 디바이스 리소스들에 대한, 가상-어드레스-대-물리적-어드레스 맵핑들과 같은, 상이한 가상 리소스 식별자 대 물리적 리소스 식별자 맵핑들은 잠재적 및 실제적 소유자들에 대해 사용될 수도 있다, 예컨대, 상이한 잠재적 소유자들은 동일한 물리적 어드레스에 맵핑된 상이한 가상 어드레스들을 사용할 수도 있다. 상이한 가상 리소스 식별자 대 물리적 리소스 식별자 맵핑들 때문에, 가상화 인터페이스 모니터 (302) 는 소유자를 소유된 컴퓨팅 디바이스 리소스와 상관시키기 위해 컴퓨팅 디바이스 리소스의 소유권에 대한 요청 또는 선언의 가상 리소스 식별자를 사용할 수도 있다.

[0038] 가상화 인터페이스 모니터 (302) 는, 컴퓨팅 디바이스 리소스의 소유권을 할당받은 엔터티 및 할당 메모리 리소스 관리자들에 의해 컴퓨팅 디바이스 리소스들의 소유권에 대한 요청들 또는 소유권의 선언들을 수신, 검출, 또는 차단할 수도 있다. 할당 메모리 리소스 관리자들은 오퍼레이팅 시스템 (306), 하이퍼바이저 (308), 및/또는 트러스트존 (310) 을 포함할 수도 있다. 컴퓨팅 디바이스 리소스의 소유권을 할당받은 엔터티는 오퍼레이팅 시스템 (306), 하이퍼바이저 (308), 트러스트존 (310), 및/또는 애플리케이션 (312) 을 포함할 수도 있다. 일부 실시형태들에서, 가상화 인터페이스 모니터 (302) 는, 컴퓨팅 디바이스 리소스의 소유권을 나타내는 엔터티들이 컴퓨팅 디바이스 리소스의 소유권에서의 변경 시에 유효하지 않은 것으로서 표시되거나 삭제될 수도 있도록 소유권 테이블을 관리할 수도 있다. 컴퓨팅 디바이스 리소스의 새로운 소유자에 대해 엔트리들이 추가되거나 유효한 것으로 마킹될 수도 있다.

[0039] 일부 실시형태들에서, 가상화 인터페이스 모니터 (302) 는 리소스 액세스 요청자의 허용된 기능들을 나타내는 인증을 트래킹할 수도 있다. 기능들의 인증은 컴퓨팅 디바이스 (10) 상에서 실행되는 컴파일러에 의해 식별되거나 기능들의 개발자들에 의해 프로그래밍될 수도 있다. 인증들은 애플리케이션 (312), 오퍼레이팅 시스템 (306), 하이퍼바이저 (308), 및/또는 트러스트존 (310) 의 기능들에 대해 적용가능할 수도 있다. 일부 실시형태들에서, 인증된 기능들을 구현할 필요가 있는 리소스 콘텐츠에 대한 액세스의 타입들은 인증서들과 상관될 수도 있다.

[0040] 기능들을 구현하기 위해 필요한 액세스들의 타입들은, 기능들이 리소스 콘텐츠에 대해 완전한, 가려지지 않은 액세스를 필요로하는지, 리소스 콘텐츠에 대해 부분적으로 가려진 액세스를 필요로하는지, 또는 리소스 콘텐츠에 대해 가려진 액세스를 필요로 하는지 여부를 나타낼 수도 있다. 리소스 콘텐츠에 대한 가려지지 않은 액세스는 리소스 콘텐츠를 가리지 위한 임의의 변경들 또는 조작들 없이 저장된 대로의 리소스 콘텐츠의 뷰를 허용할 수도 있고, 리소스 콘텐츠를 판독 및 기입하는 것을 허용할 수도 있다. 리소스 콘텐츠에 대한 부분적으로 가려진 액세스는 리소스 콘텐츠의 검색 및 산술적 조작을 허용할 수도 있고, 부분적 또는 전체적 호모모픽 암호화의 적용을 통해 달성될 수도 있다. 리소스 콘텐츠에 대한 가려진 액세스는 리소스 콘텐츠에 대한 판독 또는 기입 액세스 없이 실행될 수도 있는 리소스 관리 동작들을 허용할 수도 있고, 강력한 암호화 및 서명 요건들의 적용을 통해 달성될 수도 있다.

[0041] 가상화 인터페이스 모니터 (302) 는 다수의 데이터를 링크 및/또는 배열하도록 구성된 테이블 또는 데이터 구조에서 컴퓨팅 디바이스 리소스에 대한 액세스를 위한 요청자에 대한 기능 인증의 속성을 저장할 수도 있다. 일부 실시형태들에서, 가상화 인터페이스 모니터 (302) 는 또한, 인증된 기능을 구현하기 위해 필요한 액세스의 타입을 저장할 수도 있다. 본 개시를 제한함이 없이, 설명의 용이성을 위해, 본원에서의 언급은 가상화 인터페이스 모니터 (302) 에 의해 저장되고 도 5 를 참조하여 본원에서 설명된 인증 테이블 (미도시) 에 대해 이루어진다.

[0042] 가상화 인터페이스 모니터 (302) 는 액세스 요청자들에 의한 컴퓨팅 디바이스 리소스들에 대한 액세스를 위한 요청들을 수신, 검출, 또는 차단할 수도 있다. 본원에서 기술된 컴퓨팅 디바이스 리소스들의 소유권을 트래킹 (tracking) 하는 것과 유사한 방식으로, 가상화 인터페이스 모니터 (302) 는, 요청 엔터티가 소유자인지 여부를 결정하기 위해 컴퓨팅 디바이스 리소스에 액세스하기 위한 요청들의 가상 리소스 식별자를 사용할 수도 있다. 가상화 인터페이스 모니터 (302) 는 컴퓨팅 디바이스 리소스에 액세스하기 위한 요청의 가상 리소스 식별자와 상관된 요청 엔터티를 발견할 수도 있다. 일부 실시형태들에서, 가상화 인터페이스 모니터 (302) 는, 요청의 가상 리소스 식별자 및 요청 엔터티 식별자를 소유권 식별자에 대해 비교함으로써, 요청 엔터티가 소유자인지 여부를 결정하기 위해 소유권 테이블을 사용할 수도 있다. 일부 실시형태들에서, 가상화 인터페이스 모니터 (302) 는, 인증 테이블에서 요청 엔터티에 대한 기능 인증들을 로케이팅하기 위해 컴퓨팅 디바이스 리소스에 대한 액세스를 위한 요청의 요청 엔터티 식별자 및/또는 요청된 액세스 또는 기능을 사용할 수도 있다. 가상화 인터페이스 모니터 (302) 는, 컴퓨팅 디바이스 리소스에 대한 액세스를 위한 요청에 대한 기능 인증 및/또는 요청 엔터티 식별자와 상관된 액세스의 타입을 식별할 수도 있다. 이들 실시형태들 중 임의의 것에서, 가상화 인터페이스 모니터 (302) 는 소유권 테이블 및/또는 인증 테이블에서 저장된 컴퓨팅 디바이스 리소스에 대한 액세스를 위한 요청에 관련된 임의의 데이터를 리소스 콘텐츠 암호화 디바이스 (304) 에 송신할 수도 있다.

[0043] 리소스 콘텐츠 암호화 디바이스 (304) 는, 리소스 콘텐츠의 가상 뷰에 적용할 모호성 (obscureness) 의 타입 및/또는 레벨을 결정하고, 컴퓨팅 디바이스 리소스에 대한 액세스를 위한 요청에 응답하여 리소스 콘텐츠의 가상 뷰를 제공하도록 구성될 수도 있다. 모호성의 타입 및/또는 레벨은 암호화의 다양한 타입들 및 레벨들을 포함할 수도 있다. 컴퓨팅 디바이스 리소스들의 가상 뷰에 적용되는 암호화는 요청 엔터티로부터 리소스 콘텐

츠를 완전히 가리기 위한 강력한 암호화 및 서명 요건들을 포함할 수도 있다. 컴퓨팅 디바이스 리소스들의 가상 뷰에 적용되는 암호화는, 요청 엔터티로부터 리소스 콘텐츠를 가리고, 하지만 요청 엔터티로 하여금 호모모픽 암호화로부터 초래되는 암호문을 검색하거나 산술적으로 조작하도록 허용하기 위한, 부분적 또는 완전한 호모모픽 암호화를 포함할 수도 있다. 암호문 상의 동작들은 요청 엔터티가 해독된 리소스 콘텐츠를 판독하도록 허용함이 없이 해독된 리소스 콘텐츠에서의 대응하는 결과들을 생성할 수도 있다. 컴퓨팅 디바이스 리소스들의 가상 뷰에 적용되는 암호화는 소유자로 하여금 리소스 콘텐츠의 가상 카피 (copy) 를 액세스하도록 허용하기 위해 소요자에 의해 해독될 수도 있는 암호화를 포함할 수도 있다. 일부 실시형태들에서, 소유자로 하여금 리소스 콘텐츠의 가상 카피를 액세스하도록 허용하기 위해 컴퓨팅 디바이스 리소스의 가상 뷰에 대해 비암호화가 적용될 수도 있다.

[0044] 리소스 콘텐츠의 가상 뷰에 적용할 암호화의 타입 및/또는 레벨을 결정하기 위해, 리소스 콘텐츠 암호화 디바이스 (304) 는 가상화 인터페이스 모니터 (302) 로부터 수신된 데이터를 암호화의 타입 및/또는 레벨과 상관시킬 수도 있다. 가상화 인터페이스 모니터 (302) 로부터 수신된 데이터는, 예를 들어, 소유자 식별자, 요청 엔터티 식별자, 요청 엔터티가 컴퓨팅 디바이스 리소스의 소유자인지 여부, 기능 인증, 액세스의 타입, 및/또는, 컴퓨팅 디바이스 리소스에 대한 액세스를 위한 요청의 가상 어드레스와 같은 가상 리소스 식별자, 또는 대응하는 물리적 어드레스를 포함할 수도 있다.

[0045] 리소스 콘텐츠 암호화 디바이스 (304) 는 가상화 인터페이스 모니터 (302) 로부터 데이터를 수신하고, 가상화 인터페이스 모니터 (302) 로부터의 데이터와 상관된 암호화의 타입 및/또는 레벨을 식별할 수도 있다. 일부 실시형태들에서, 암호화의 타입 및/또는 레벨은 액세스 데이터의 타입의 일부로서 가상화 인터페이스 모니터 (302) 에 의해 제공될 수도 있다. 일부 실시형태들에서, 리소스 콘텐츠 암호화 디바이스 (304) 는 가상화 인터페이스 모니터 (302) 로부터 수신된 데이터와 암호화의 타입 및/또는 레벨 사이의 프로그래밍된 상관들을 이용하여 암호화의 타입 및/또는 레벨을 결정할 수도 있다. 예를 들어, 요청 엔터티가 소유자라는 것을 표시하는 데이터는 가벼운 또는 무 암호화와 상관될 수도 있는 한편, 요청 엔터티가 소유자가 아니라는 것을 표시하는 데이터는 강력한 암호화와 상관될 수도 있다. 유사하게, 요청된 기능이 비-소유자의 인증된 기능이라는 것을 표시하는 데이터는 전체적 또는 부분적 호모모픽 암호화와 상관될 수도 있고, 요청된 기능이 비-소유자의 비-인증된 기능이라는 것을 표시하는 데이터는 강력한 암호화와 상관될 수도 있다.

[0046] 데이터 보호 시스템 (300) 은 컴퓨팅 디바이스 리소스로부터 요청된 리소스 콘텐츠를 취출 (retrieve) 할 수도 있고, 리소스 콘텐츠 암호화 디바이스 (304) 는 수신된 리소스 콘텐츠의 가상 뷰에 대해 암호화의 타입 및/또는 레벨을 적용할 수도 있다. 데이터 보호 시스템 (300) 은 요청된 리소스 콘텐츠의 가려진 또는 가려지지 않은 가상 뷰를 요청 엔터티에 리턴할 수도 있다.

[0047] 일부 실시형태들에서, 데이터 보호 시스템 (300) 은 컴퓨팅 디바이스 리소스로부터 요청된 리소스 콘텐츠를 취출할 수도 있고, 가상화 인터페이스 모니터 (302) 는 컴퓨팅 디바이스 리소스에 대한 액세스를 위한 요청에 대해 액세스의 타입에 기초하여 신호를 송신할 수도 있다. 상이한 신호들은 리소스 콘텐츠 암호화 디바이스 (304) 로 하여금 취출된 리소스 콘텐츠의 가상 뷰에 대해 모호성의 타입 및/또는 레벨을 적용하도록 트리거 (trigger) 할 수도 있다. 데이터 보호 시스템 (300) 은 요청된 리소스 콘텐츠의 암호화된 또는 암호화되지 않은 가상 뷰를 요청 엔터티에 리턴할 수도 있다.

[0048] 데이터 보호 시스템 (300) 은 도 3 에서 예시된 바와 같은 하드웨어에서 구현될 수도 있다. 컴퓨팅 디바이스 (10) 는 오퍼레이팅 시스템 (306), 하이퍼바이저 (308), 트러스트존 (310), 및/또는 애플리케이션 (312) 을 포함하는, 소프트웨어를 실행할 수도 있다. 컴퓨팅 디바이스 (10) 는, 페이지 테이블들을 저장하는 랜덤 액세스 메모리 (RAM) 를 포함할 수도 있는 메모리 (16), 변환 색인 버퍼 (translation lookaside buffer) (314), CPU 를 포함할 수도 있는 프로세서 (14), 및 데이터 보호 시스템 (300) 과 같은 하드웨어 컴포넌트들을 포함할 수도 있다. 데이터 보호 시스템 (300) 은, 데이터 보호 시스템 (300) 을 구현하도록 구성된 SoC (12) 또는 프로세서 (14) 와 같은 전용 하드웨어 또는 범용 하드웨어를 포함할 수도 있다. 가상화 인터페이스 모니터 (302) 는 프로세서 (14) 또는 프로세서 코어 (200, 201, 202, 203), 및 버퍼를 포함할 수도 있는 메모리 (16) 와 같은 전용 하드웨어 또는 범용 하드웨어를 포함할 수도 있다. 리소스 콘텐츠 암호화 디바이스 (304) 는 프로세서 (14), 프로세서 코어 (200, 201, 202, 203), 및 암호화 엔진 또는 하드웨어 가속기, 및 버퍼를 포함할 수도 있는 메모리 (16) 와 같은 전용 하드웨어 또는 범용 하드웨어를 포함할 수도 있다.

[0049] 도 4 는 데이터 보호 시스템 (300) 이 컴퓨팅 디바이스 리소스의 소유권의 데이터를 저장하기 위해 사용할 수도 있는 소유권 테이블 (400) 의 비-제한적 예를 나타낸다. 다양한 구현들은, 소유자 식별자들, 가상 어드레스

들과 같은 가상 리소스 식별자들, 물리적 어드레스들과 같은 물리적 리소스 식별자들, 및 유효성 표시자들을 포함하는 소유권 데이터의 상이한 조합들 및 정렬을 포함할 수도 있다. 일부 구현들에서, 가상 리소스 식별자들 및 물리적 리소스 식별자들은 상호교환가능하게 사용될 수도 있다.

[0050] 예시적인 소유권 테이블 (400) 은 소유자 식별자들 열 (402) 및 가상 리소스 식별자들 열 (404) 을 포함할 수도 있다. 이하에서 추가로 논의되는 바와 같이, 소유권 테이블 (400) 은 또한 선택적 유효성 표시자들 칼럼 (406) 을 포함할 수도 있다. 소유권 테이블 (400) 은 다수의 행들, 예를 들어, 컴퓨팅 디바이스 리소스의 상이한 소유권을 각각 나타내는 행들 (408-414) 을 포함할 수도 있다.

[0051] 소유자 식별자들 열 (402) 은 컴퓨팅 디바이스의 각각의 소유자 또는 잠재적 소유자에 대한 고유한 식별자들을 포함할 수도 있다. 소유자 식별자들은 컴퓨팅 디바이스 리소스의 소유자인 컴퓨팅 디바이스 리소스에 대한 액세스를 요청하는 엔터티의 아이덴터티를 통신하기 위해 사용될 수도 있다.

[0052] 가상 리소스 식별자들 열 (404) 은, 행 (408-414) 에서와 같이, 예를 들어, 동일한 엔트리의 상관된 소유자 또는 잠재적 소유자에 대해, 가상 어드레스 대 물리적 어드레스 맵에 따라, 컴퓨팅 디바이스 리소스의 물리적 리소스 식별자에 맵핑되는, 가상 어드레스와 같은, 가상 기소스 식별자를 포함할 수도 있다. 언급된 바와 같이, 소유자 또는 잠재적 소유자를 컴퓨팅 디바이스 리소스와 상관시키기 위해, 컴퓨팅 디바이스 리소스의 물리적 어드레스 및 물리적 컴퓨팅 디바이스 리소스 식별자를 포함하는 다른 데이터가 사용될 수도 있다.

[0053] 일부 구현들에서, 소유권 테이블 (400) 은 오직 컴퓨팅 디바이스 리소스들의 현재 소유자들에 대한 엔트리들만을 포함한다. 이러한 구현들에서, 컴퓨팅 디바이스 리소스의 소유권에서의 변경에 응답하여 소유권 테이블 (400) 로부터 엔트리가 제거될 수도 있다. 엔트리들을 제거하는 것은 제거된 엔트리들을 삭제, 무효화 또는 덮어쓰기하는 것을 수반할 수도 있다.

[0054] 일부 구현들에서, 소유권 테이블 (400) 은, 엔트리가 동일한 엔트리의 소유자 식별자와 연관된 소유자에 의한 컴퓨팅 디바이스 리소스의 현재 소유권을 나타내는지 여부를 나탸내기 위한 값을 포함할 수도 있는, 선택적 유효성 표시자들 열 (406) 을 포함할 수도 있다. 선택적 유효성 표시자들 열 (406) 을 포함하는 것은, 컴퓨팅 디바이스 리소스들의 소유자들의 과거, 현재, 및 잠재적 엔트리들의 저장을 허용할 수도 있다. 컴퓨팅 디바이스 리소스의 현재 소유권을 나타내는 값을 포함하는 엔트리들은, 행들 (408, 410, 및 414) 에서 나타낸 바와 같이 불리언 값 "1" 과 같이, 선택적 유효성 표시자들 열 (406) 에서의 지정된 값을 포함할 수도 있다. 컴퓨팅 디바이스 리소스의 과거 또는 잠재적 소유권을 나타내는 값을 포함하는 엔트리들은, 행 (412) 에서 나타낸 바와 같이 불리언 값 "0" 과 같이, 선택적 유효성 표시자들 열 (406) 에서의 다른 지정된 값을 포함할 수도 있다. 선택적 유효성 표시자들 열 (406) 을 포함하는 구현들은 컴퓨팅 디바이스 리소스의 소유권에서의 변화에 응답하여 비-현재 소유권의 엔트리들을 보유할 수도 있다. 선택적 유효성 표시자들을 포함하는 실시형태들은, 컴퓨팅 디바이스 리소스의 소유권이 취해짐에 따라 소유권 테이블 (400) 에 새로운 엔트리들을 추가할 수도 있고, 또는, 소유권 테이블 (400) 은 컴퓨팅 디바이스 리소스들 및 그것들의 잠재적 소유자들의 가능한 조합들의 일부 또는 전부로 사전-팝퓰레이팅될 수도 있다. 일부 구현들에서, 소유권 테이블 (400) 에서의 엔트리들의 수에 대해 제한 "N" 이 존재할 수도 있고, 엔트리들은 현재의 또는 잠재적 소유권들을 추가하기 위해 대체 기준에 따라 제거될 수도 있다.

[0055] 예시적인 소유권 테이블 (400) 은 다양한 구현들에서 어드레싱될 있는 다양한 소유권 상황들을 예시한다. 예를 들어, 행 (408) 은, 소유자 및 컴퓨팅 디바이스 리소스에 대한 가상 리소스 식별자 대 컴퓨팅 디바이스 리소스 맵핑에 따라, 소유자 식별자 "01" 에 의해 지정된 소유자 엔터티가 가상 리소스 식별자 "VA1" 에 의해 표현되는 컴퓨팅 디바이스 리소스를 소유할 수도 있는 것을 나타낸다. 다양한 구현들에서, 가상 리소스 식별자 "VA1" 는 소유자 및 컴퓨팅 디바이스 리소스에 대한 물리적 어드레스에 맵핑되는 가상 어드레스일 수도 있다. 선택적 유효성 표시자들 열 (406) 을 배제하는 구현들에서, 행 (408) 에서의 데이터의 존재는, 소유자 식별자 "01" 에 의해 지정된 소유자 엔터티가 가상 리소스 식별자 "VA1" 에 의해 표현되는 컴퓨팅 디바이스 리소스를 현재 소유하고 있는 것을 나타낼 수도 있다. 선택적 유효성 표시자들 열 (406) 을 포함하는 예들에서, 요효성 표시자의 값이 "1" 임에 따라, 동일한 결과가 나타내어질 수도 있다.

[0056] 행 (410) 의 추가적인 포함은, 소유자 및 컴퓨팅 디바이스 리소스에 대한 가상 리소스 식별자 대 컴퓨팅 디바이스 리소스 맵핑에 따라, 행 (408) 에서의 동일한 소유자 엔터티가 또한, 가상 리소스 식별자 "VA2" 에 의해 표현되는 컴퓨팅 디바이스 리소스를 소유할 수도 있는 것을 나타낸다.

[0057] 행 (412) 은, 소유자 및 컴퓨팅 디바이스 리소스에 대한 가상 리소스 식별자 대 컴퓨팅 디바이스 리소스 맵핑에

따라, 소유자 식별자 "O2" 에 의해 지정된 소유자 엔터티가 가상 리소스 식별자 "VB1" 에 의해 표현되는 컴퓨팅 디바이스 리소스의 소유자일 수도 있는 것을 나타낸다. 하지만, 선택적 유효성 표시자들 열 (406) 에서의 "0" 의 유효성 표시자 값은, 소유자 식별자 "O2" 에 의해 지정된 소유자 엔터티가, 가상 리소스 식별자 "VB1" 에 의해 표시된 컴퓨팅 디바이스 리소스의, 현재 소유자라기 보다는, 과거의 또는 잠재적인 소유자임을 나타낼 수도 있다. 선택적 유효성 표시자들 열 (406) 을 배제하는 일부 구현들에서, 행 (412) 은 소유권 테이블 (400) 로부터 생략될 수도 있다.

[0058] 도 5 는, 컴퓨팅 디바이스 리소스들에 대한 과거, 현재, 및/또는 잠재적 요청 엔터티들의 기능 인증들의 데이터를 저장하기 위해 데이터 보호 시스템 (300) 이 사용할 수도 있는 인증 테이블 (500) 의 비-제한적인 예를 나타낸다. 다양한 구현들은, 요청 엔터티 식별자들, 인증 데이터 또는 인증 데이터 레퍼런스들, 및 액세스 타입들을 포함하는, 기능 인증 데이터의 상이한 조합들 및 정렬을 포함할 수도 있다.

[0059] 일부 구현들에서, 용어들 인증 데이터 및 인증 데이터 레퍼런스들은 상호교환가능하게 사용될 수도 있다. 예시적인 인증 테이블 (500) 은 요청 엔터티 식별자들 열 (502) 및 인증서들 열 (504) 을 포함한다. 본원에서 추가로 논의되는 바와 같이, 인증 테이블 (500) 은 또한 선택적 액세스 타입들 열 (506) 을 포함할 수도 있다. 인증 테이블 (500) 은 다수의 행들, 예를 들어, 컴퓨팅 디바이스 리소스들에 대한 요청 엔터티의 상이한 인증된 기능을 각각 표현하는 행들 (508-514) 을 포함할 수도 있다.

[0060] 요청 엔터티 식별자들 열 (502) 은 컴퓨팅 디바이스의 각각의 요청 엔터티 또는 잠재적 요청 엔터티에 대한 고유한 식별자들을 포함할 수도 있다. 요청 엔터티 식별자들은 컴퓨팅 디바이스 리소스에 대한 액세스를 요청하는 엔터티의 아이덴터티를 통신하기 위해 사용될 수도 있다.

[0061] 인증서들 열 (504) 은, 요청 엔터티에 대한 또는 요청 엔터티의 기능에 대한 인증서, 또는 인증서가 저장되는 로케이션에 대한 포인터와 같은 레퍼런스를 포함할 수도 있다. 일부 구현들에서, 인증 테이블 (500) 은 오직, 컴퓨팅 디바이스 리소스들에 대한 현재 요청 엔터티들에 대한 엔트리들만을 포함한다. 이러한 구현들에서, 그들 각각의 소유된 컴퓨팅 디바이스 리소스들에 대한 액세스를 요청하는 어떤 소유자들도 인증 테이블 (500) 에 리스트되지 않을 수도 있도록, 컴퓨팅 디바이스 리소스의 소유권에서의 변화에 응답하여 인증 테이블 (500) 로부터 엔트리가 제거될 수도 있다. 엔트리들을 제거하는 것은 제거된 엔트리들을 삭제하는 것, 무효화하는 것 또는 덮어쓰기하는 것을 수반할 수도 있다.

[0062] 일부 구현들에서, 인증 테이블 (500) 에 대한 엔트리들은, 컴퓨팅 디바이스 리소스들에 대해 액세스하기 위한 요청들이 이루어짐에 따라 추가될 수도 있고, 또는, 인증 테이블 (500) 은 잠재적인 요청 엔터티들 및 그들의 인증서들의 가능합 조합의 일부 또는 전부로 사전-팝퓰레이팅될 수도 있다. 일부 구현들에서, 컴퓨팅 디바이스 리소스의 소유권에서의 변화에도 불구하고 엔트리들은 유지될 수도 있다. 인증 테이블 (500) 에서 요청 엔터티들로서 소유자들을 포함하는 일부 구현들에서, 컴퓨팅 디바이스 리소스의 소유권은 리소스 콘텐츠의 가상적 뷰를 암호화하기 전에 확인될 수도 있다. 일부 구현들에서, 인증 테이블 (500) 에서의 엔트리들의 수에 대해 제한 "M" 이 존재할 수도 있고, 엔트리들은 현재의 또는 잠재적 요청 엔터티들을 추가하기 위해 대체 기준에 따라 제거될 수도 있다.

[0063] 일부 구현들에서, 인증 테이블 (500) 은 선택적 액세스 타입들 열 (506) 을 포함할 수도 있고, 이는 요청 엔터티가 허가되는 리소스 콘텐츠들에 대한 액세스의 타입을 나타내기 위한 값을 포함할 수도 있다. 선택적 액세스 타입들 열 (506) 을 포함하는 것은, 채용할 암호화의 타입을 결정하는데 보다 적은 시간 및 리소스들이 소비될 수도 있으므로 보다 빠른 암호화를 허용할 수도 있다. 요청 엔터티 및 인증된 기능에 대한 액세스 타입들을 나타내는 값을 포함하는 엔트리들은 암호화의 타입 및/또는 레벨과 상관된 액세스 타입의 식별자를 포함할 수도 있고, 또는, 암호화의 타입 및/또는 레벨의 식별자를 포함할 수도 있다. 선택적 액세스 타입들 열 (506) 에서의 값은 인증된 기능 및/또는 요청 엔터티가 소유자인지 여부와 상관될 수도 있다.

[0064] 일부 구현들에서, 소유자 요청 엔터티는 인증된 기능에 대해, 또는 기능에 무관하게, 리소스 콘텐츠에 대한 가려지지 않은 액세스를 승인받을 수도 있다. 행 (508) 은 또한 요청된 컴퓨팅 디바이스 리소스의 소유자인 요청 엔터티의 일 예를 나타낸다. 행들 (510-514) 은 요청된 컴퓨팅 디바이스 리소스의 소유자들이 아닌 요청 엔터티들을 나타낸다. 행들 (510-514) 에서의 요청 엔터티들의 각각의 인증된 기능은, 데이터 보호 시스템 (300) 이 요청 엔터티에 제공된 요청된 리소스 콘텐츠들의 가상 뷰에 적용할 수도 있는 암호화의 타입 및/또는 레벨을 제어하는 특정된 액세스 타입과 상관될 수도 있다. 예를 들어, 행 (510) 은, 요청 엔터티 "R1" 에 대한 인증서 "CA2" 가 요청된 리소스 콘텐츠의 가상 뷰의 오직 부분적 가림만을 허용할 수도 있음을 나타낸다. 데이터 보호 시스템 (300) 은 요청 엔터티 "R1" 에 의해 이루어진 요청에 대해 요청된 리소스 콘텐츠의

가상 뷰들에 대해 전체적 또는 부분적 호모모픽 암호화를 적용할 수도 있다. 유사하게, 행들 (512 및 514) 은, 요청 엔터티들 "R2" 및 "RN" 각각에 대한 인증서들 "CB1" 및 "CC1" 은 요청된 리소스 콘텐츠의 가상 뷰들의 오직 가림만을 허용할 수도 있음을 나타낸다. 데이터 보호 시스템 (300) 은, 요청 엔터티들 "R2" 및 "RN" 에 의해 이루어진 요청들에 대해 요청된 리소스 콘텐츠의 가상 뷰에 대해 강한 암호화를 적용할 수도 있다.

[0065] 데이터 보호 시스템 (300), 가상화 인터페이스 모니터 (302), 리소스 콘텐츠 암호화 디바이스 (304), 소유권 테이블 (400), 및 인증 테이블 (500) 의 컴포넌트들은 청구항들의 범위로부터 벗어남이 없이 다양한 구현들에서 상이하게 배열될 수도 있다. 일부 구현들에서, 소유권 테이블 (400) 및 인증 테이블 (500) 은 보다 많은 테이블들로 결합, 분할될 수도 있거나, 소유권 테이블 (400) 및 인증 테이블 (500) 의 다른 것에 포함되는 것으로 기술된 하나 이상의 항목들을 포함할 수도 있다.

[0066] 도 6 은 다양한 실시형태들에 따른, 가상 리소스 뷰들을 이용하여 데이터를 보호하기 위한 방법 (600) 을 나타낸다. 방법 (600) 은 데이터 보호 시스템, 가상화 인터페이스 모니터, 및/또는 리소스 콘텐츠 암호화 디바이스를 구현하는 전용 하드웨어 상에서 및/또는 프로세서와 같은 범용 하드웨어 상에서 실행되는 소프트웨어를 이용하여 컴퓨팅 디바이스에서 실행될 수도 있다.

[0067] 블록 (602) 에서, 컴퓨팅 디바이스는 소유자에 대해 컴퓨팅 디바이스 리소스의 소유권을 할당하도록 리소스 관리자를 실행할 수도 있다. 상기 논의된 바와 같이, 리소스 관리자는 오퍼레이팅 시스템, 하이퍼바이저, 및/또는 트러스트존을 포함할 수도 있고, 소유자는 애플리케이션, 오퍼레이팅 시스템, 하이퍼바이저, 및/또는 트러스트존을 포함할 수도 있다. 소유자에게 컴퓨팅 디바이스 리소스의 소유권을 할당하는 것은 소유자가 컴퓨팅 디바이스 리소스의 소유권을 취할 준비가 된 경우에 리소스 관리자가 소유자에게 소유권을 승인하도록 허용한다. 예를 들어, 컴퓨팅 디바이스 리소스의 소유권은 소유자에게 할당될 수도 있지만, 소유자는 컴퓨팅 디바이스 리소스의 소유권을 취할 준비가 되기 전에 완료할 다른 프로세스들 또는 이용가능하게 될 다른 리소스들에 대해 대기하고 있을 수도 있다. 컴퓨팅 디바이스 리소스의 소유권의 할당은, 소유권이 일정 기간 내에 취해지지 않는 경우에 만료될 수도 있고, 이에 의해 컴퓨팅 디바이스 리소스가 다른 소유자들에 대한 할당을 위해 이용가능하게 된다. 일부 실시형태들에서, 컴퓨팅 디바이스 리소스의 소유권의 할당은, 소유권에 대한 요청, 소유권에 대한 큐에서의 다음 소유자, 리소스의 이용가능성의 브로드캐스트 또는 다이렉트 신호에 대해 응답하기 위한 제 1 소유자, 또는, 전력 및 성능 파라미터들을 포함하는 다양한 기준들에 기초하여 다음 소유자를 결정하기 위한 알고리즘에 대해 응답적일 수도 있다.

[0068] 블록 (604) 에서, 컴퓨팅 디바이스는 할당된 소유자에 의한 컴퓨팅 디바이스 리소스들의 소유권에 대한 요청들을 모니터링할 수도 있다. 일부 실시형태들에서, 컴퓨팅 디바이스 리소스의 할당된 소유자는 컴퓨팅 디바이스 리소스의 소유권의 할당의 수용을 확인응답하기 위해 컴퓨팅 디바이스의 소유권을 요청할 수도 있다. 일부 실시형태들에서, 컴퓨팅 디바이스 리소스의 소유권에 대한 요청은 컴퓨팅 디바이스 리소스의 할당된 소유자의 소유권의 다른 컴포넌트들, 시스템들, 및/또는 잠재적 소유자들에 시그널링될 수도 있다. 할당된 소유자에 의한 컴퓨팅 디바이스 리소스의 소유권에 대한 요청을 모니터링하기 위해, 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은 컴퓨팅 디바이스 리소스들의 소유권에 대한 요청을 수신, 검출, 또는 차단할 수도 있다.

[0069] 블록 (606) 에서, 컴퓨팅 디바이스는 컴퓨팅 디바이스 리소스의 소유권의 변화들을 트래킹할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은 컴퓨팅 디바이스 리소스의 소유자인 엔터티를 결정하기 위해 컴퓨팅 디바이스 리소스의 소유권에 대한 요청의 정보를 이용할 수도 있다. 컴퓨팅 디바이스 리소스의 소유권을 트래킹하기 위해, 컴퓨팅 디바이스는 도 7 을 참조하여 방법 (700) 에 대해 추가로 설명되는 바와 같이 소유권 테이블과 같은 테이블 또는 데이터 구조를 업데이트할 수도 있다.

[0070] 블록 (608) 에서, 컴퓨팅 디바이스는 임의의 엔터티, 소유자, 또는 비-소유자에 의한 컴퓨팅 디바이스 리소스들을 액세스하기 위한 요청들을 모니터링할 수도 있다. 일부 실시형태들에서, 컴퓨팅 디바이스 리소스의 소유자는 리소스 콘텐츠에 판독 또는 기입하기 위해 컴퓨팅 디바이스 리소스를 액세스하도록 요청할 수도 있다. 일부 실시형태들에서, 비-소유자들은, 리소스 콘텐츠를 이동, 카피, 또는 검색하는 것과 같이 리소스 콘텐츠의 관리 기능들을 구현하기 위해 컴퓨팅 디바이스 리소스에 대한 액세스를 합법적으로 요청할 수도 있다. 하지만, 비-소유자들에 의한 컴퓨팅 디바이스 리소스를 액세스하기 위한 일부 요청들은 리소스 콘텐츠에 대한 액세스를 얻기 위해 비-소유자에게 영향을 미치거나 비-소유자의 제어를 취한 악성 행위자들에 의해 촉구될 수도 있다. 컴퓨팅 디바이스 리소스들을 액세스하기 위한 요청들을 모니터링하기 위해, 프로세서, 데이터 보호 시

스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은 컴퓨팅 디바이스 리소스들에 대해 액세스하기 위한 요청을 수신, 검출, 또는 차단할 수도 있다. 컴퓨팅 디바이스는 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에서 타겟팅된 가상 리소스 식별자들과 같이, 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청으로부터 정보를 추출할 수도 있다. 이에 의해, 컴퓨팅 디바이스는 컴퓨팅 디바이스 리소스들을 액세스하기 위한 요청들 및 그 요청들에 대한 응답에서 사용되는 컴퓨팅 디바이스 리소스들의 가상 리소스 식별자들을 번역하는 것을 담당하는 컴퓨팅 디바이스의 가상화 인터페이스를 모니터링할 수도 있다. 예를 들어, 컴퓨팅 디바이스는 컴퓨팅 디바이스 리소스의 가상 어드레스를 추출하고, 가상 어드레스 및 물리적 어드레스 변환들을 담당하는 가상화 인터페이스를 모니터링할 수도 있다.

[0071] 결정 블록 (610) 에서, 컴퓨팅 디바이스는, 컴퓨팅 디바이스 리소스들을 액세스하기 위한 모니터링된 요청이 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에서 타겟팅된 컴퓨팅 디바이스 리소스의 소유자로부터 유래되는 것인지 여부를 결정할 수도 있다. 동일한 컴퓨팅 디바이스 리소스에 대해 상이한 엔터티들, 소유자들 및 비-소유자들이 상이한 가상 리소스 식별자들 대 컴퓨팅 디바이스 리소스 맵들을 채용할 수도 있다. 가상화 인터페이스는 컴퓨팅 디바이스의 엔터티들의 어느 것이 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청을 발행하였는지를 식별하기 위해 사용될 수도 있다.

[0072] 결정 블록 (610) 에서의 동작들의 일부로서, 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은, 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청으로부터 추출된 정보를 사용하고, 그것을 소유권 테이블에서의 정보에 대해 비교할 수도 있다. 일부 구현들에서, 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에서 타겟팅된 가상 리소스 식별자는 요청 엔터티와 상관될 수도 있다. 상관은 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에서 타겟팅된 가상 리소스 식별자에 대한 요청을 실시할 엔터티를 식별하기 위해 가상화 인터페이스 맵핑들을 이용하여 이루어질 수도 있다. 일부 구현들에서, 식별된 요청자는 소유권 테이블에서의 소유자 식별자로서 겹칠 수도 있는 엔터티 식별자와 상관될 수도 있다.

[0073] 일부 구현들에서, 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에 관련된 엔터티 식별자 및/또는 가상 리소스 식별자는 매치 (match) 가 발견되는지 여부를 결정하기 위해 소유권 테이블에서의 동일한 타입들의 정보의 엔트리들에 대해 비교될 수도 있다. 일부 구현들에서, 소유권 테이블은 오직 현재 소유자들의 엔트리들만을 포함할 수도 있고, 매치는 요청자가 소유자임을 나타낼 수도 있는 한편, 매치가 없는 것은 요청자가 비-소유자임을 나타낼 수도 있다. 일부 구현들에서, 소유권 테이블은 컴퓨팅 디바이스 리소스들의 과거, 현재, 및/또는 잠재적 소유자들의 엔트리들을 포함할 수도 있고, 유효성 표시자와 같은 소유권 테이블로부터의 추가적인 정보는 매치가 또한 요청자가 소유자 또는 비-소유자인 것을 나타내는지 여부를 결정하기 위해 체크될 수도 있다. 예를 들어, 유효성 표시자는 요청자가 소유자인 것을 나타내는 매칭 엔트리가 유효한 것을 나타낼 수도 있다. 반대로, 유효성 표시자는 요청자가 비-소유자인 것을 나타내는, 매칭 엔트리가 유효하지 않은 것을 나타낼 수도 있다.

[0074] 컴퓨팅 디바이스 리소스를 액세스하기 위한 모니터링된 요청이 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에서 타겟팅된 컴퓨팅 디바이스 리소스의 소유자로부터 발신된 것이라고 결정하는 것에 응답하여 (즉, 결정 블록 (610) = "예"), 컴퓨팅 디바이스는, 블록 (612) 에서 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에 응답하여 제공된 리소스 콘텐츠의 가려지지않은/암호화되지않은 가상 뷰를 제공할 수도 있다. 특정된 가상 리소스 식별자에 대한 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청은 컴퓨팅 디바이스로 하여금 컴퓨팅 디바이스 리소스의 리소스 콘텐츠를 요청자에게 리턴하도록 촉구할 수도 있다. 일부 구현들에서, 컴퓨팅 디바이스는 가상 뷰로서 리소스 콘텐츠를 제공하도록 구성될 수도 있다. 이와 같이, 컴퓨팅 디바이스는 요청 엔터티에 의한 리소스 콘텐츠의 프로세싱 동안 버그 또는 에러의 경우에 손상되는 것으로부터 리소스 콘텐츠를 보호하는 것이 가능할 수도 있다. 컴퓨팅 디바이스는 또한, 가상 뷰들을 이용함으로써 리소스 콘텐츠에 대한 상이한 액세스를 동시에 다수의 엔터티들에 제공하는 것이 가능할 수도 있다. 일부 구현들에서, 컴퓨팅 디바이스 리소스의 소유자는 리소스 콘텐츠에 대한 악성 액세스에 대해 사용되지 않도록 신뢰될 수도 있어서, 소유자는 소유자 컴퓨팅 디바이스 리소스로부터의 리소스 콘텐츠의 가려지지않은/암호화되지않은 가상 뷰가 제공된다. 일부 구현들에서, 프로세서, 데이터 보호 시스템 및/또는 리소스 콘텐츠 암호화 디바이스를 포함하는 컴퓨팅 디바이스의 컴포넌트들은 가상 뷰의 가림/암호화 없이 리소스 콘텐츠의 가상 뷰를 생성 또는 패스할 수도 있다. 일부 구현들에서, 컴퓨팅 디바이스 컴포넌트들은 리소스 콘텐츠의 가상 뷰의 가림/암호화가 필요하지 않음에 따라 바이패스될 수도 있다.

[0075] 컴퓨팅 디바이스 리소스를 액세스하기 위한 모니터링된 요청이 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에서 타겟팅된 컴퓨팅 디바이스 리소스의 비-소유자로부터 발신된 것이라고 결정하는 것에 응답하여 (즉, 결정

블록 (610) = "아니오"), 컴퓨팅 디바이스는, 블록 (614) 에서 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청에 응답하여 제공된 리소스 콘텐츠의 가상 뷰를 가릴 수도 있다. 컴퓨팅 디바이스는, 도 8 을 참조하여 방법 (800) 과 관련하여 추가로 설명되는 바와 같이, 리소스 콘텐츠의 가상 뷰를 가리기 위한 암호화의 타입 및/또는 레벨을 결정할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 리소스 콘텐츠 암호화 디바이스를 포함하는 컴퓨팅 디바이스의 컴포넌트들은 비-소유잗르을 통한 악성 액세스로부터 리소스 콘텐츠를 보호하기 위해 리소스 콘텐츠의 가상 뷰를 가릴 수도 있다. 일부 구현들에서, 리소스 콘텐츠의 가상 뷰를 가리는 것은 비-소유자들이 리소스 콘텐츠의 분명한 뷰를 가짐이 없이 적법한 액세스 및 관리상의 기능들을 구현하는 것을 금지하지 않는다. 일 예에서, 리소스 콘텐츠는, 리소스 콘텐츠가 변경되지 않고 오직 그것들의 로케이션이 변경됨에 따라 블록에서 이동되고 있을 때 중요하지 않은 것일 수도 있고, 또한 리소스 콘텐츠를 이동시키는 엔터티는 리소스 콘텐츠의 데이터의 상세한 특성을 알 필요도 없다. 다른 예에서, 리소스 콘텐츠를 부분적으로 가리는 것은, 가려지지않은 리소스 콘텐츠에서의 필요한 피드백 또는 대응하는 변경들을 제공하는 비-소유자들에 의한 기능들을 구현하기 위해 충분할 수도 있는 암호문의 일부 검색 및 산술적 조작을 허용할 수도 있다.

[0076] 블록 (616) 에서, 컴퓨팅 디바이스는 리소스 콘텐츠의 가려진/암호화된 가상 뷰를 제공할 수도 있다. 블록 (612) 에서의 가려지지않은/암호화되지않은 가상 뷰들의 제공과 유사하게, 컴퓨팅 디바이스는 리소스 콘텐츠의 가상 뷰를 요청 엔터티에 제공할 수도 있다. 하지만, 비-소유자들에게 제공된 가상 뷰들은 가림/암호화된다.

[0077] 블록 (618) 에서, 컴퓨팅 디바이스는 소유된 컴퓨팅 디바이스 리소스들의 릴리스들을 트래킹할 수도 있다. 블록 (604) 에서 컴퓨팅 디바이스 리소스들의 소유권에 대해 요청들을 모니터링하는 것과 유사한 방식으로, 컴퓨팅 디바이스는 소유된 컴퓨팅 디바이스 리소스들의 릴리스를 나타내는 신호를 수신, 검출, 또는 차단할 수도 있다. 릴리스 신호 (release signal) 는 컴퓨팅 디바이스 리소스가 소유권에 대해 이용가능한 것을 컴퓨팅 디바이스의 컴포넌트들 또는 다른 엔터티들에게 통지할 수도 있다. 일부 실시형태들에서, 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은 릴리스 신호에 응답하여 소유권 테이블을 업데이트할 수도 있다. 일부 실시형태들에서, 전의 소유자에 의한 컴퓨팅 디바이스 리소스의 소유권을 나타내는 엔트리는 소유권 테이블로부터 제거되거나 유효하지 않은 것으로 마킹될 수도 있다.

[0078] 도 7 은 다양한 실시형태들에 따른, 컴퓨팅 디바이스 리소스들의 소유권을 트래킹하기 위한 방법 (700) 을 나타낸다. 방법 (700) 은 데이터 보호 시스템, 가상화 인터페이스 모니터, 및/또는 리소스 콘텐츠 암호화 디바이스를 구현하는 전용 하드웨어 상에서 및/또는 프로세서와 같은 범용 하드웨어 상에서 실행되는 소프트웨어를 이용하여 컴퓨팅 디바이스에서 실행될 수도 있다.

[0079] 결정 블록 (702) 에서, 컴퓨팅 디바이스는 컴퓨팅 디바이스 리소스에 대해 소유권 테이블과 같은 데이터 구조 또는 테이블에서 엔트리가 존재하는지 여부를 결정할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은, 컴퓨팅 디바이스 리소스들을 액세스하기 위한 요청들의 가상 리소스 식별자들을 소유권 테이블의 엔트리들에 저장된 대응하는 정보의 값들에 대해 비교할 수도 있다. 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청의 동일한 가상 리소스 식별자를 갖는 엔트리는, 컴퓨팅 디바이스의 컴포넌트에 대해 엔트리가 존재하는 것을 나타낼 수도 있다. 추가적으로, 상이한 소유자들은 동일한 컴퓨팅 디바이스 리소스에 맵핑할 상이한 가상 리소스 식별자들을 사용할 수도 있기 때문에, 가상 리소스 식별자를 갖는 엔트리는, 요청 소유자에 의해 소유된 컴퓨팅 디바이스의 컴포넌트에 대해 엔트리가 존재하는 것을 나타낼 수도 있다. 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청의 동일한 가상 리소스 식별자를 갖는 엔트리의 결여는, 컴퓨팅 디바이스의 컴포넌트에 대해 아무런 엔트리도 존재하지 않는 것을 나타낼 수도 있다. 하지만, 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청의 동일한 가상 리소스 식별자들을 갖는 엔트리의 결여는 그보다는 오히려, 컴퓨팅 디바이스 리소스의 소유권을 요청하는 현재 소유자에 의해 과거에, 현재, 또는 잠재적으로 소유되는 컴퓨팅 디바이스의 컴포넌트에 대한 엔트리의 결여를 나타낼 수도 있다. 상이한 소유자들은 동일한 컴퓨팅 디바이스 리소스에 맵핑할 상이한 가상 리소스 식별자들을 이용할 수도 있기 때문에, 컴퓨팅 디바이스의 다른 과거, 현재, 또는 잠재적 소유자들에 대해 엔트리들이 존재할 수도 있다. 일부 구현들에서, 컴퓨팅 디바이스는 또한, 다른 과거, 현재, 또는 잠재적 소유자들에 의해 사용되는 컴퓨팅 디바이스의 컴포넌트의 가상 리소스 식별자들을 체크할 수도 있다.

[0080] 컴퓨팅 디바이스 리소스에 대한 소유권 테이블에서 엔트리가 존재하지 않는다고 결정하는 것에 응답하여 (즉, 결정 블록 (702) = "아니오"), 컴퓨팅 디바이스는 블록 (710) 에서 컴퓨팅 디바이스 리소스에 대한 소유권 테이블에서 엔트리를 생성할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은, 기존의 엔트리를 편집하거나 새로운 엔트리를 생서하기 위해, 컴퓨팅 디바

이스 리소스의 소유권에 대한 요청의 가상 리소스 식별자 및/또는 가상 리소스 식별자에 상관된 식별된 소유자 식별자를 포함하는 데이터를 소유권 테이블에 기입할 수도 있다. 일부 구현들에서, 기존의 엔트리들은 진부해진 것이거나 컴퓨팅 디바이스 리소스들의 소유권의 상태에 더 이상 관련되지 않을 수도 있고, 덮어쓰기될 수도 있다.

[0081] 일부 실시형태들에서, 선택적 블록 (712) 에서, 컴퓨팅 디바이스는, 본원에서 추가로 상세히 설명되는 바와 같이, 컴퓨팅 디바이스 리소스의 요청 소유자에 대해 새로운 엔트리를 마킹할 수도 있다. 컴퓨팅 디바이스는, 도 6 을 참조하여 설명된 바와 같이, 블록 (608) 에서 임의의 엔터티에 의해 컴퓨팅 디바이스 리소스들을 액세스하기 위한 요청을 모니터링하도록 진행할 수도 있다.

[0082] 컴퓨팅 디바이스 리소스들에 대한 소유권 테이블에서 엔트리가 존재한다고 결정하는 것에 응답하여 (즉, 결정 블록 (702) = "예"), 컴퓨팅 디바이스는 결정 블록 (704) 에서 컴퓨팅 디바이스 리소스의 요청 소유자가 컴퓨팅 디바이스 리소스의 이전 소유자와 동일한지 여부를 결정할 수도 있다. 본원에서 논의된 바와 같이, 컴퓨팅 디바이스 리소스의 과거, 현재, 또는 잠재적 소유자는 컴퓨팅 디바이스 리소스의 소유권에 대한 요청의 가상 리소스 식별자 또는 상관된 소유자 식별자에 의해 식별될 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은, 요청 소유자가 동일한 컴퓨팅 디바이스 리소스에 대한 엔트리에서 리스트된 소유자와 동일한지 여부를 결정하기 위해, 컴퓨팅 디바이스 리소스에 대한 소유권 요청의 데이터 및 식별된 엔트리들을 비교할 수도 있다.

[0083] 컴퓨팅 디바이스 리소스의 요청 소유자가 컴퓨팅 디바이스 리소스의 이전 소유자와 동일하지 않다고 결정하는 것에 응답하여 (즉, 결정 블록 (704) = "아니오"), 컴퓨팅 디바이스는 선택적 블록 (708) 에서 상이한 소유자를 갖는 컴퓨팅 디바이스 리소스에 대한 엔트리를 제거하거나 유효하지 않은 것으로 마킹할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은 컴퓨팅 디바이스 리소스 소유권 요청과 동일한 컴퓨팅 디바이스 리소스의 상이한 소유자를 갖는 임의의 엔트리를 제거할 수도 있다. 일부 실시형태들에서, 컴퓨팅 디바이스 리소스 소유권 요청과 동일한 컴퓨팅 디바이스 리소스에 대해 상이한 소유자들을 갖는 엔트리들은 유지되지만 소유권 테이블에서의 엔트리에 대해 유효성 표시자를 설정함으로써 유효하지 않은 것으로서 마킹될 수도 있다. 동일한 컴퓨팅 디바이스 리소스에 대한 다른 엔트리들은 그것들의 가상 리소스 식별자들 및 동일한 컴퓨팅 디바이스 리소스에 대한 그것들 각각의 맵핑들에 의해 식별될 수도 있다.

[0084] 본원에서 추가로 설명되는 바와 같이, 블록 (710) 에서, 컴퓨팅 디바이스는 컴퓨팅 디바이스 리소스에 대한 소유권 테이블에서 엔트리를 생성할 수도 있고, 선택적 블록 (712) 에서, 컴퓨팅 디바이스는 컴퓨팅 디바이스 리소스의 요청 소유자에 대해 새로운 엔트리를 마킹할 수도 있다. 컴퓨팅 디바이스는 도 6 을 참조하여 설명된 바와 같이 블록 (608) 에서 임의의 엔터티에 의해 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청들을 모니터링할 수도 있다.

[0085] 컴퓨팅 디바이스 리소스의 요청 소유자가 컴퓨팅 디바이스 리소스의 이전 소유자와 동일하다고 결정하는 것에 응답하여 (즉, 결정 블록 (704) = "예"), 컴퓨팅 디바이스는 선택적 결정 블록 (706) 에서 컴퓨팅 디바이스 리소스의 요청 소유자와 동일한 소유자에 대한 엔트리가 유효한지 여부를 결정할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은, 동일한 컴퓨팅 디바이스 리소스 및 소유자에 대해 소유권 테이블에서의 엔트리에 대한 유효성 표시자의 값을 체크할 수도 있다.

[0086] 컴퓨팅 디바이스 리소스의 요청 소유자와 동일한 소유자에 대한 엔트리가 유효하다고 결정하는 것에 응답하여 (즉, 결정 블록 (706) = "예"), 컴퓨팅 디바이스는 도 6 을 참조하여 설명된 바와 같이 블록 (608) 에서 임의의 엔터티에 의해 컴퓨팅 디바이스 리소스를 액세스하기 위한 요청들을 모니터링할 수도 있다.

[0087] 컴퓨팅 디바이스 리소스의 동일한 소유자에 대한 엔트리가 유효하지 않다고 결정하는 것에 응답하여 (즉, 결정 블록 (706) = "아니오"), 컴퓨팅 디바이스는 선택적 블록 (712) 에서 컴퓨팅 디바이스 리소스의 동일한 소유자에 대한 엔트리를 유효한 것으로서 마킹할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은 그 엔트리가 유효하지 않다기보다는 유효하다고 표시하기 위해 소유권 테이블에서 유효성 표시자의 값을 수정할 수도 있다. 컴퓨팅 디바이스는 도 6 을 참조하여 설명된 바와 같이 블록 (608) 에서 임의의 엔터티에 의해 컴퓨팅 디바이스 리소스들을 액세스하기 위한 요청들을 모니터링할 수도 있다.

[0088] 도 8 은 리소스 콘텐츠의 가상 뷰들에 대해 암호화를 적용하기 위해 인증서들을 이용하기 위한 일 실시형태의

방법 (800) 을 나타낸다. 방법 (800) 은 데이터 보호 시스템, 가상화 인터페이스 모니터, 및/또는 리소스 콘텐츠 암호화 디바이스를 구현하는 전용 하드웨어 상에서 및/또는 프로세서와 같은 범용 하드웨어 상에서 실행되는 소프트웨어를 이용하여 컴퓨팅 디바이스에서 실행될 수도 있다.

[0089] 블록 (802) 에서, 컴퓨팅 디바이스는 비-소유자 컴퓨팅 디바이스 리소스 액세스 요청자가 기능을 위한 인증서와 연관되는지 여부를 결정할 수도 있다. 본원에서 논의된 바와 같이, 비-소유자 리소스 관리자들 및 애플리케이션들, 또는 비-소유자 요청 엔터티들은 그들이 소유하지 않는 컴퓨팅 디바이스 리소스들에 대해 컴퓨팅 디바이스 리소스 액세스 요청들을 실시할 수도 있다. 리소스 관리자들 및 애플리케이션들은 컴퓨팅 디바이스의 컴파일러에 의해 또는 개발자들에 의해 인증되는 기능들을 실행하도록 구성될 수도 있다. 기능의 인증서는, 비-소유자 요청 엔터티들에 대해 허용되는 리소스 콘텐츠에 대한 액세스의 레벨을 나타낼 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 가상화 인터페이스 모니터와 같은 컴퓨팅 디바이스의 컴포넌트들은, 비-소유자 요청 엔터티들에 대해 인증 테이블과 같은 데이터 구조 또는 테이블에서 엔트리들이 존재하는지 여부를 결정할 수도 있다. 요청 엔터티 식별자는 상관된 비-소유자 요청 엔터티에 대해 인증 테이블에서 엔트리를 나타낼 수도 있다. 인증 테이블에서의 엔트리의 결여는 요청 엔터티가 인증되지 않은 것을 나타낼 수도 있다.

[0090] 비-소유자 요청 엔터티가 기능에 대한 인증서와 연관된다고 결정하는 것에 응답하여 (즉, 결정 블록 (802) = "예"), 컴퓨팅 디바이스는, 결정 블록 (804) 에서 리소스 콘텐츠에 대한 액세스가 부분적으로 또는 전체적으로 가려지는 것으로서 지정되는지 여부를 결정할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 리소스 콘텐츠 암호화 디바이스를 포함하는 컴퓨팅 디바이스의 컴포넌트들은 비-소유자 요청 엔터티와 상관된 각각의 인증서로부터, 또는 인증 테이블에서의 비-소유자 요청 엔터티에 대한 엔트리로부터 액세스 타입을 취출할 수도 있다. 일부 구현들에서, 인증서 또는 인증서에 대한 레퍼런스는 인증 테이블에서 비-소유자 요청 엔터티에 대한 엔트리에 저장될 수도 있다. 컴퓨팅 디바이스는 인증 테이블로부터 또는 인증서에 대한 레퍼런스의 로케이션으로부터 인증된 것을 취출할 수도 있다. 인증서의 데이터로부터, 컴퓨팅 디바이스는 비-소유자 요청 엔터티에 대한 액세스를 취출할 수도 있다. 일부 구현들에서, 인증 테이블은 비-소유자 요청 엔터티들에 대한 엔트리들에서 액세스 타입을 포함할 수도 있고, 컴퓨팅 디바이스는 인증 테이블에서의 대응하는 엔트리로부터 액세스 타입을 취출할 수도 있다. 본원에서 논의된 바와 같이, 액세스 타입은 비-소유자 요청 엔터티에 리소스 콘텐츠의 가상 뷰를 제공함에 있어서 사용되는, 암호화의 타입 및/또는 레벨, 또는 가림의 레벨을 지정할 수도 있다.

[0091] 리소스 콘텐츠에 대한 액세스가 부분적으로 가려지는 것으로서 지정된다고 결정하는 것에 응답하여 (결정 블록 (804) = "부분적으로"), 컴퓨팅 디바이스는 블록 (806) 에서 리소스 콘텐츠의 가상 뷰를 가림/암호화할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 리소스 콘텐츠 암호화 디바이스를 포함하는 컴퓨팅 디바이스의 컴포넌트들은, 리소스 콘텐츠의 보기, 사용, 또는 조작을 방지하지만 암호문의 검색 또는 산술적 조작을 허용하도록 구성된 부분적 또는 전체적 호모모픽 암호화를 이용하여 리소스 콘텐츠의 가상 뷰를 가림/암호화할 수도 있다. 본원에서 논의된 바와 같이, 비-소유자 요청 엔터티들은, 리소스 콘텐츠 상에서 기능들을 구현하는 것처럼 유사한 결과들을 초래하는, 리소스 콘텐츠에 대한 액세스 없이, 일부 기능들, 암호문의 검색 또는 산술적 조작을 여전히 구현할 수도 있다. 달리 말하면, 비-소유자 요청 엔터티들은 리소스 콘텐츠를 판독, 기입, 조작, 또는 해석하는 것이 가능하지 않으면서도 어떤 기능들을 구현할 수도 있고, 하지만, 리소스 콘텐츠를 판독, 기입, 조작, 또는 해석하는 것이 가능한 것과 유사한 겨과들을 여전히 생성할 수도 있다.

[0092] 비-소유자 요청 엔터티가 기능에 대한 인증서와 연관되지 않는다고 결정하는 것에 응답하여 (즉, 결정 블록 (802) = "아니오"), 또는, 리소스 콘텐츠에 대한 액세스가 전체적으로 가려지는 것으로서 지정된다고 결정하는 것에 응답하여 (결정 블록 (804) = "전체적으로"), 컴퓨팅 디바이스는 본원에서 추가적으로 설명되는 바와 같이 블록 (808) 에서 리소스 콘텐츠의 가상 뷰를 가림/암호화할 수도 있다. 프로세서, 데이터 보호 시스템 및/또는 리소스 콘텐츠 암호화 디바이스를 포함하는 컴퓨팅 디바이스의 컴포넌트들은 리소스 콘텐츠의 보기, 사용, 또는 조작을 방지하도록 구성된 강력한 암호화를 이용하여 리소스 콘텐츠의 가상 뷰를 가림/암호화할 수도 있다. 본원에서 논의된 바와 같이, 비-소유자 요청 엔터티들은, 리소스 콘텐츠에 대한 액세스 없이, 하지만 리소스 콘텐츠를 갖는 데이터의 불명료한 블록에 대한 액세스를 가지고, 관리상의 기능들과 같은 일부 기능들을 여전히 구현할 수도 있다. 달리 말하면, 비-소유자 요청 엔터티들은 리소스 콘텐츠를 판독, 기입, 조작, 또는 해석하는 것이 가능하지 않으면서도 어떤 기능들을 구현할 수도 있다.

[0093] 컴퓨팅 디바이스는 도 6 을 참조하여 설명된 바와 같이 블록 (616) 에서 요청 엔터티에 대해 리소스 콘텐츠의 가려진/암호화된 가상 뷰를 제공할 수도 있다.

[0094] 다양한 실시형태들 (도 1 내지 도 8 을 참조하여 상기 논의된 실시형태들을 포함하지만, 이들에 제한되지는 않음) 은 도 9 에서 예시된 다양한 실시형태들에의 이용에 적합한 일 예의 모바일 컴퓨팅 디바이스를 포함할 수도 있는 매우 다양한 컴퓨팅 디바이스들에서 구현될 수도 있다. 모바일 컴퓨팅 디바이스 (900) 는 내부 메모리 (906) 에 커플링된 프로세서 (902) 를 포함할 수도 있다. 프로세서 (902) 는 일반적인 또는 특정 프로세싱 태스크들을 위해 지정된 하나 이상의 멀티-코어 집적 회로들일 수도 있다. 내부 메모리 (906) 는 휘발성 또는 비휘발성 메모리일 수도 있고, 또한 보안 및/또는 암호화된 메모리, 또는 비보안 및/또는 비암호화된 메모리, 또는 그 임의의 조합일 수도 있다. 레버리징될 수 있는 메모리 타입들의 예들은 DDR, LPDDR, GDDR, WIDEIO, RAM, SRAM, DRAM, P-RAM, R-RAM, M-RAM, STT-RAM, 및 임베디드 동적 랜덤 액세스 메모리 (DRAM) 를 포함하지만 이들에 제한되지는 않는다.

[0095] 프로세서 (902) 는 터치 스크린 능력을 가질 수도 있거나 가지지 못할 수도 있는 모바일 컴퓨팅 디바이스의 디스플레이 (912) 에 커플링될 수도 있다. 일부 구현들에서, 디스플레이 (912) 는 저항성-감지 터치스크린, 용량성-감지 터치스크린, 적외선 감지 터치스크린 등과 같은 터치스크린 패널 (912) 일 수도 있다. 터치스크린 디스플레이 (912) 는 터치스크린 제어기 (904) 및 프로세서 (902) 에 커플링될 수도 있다.

[0096] 모바일 컴퓨팅 디바이스 (900) 는 하나 이상의 무선 신호 트랜시버들 (908) (예를 들어, Peanut, Bluetooth, Zigbee, Wi-Fi, RF 라디오) 및 서로에 및/또는 프로세서 (902) 에 커플링된, 통신물들을 전송 및 수신하기 위한, 안테나 (910) 를 가질 수도 있다. 트랜시버들 (908) 및 안테나 (910) 는 다양한 무선 송신 프로토콜 스택들 및 인터페이스들을 구현하기 위해 상기 언급된 회로부와 함께 이용될 수도 있다. 모바일 컴퓨팅 디바이스 (900) 는 셀룰러 네트워크를 통한 통신을 가능하게 하고 프로세서에 커플링되는 셀룰러 네트워크 무선 모뎀 칩 (916) 을 포함할 수도 있다.

[0097] 모바일 컴퓨팅 디바이스 (900) 는 프로세서 (902) 에 커플링된 주변 디바이스 접속 인터페이스 (918) 를 포함할 수도 있다. 주변 디바이스 접속 인터페이스 (918) 는 하나의 타입의 접속을 수락하도록 단독으로 구성될 수도 있거나, 또는 USB, FireWire, Thunderbolt, 또는 PCIe 와 같은, 공통 또는 독점적인, 다양한 타입들의 물리 및 통신 접속들을 수락하도록 구성될 수도 있다. 주변 디바이스 접속 인터페이스 (918) 는 또한 유사하게 구성된 주변 디바이스 접속 포트 (미도시) 에 커플링될 수도 있다.

[0098] 모바일 컴퓨팅 디바이스 (900) 는 또한 오디오 출력들을 제공하기 위한 스피커 (914) 를 포함할 수도 있다. 모바일 컴퓨팅 디바이스 (900) 는 또한, 본 명세서에서 논의된 컴포넌트들의 전부 또는 일부를 포함하기 위해, 플라스틱, 금속, 또는 재료들의 조합으로 구성된, 하우징 (920) 을 포함할 수도 있다. 모바일 컴퓨팅 디바이스 (900) 는 일회용 또는 재충전가능한 배터리와 같은, 프로세서 (902) 에 커플링된 전력 소스 (power source) (922) 를 포함할 수도 있다. 재충전가능한 배터리는 또한 모바일 컴퓨팅 디바이스 (900) 의 외부의 소스로부터 충전 전류를 수신하기 위해 주변 디바이스 접속 포트에 커플링될 수도 있다. 모바일 컴퓨팅 디바이스 (900) 는 또한 사용자 입력들을 수신하기 위한 물리적 버튼 (924) 을 포함할 수도 있다. 모바일 컴퓨팅 디바이스 (900) 는 또한 모바일 컴퓨팅 디바이스 (900) 를 턴 온 및 턴 오프하기 위한 전력 버튼 (926) 을 포함할 수도 있다.

[0099] 다양한 실시형태들 (도 1 내지 도 8 을 참조하여 상기 논의된 실시형태들을 포함하지만 이들에 제한되지는 않음) 은 도 10 에 예시된 랩톱 컴퓨터 (1000) 와 같은 다양한 모바일 컴퓨팅 디바이스들을 포함할 수도 있는, 매우 다양한 컴퓨팅 시스템들에서 구현될 수도 있다. 많은 랩톱 컴퓨터들은 컴퓨터의 포인팅 디바이스로서 기능하고, 따라서 상기 설명되고 터치 스크린 디스플레이를 갖춘 컴퓨팅 디바이스들 상에서 구현된 것들과 유사한 드래그, 스크롤, 및 플릭 제스처들을 수신할 수도 있는 터치패드 터치 표면 (1017) 을 포함한다. 랩톱 컴퓨터 (1000) 는 통상적으로 휘발성 메모리 (1012) 및 대용량 비휘발성 메모리, 이를 테면 플래시 메모리의 디스크 드라이브 (1013) 에 커플링된 프로세서 (1011) 를 포함할 것이다. 추가적으로, 컴퓨터 (1000) 는 무선 데이터 링크에 접속될 수도 있는 전자기 방사선을 전송 및 수신하기 위한 하나 이상의 안테나 (1008) 및/또는 프로세서 (1011) 에 커플링된 셀룰러 전화기 트랜시버 (1016) 를 가질 수도 있다. 컴퓨터 (1000) 는 또한 프로세서 (1011) 에 커플링된 플로피 디스크 드라이브 (1014) 및 콤팩트 디스크 (CD) 드라이브 (1015) 를 포함할 수도 있다. 노트북 구성에서, 컴퓨터 하우징은 모두가 프로세서 (1011) 에 커플링되는 터치패드 (1017), 키보드 (1018), 및 디스플레이 (1019) 를 포함한다. 컴퓨팅 디바이스의 다른 구성들은 잘 알려진 바와 같이 프로세서에 (예를 들어,범용 직렬 버스 (USB) 입력을 통해) 커플링된 컴퓨터 마우스 또는 트랙볼을 포함할 수도 있으며, 이는 또한 다양한 실시형태들과 함께 이용될 수도 있다.

[0100] 다양한 실시형태들 (도 1 내지 도 8 을 참조하여 상기 논의된 실시형태들을 포함하지만 이들에 제한되지는

않음) 은 서버들과 같은 다양한 상업적으로 이용가능한 컴퓨팅 디바이스들 중 임의의 것을 포함할 수도 있는 매우 다양한 컴퓨팅 디바이스들에서 구현될 수도 있다. 일 예의 서버 (1100) 가 도 11 에 예시된다. 이러한 서버 (1100) 는 통상적으로 휘발성 메모리 (1102) 및 디스크 드라이브 (1104) 와 같은 대용량 비휘발성 메모리에 커플링된 하나 이상의 멀티-코어 프로세서 어셈블리들 (1101) 을 포함한다. 도 11 에 예시한 바와 같이, 멀티-코어 프로세서 어셈블리들 (1101) 은 그들을 어셈블리의 랙들에 삽입함으로써 서버 (1100) 에 부가될 수도 있다. 서버 (1100) 는 또한, 프로세서 (1101) 에 커플링된 플로피 디스크 드라이브, 콤팩트 디스크 (CD) 또는 DVD 디스크 드라이브 (1106) 를 포함할 수도 있다. 서버 (1100) 는 또한, 다른 브로드캐스트 시스템 컴퓨터들 및 서버들에 커플링된 로컬 영역 네트워크, 인터넷, 공중 교환 전화 네트워크, 및/또는 셀룰러 데이터 네트워크 (예를 들어, CDMA, TDMA, GSM, PCS, 3G, 4G, LTE, 또는 임의의 다른 타입의 셀룰러 데이터 네트워크) 와 같은, 네트워크 (1105) 와 네트워크 인터페이스 접속들을 확립하기 위해 멀티-코어 프로세서 어셈블리들 (1101) 에 커플링된 네트워크 액세스 포트들 (1103) 을 포함할 수도 있다.

[0101] 다양한 실시형태들의 동작들을 수행하기 위한 프로그래밍가능 프로세서 상에서의 실행을 위한 컴퓨터 프로그램 코드 또는 "프로그램 코드" 는 C, C++, C#, Smalltalk, Java, JavaScript, Visual Basic, 구조화 질의 언어 (예를 들어, Transact-SQL), Perl 과 같은 하이 레벨 프로그래밍 언어로, 또는 다양한 다른 프로그래밍 언어들로 기록될 수도 있다. 본 출원에서 사용되는 바와 같은 컴퓨터 판독가능 저장 매체 상에 저장된 프로그램 코드 또는 프로그램들은 포맷이 프로세서에 의해 이해가능한 머신 언어 코드 (이를 테면 오브젝트 코드) 를 지칭할 수도 있다.

[0102] 전술한 방법 설명들 및 프로세스 흐름도들은 예시적인 예들로서 단순히 제공될 뿐이며 다양한 실시형태들의 동작들이 제시된 순서로 수행되어야 한다는 것을 요구하거나 또는 의미하도록 의도되지 않는다. 당업자에 의해 인식될 바와 같이, 전술한 실시형태들에서의 동작들의 순서는 임의의 순서로 수행될 수도 있다. "그 후에", "그 후", "다음에" 등과 같은 단어들은 동작들의 순서를 제한하도록 의도되지 않는다; 이들 단어들은 방법들의 설명을 통하여 독자를 안내하는데 단순히 사용된다. 게다가, 관사들 "a", "an" 또는 "the" 를 이용한, 단수로의 청구항 엘리먼트들에 대한 어떤 언급도 그 엘리먼트를 단수로 제한하는 것으로서 해석되지 않는다.

[0103] 다양한 실시형태들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 동작들은 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양자의 조합들로서 구현될 수도 있다. 하드웨어와 소프트웨어의 이 상호교환가능성을 명확히 예시하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 동작들은 일반적으로 그들의 기능성의 관점에서 상기 설명되었다. 이러한 기능성이 하드웨어로서 구현되는지 소프트웨어로서 구현되는지는 전체 시스템에 부과된 설계 제약들 및 특정한 애플리케이션에 의존한다. 당업자들은 각각의 특정한 애플리케이션에 대해 다양한 방식들로 설명된 기능성을 구현할 수도 있지만, 이러한 구현 판정들은 청구항들의 범위로부터 벗어남을 야기하는 것으로 해석되어서는 안된다.

[0104] 본 명세서에서 개시된 실시형태들과 관련하여 설명된 다양한 예시적인 로직들, 논리 블록들, 모듈들, 및 회로들을 구현하는데 이용되는 하드웨어는 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적 회로 (ASIC), 필드 프로그래밍가능 게이트 어레이 (FPGA) 또는 다른 프로그래밍가능 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 그 임의의 조합으로 구현 또는 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수도 있다. 대안적으로, 일부 동작들 또는 방법들은 주어진 기능에 특정적인 회로부에 의해 수행될 수도 있다.

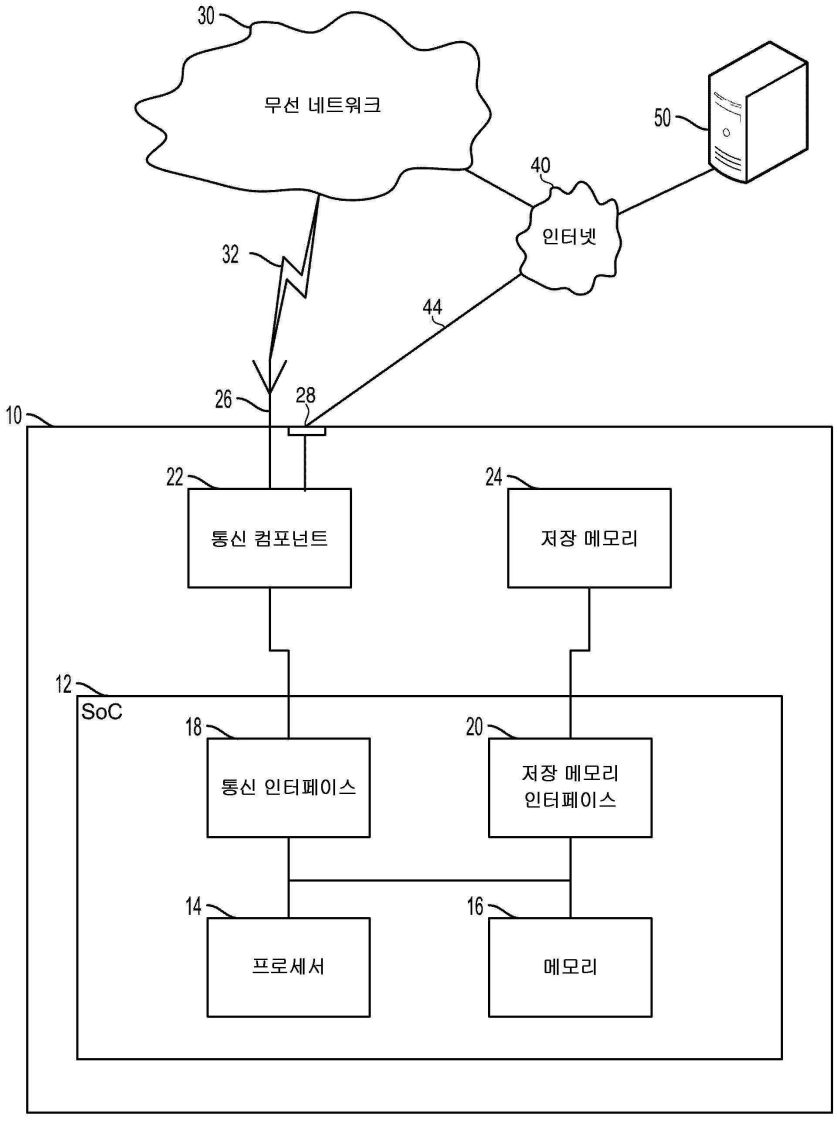
[0105] 하나 이상의 실시형태들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 그 임의의 조합으로 구현될 수도 있다. 소프트웨어로 구현되면, 기능들은 비일시적 컴퓨터 판독가능 매체 또는 비일시적 프로세서 판독가능 매체 상에 하나 이상의 명령들 또는 코드로서 저장될 수도 있다. 본 명세서에서 개시된 방법 또는 알고리즘의 동작들은 비일시적 컴퓨터 판독가능 또는 프로세서 판독가능 저장 매체 상에 상주할 수도 있는 프로세서 실행가능 소프트웨어 모듈로 구현될 수도 있다. 비일시적 컴퓨터 판독가능 또는 프로세서 판독가능 저장 매체들은 컴퓨터 또는 프로세서에 의해 액세스될 수도 있는 임의의 저장 매체들일 수도 있다. 제한이 아닌 일 예로, 이러한 비일시적 컴퓨터 판독가능 또는 프로세서 판독가능 매체들은 RAM, ROM, EEPROM, FLASH 메모리, CD-ROM 또는 다른 광 디스크 스토리지, 자기 디스크 스토리지 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 저장하는데 이용될 수도 있거나 또는 컴퓨터에 의해 액세스될 수도 있는 임의의 다른 매체를 포함할 수도 있다. 디스크 (disk) 및 디스크 (disc) 는 본 명세서에서 사

용한 바와 같이, 콤팩트 디스크 (CD), 레이저 디스크, 광 디스크, 디지털 다기능 디스크 (DVD), 플로피 디스크, 및 블루-레이 디스크를 포함하고, 여기서 디스크 (disk) 들은 보통 데이터를 자기적으로 재생하는 한편, 디스크 (disc) 들은 레이저들로 데이터를 광학적으로 재생한다. 상기의 조합들이 또한 비일시적 컴퓨터 판독가능 및 프로세서 판독가능 매체들의 범위 내에 포함된다. 추가적으로, 방법 또는 알고리즘의 동작들은, 컴퓨터 프로그램 제품에 통합될 수도 있는, 비일시적 프로세서 판독가능 매체 및/또는 컴퓨터 판독가능 매체 상에 코드들 및/또는 명령들 중 하나 또는 임의의 조합 또는 세트로서 상주할 수도 있다.

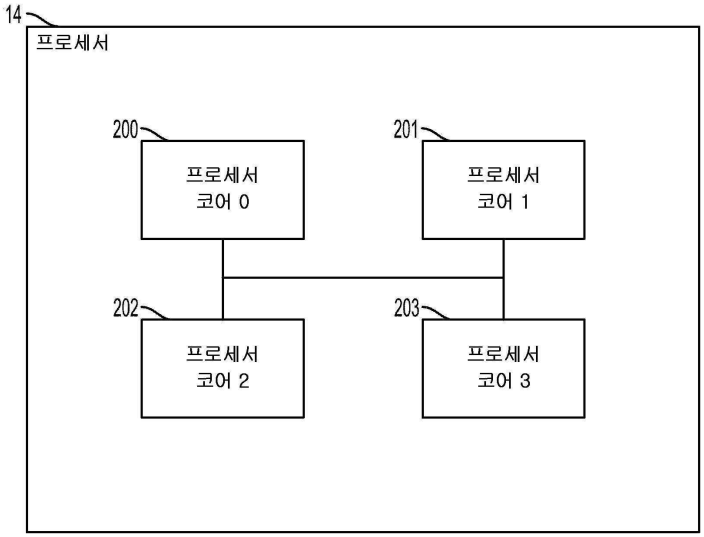
[0106] 개시된 실시형태들의 전술한 설명은 임의의 당업자가 청구항들을 제조 또는 이용하는 것을 가능하게 하기 위해 제공된다. 이들 실시형태들에 대한 다양한 변경들은 당업자들에게 용이하게 명백할 것이며, 본 명세서에서 정의된 일반적인 원리들은 청구항들의 범위로부터 벗어남 없이 다른 실시형태들에 적용될 수도 있다. 따라서, 본 개시는 본 명세서에서 도시된 실시형태들에 제한되는 것으로 의도되지 않고 다음의 청구항들 및 본 명세서에서 개시된 원리들 및 신규한 피처들에 부합하는 최광의 범위를 부여받게 하려는 것이다.

도면

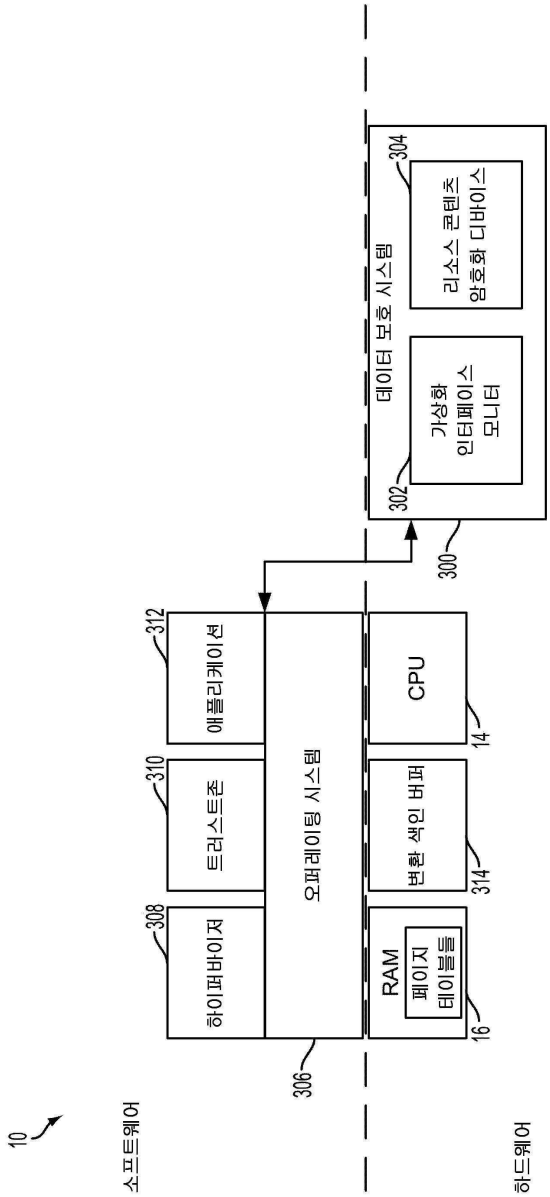
도면1



도면2



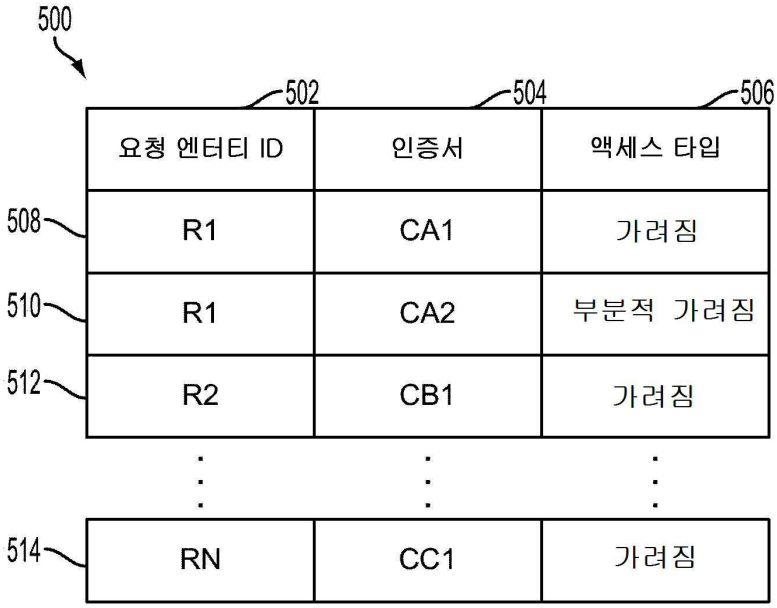
도면3


데이터 보호 시스템
304
리소스 콘텐츠 암호화 디바이스
302
가상화 인터페이스 모니터
300
312
애플리케이션
310
트러스트존
308
하이퍼바이저
306
오퍼레이팅 시스템
CPU
14
변환 색인 버퍼
314
RAM
페이지 테이블들
16
10
소프트웨어
하드웨어

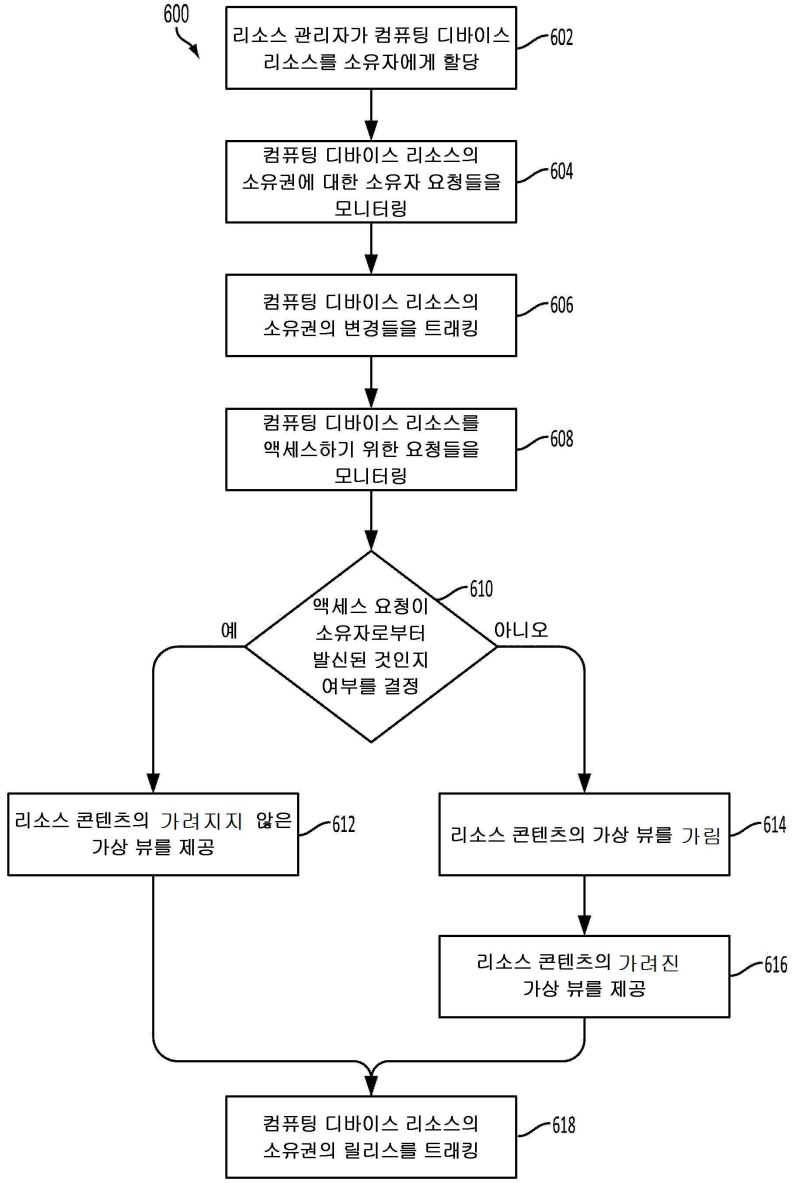
도면4


400
402
404
406
소유자 ID
가상 어드레스
유효성
408
O1
VA1
1
410
O1
VA2
1
412
O2
VB1
0
414
ON
VC1
1

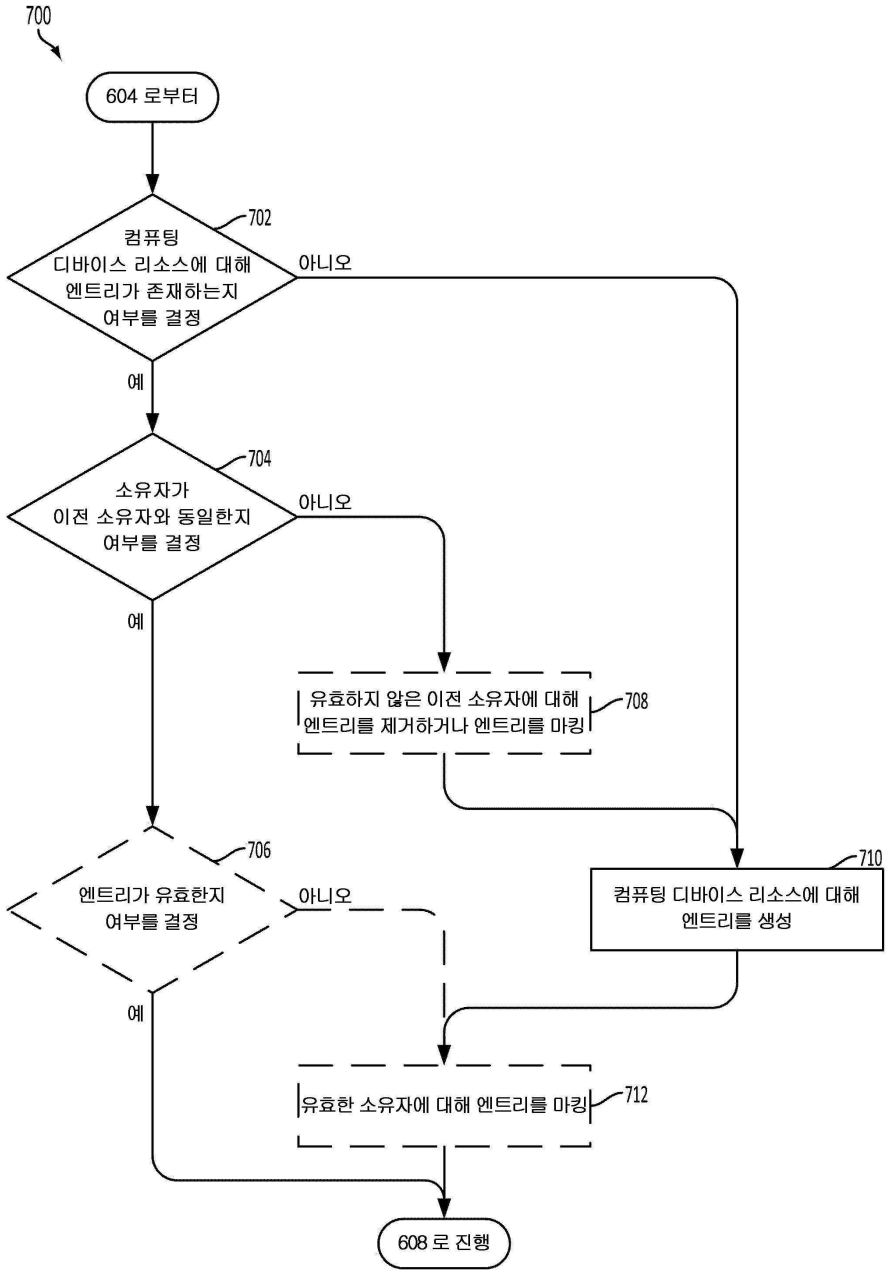
도면5


500
502
504
506
요청 엔터티 ID
인증서
액세스 타입
508
R1
CA1
가려짐
510
R1
CA2
부분적 가려짐
512
R2
CB1
가려짐
514
RN
CC1
가려짐

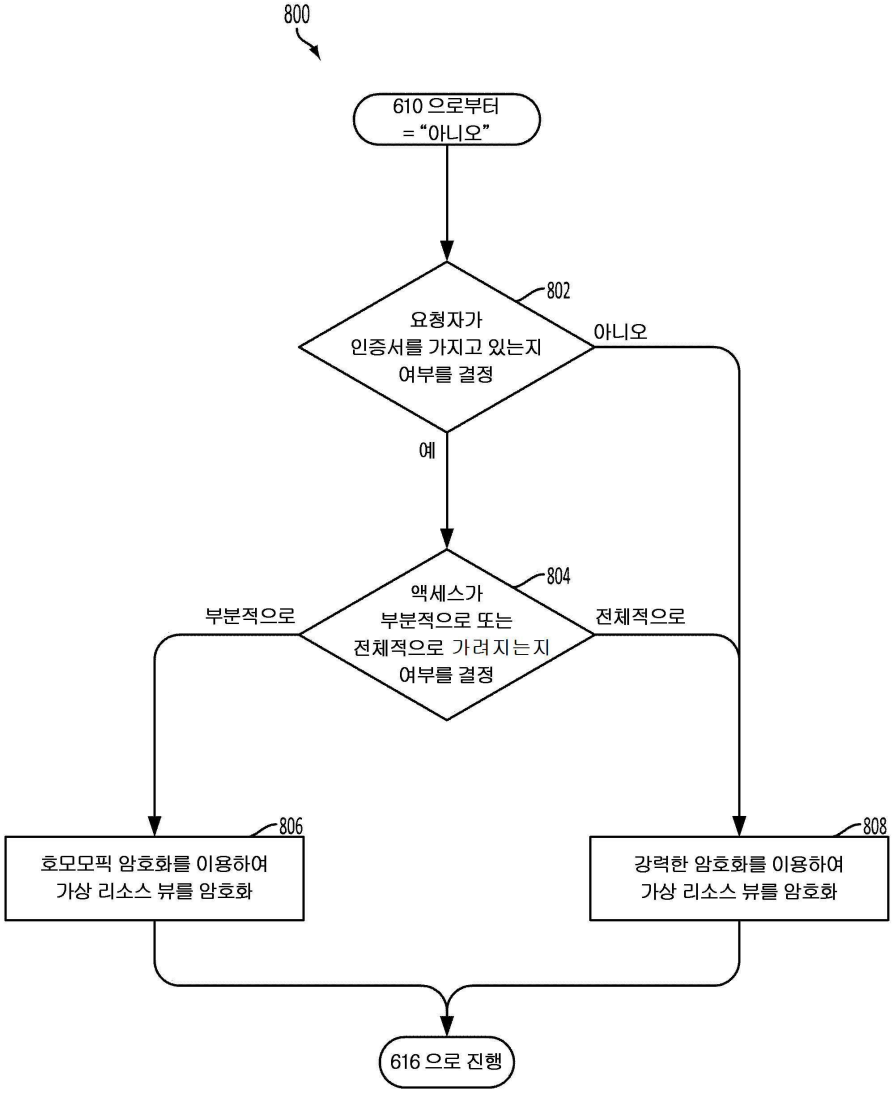
도면6


600
리소스 관리자가 컴퓨팅 디바이스 리소스를 소유자에게 할당
602
컴퓨팅 디바이스 리소스의 소유권에 대한 소유자 요청들을 모니터링
604
컴퓨팅 디바이스 리소스의 소유권의 변경들을 트래킹
606
컴퓨팅 디바이스 리소스를 액세스하기 위한 요청들을 모니터링
608
액세스 요청이 소유자로부터 발신된 것인지 여부를 결정
610
예
아니오
리소스 콘텐츠의 가려지지 않은 가상 뷰를 제공
612
리소스 콘텐츠의 가상 뷰를 가림
614
리소스 콘텐츠의 가려진 가상 뷰를 제공
616
컴퓨팅 디바이스 리소스의 소유권의 릴리스를 트래킹
618

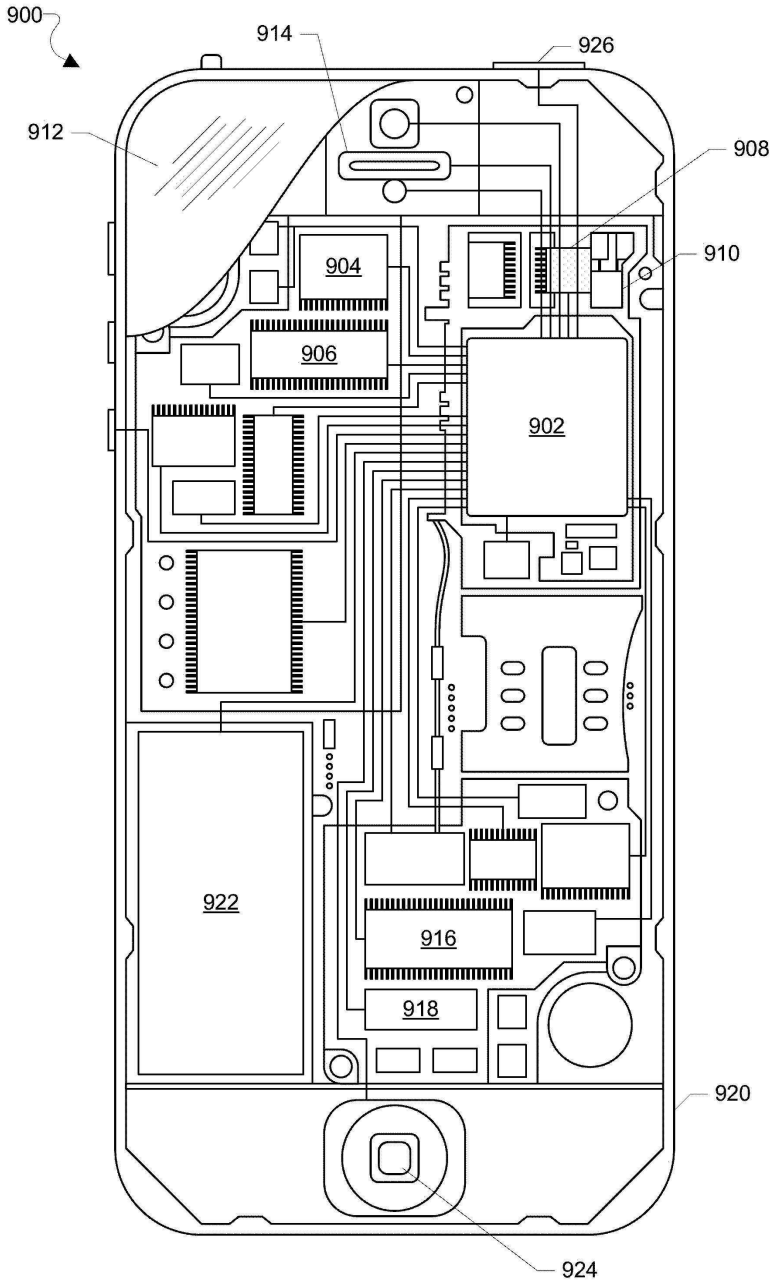
도면7


700
604 로부터
702
컴퓨팅 디바이스 리소스에 대해 엔트리가 존재하는지 여부를 결정
아니오
예
704
소유자가 이전 소유자와 동일한지 여부를 결정
아니오
예
708
유효하지 않은 이전 소유자에 대해 엔트리를 제거하거나 엔트리를 마킹
706
엔트리가 유효한지 여부를 결정
아니오
예
710
컴퓨팅 디바이스 리소스에 대해 엔트리를 생성
712
유효한 소유자에 대해 엔트리를 마킹
608 로 진행

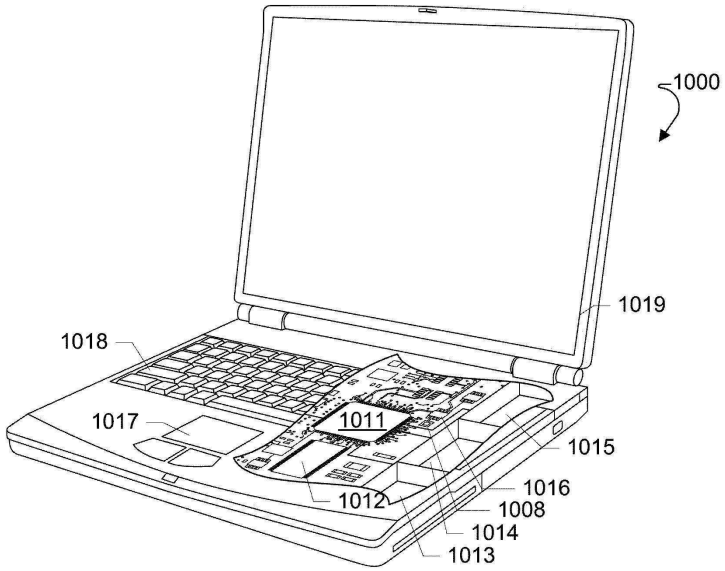
도면8


800
610 으로부터
= "아니오"
802
요청자가
인증서를 가지고 있는지
여부를 결정
아니오
예
804
액세스가
부분적으로 또는
전체적으로 가려지는지
여부를 결정
부분적으로
전체적으로
806
호모모픽 암호화를 이용하여
가상 리소스 뷰를 암호화
808
강력한 암호화를 이용하여
가상 리소스 뷰를 암호화
616 으로 진행

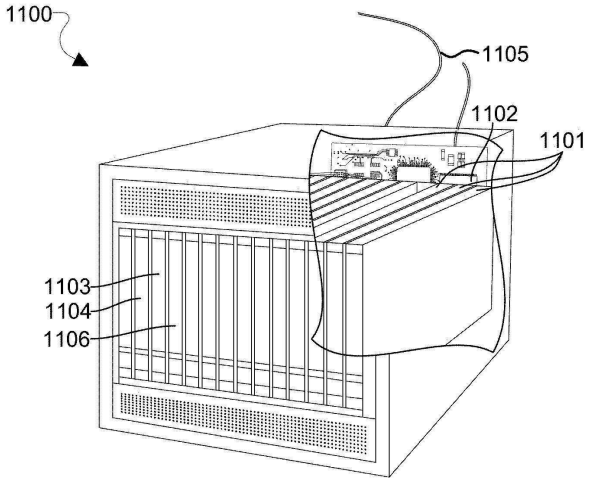
도면9



도면10


1000
1019
1018
1017
1011
1015
1016
1012
1008
1014
1013

도면11


1100
1105
1102
1101
1103
1104
1106