(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년02월10일
(11) 등록번호 10-2361884
(24) 등록일자 2022년02월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/74 (2013.01) *G06F 12/14* (2006.01)
H04L 9/06 (2006.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
G06F 21/74 (2013.01)
G06F 12/1408 (2013.01)
(21) 출원번호 10-2018-7033884
(22) 출원일자(국제) 2017년05월18일
심사청구일자 2020년04월17일
(85) 번역문제출일자 2018년11월22일
(65) 공개번호 10-2019-0009755
(43) 공개일자 2019년01월29일
(86) 국제출원번호 PCT/US2017/033198
(87) 국제공개번호 WO 2017/205155
국제공개일자 2017년11월30일
(30) 우선권주장
15/163,443 2016년05월24일 미국(US)
(56) 선행기술조사문헌
VICTOR COSTAN et al, "Intel SGX Explained", international association for cryptologic research, 2016.01.31.
WO2015094261 A1
US20120159184 A1

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
첸 링 토니
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 어텐션: 페이턴트 그룹 도켓팅 (빌딩 8/1000) 마이크로소프트 테크놀로지 라이센싱, 엘엘씨
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 15 항 심사관 : 구대성

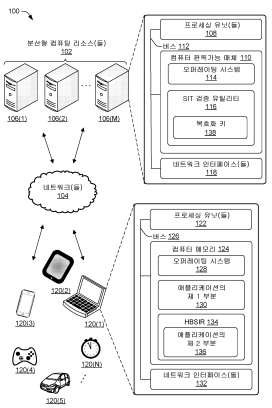
(54) 발명의 명칭 **전자 장치의 불법 복제 및 불법 행위 방지에 하드웨어 기반 보안 격리 영역의 사용**

(57) 요 약

전자 장치 상에서의 불법 복제 및 불법 행위를 방지하는 데 보안 격리 기술을 사용하는 시스템 및 방법. 일부 예에서, 전자 장치는 하드웨어 기반 보안 격리 기술을 사용하여, 컴퓨터 메모리에 애플리케이션의 제 1 부분을 저장하고 또한 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 애플리케이션의 제 2 부분을 저장할 수 있으며,

(뒷면에 계속)

대 표 도 - 도1



상기 애플리케이션의 제 2 부분은 암호화 부분 및 평문 부분을 포함한다. 또한, 전자 장치는 하드웨어 기반 보안 격리 기술을 사용하여, 서버와 보안 암호화 통신 채널을 수립하고, 보안 암호화 통신 채널을 거쳐서 서버로 데이터를 전송하고, 보안 암호화 통신 채널을 거쳐서 서버로부터 복호화 키를 수신하고, 복호화 키를 사용하여 암호화 부분을 복호화할 수 있다. 그 후에 전자 장치는 애플리케이션의 제 1 부분 및 애플리케이션의 제 2 부분을 사용하여 애플리케이션을 실행할 수 있다.

(52) CPC특허분류
H04L 63/0428 (2013.01)
H04L 63/061 (2013.01)
H04L 63/0853 (2013.01)
H04L 9/0618 (2013.01)

명 세 서

청구범위

청구항 1

불법 복제 및 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하는 방법으로서,

전자 장치의 컴퓨터 메모리에 애플리케이션의 제 1 부분을 저장하는 단계 - 상기 애플리케이션은 상기 애플리케이션의 실행에 필요한 제 2 부분을 더 포함함 - 와,

상기 전자 장치의 상기 컴퓨터 메모리의 보안 격리 영역(a secure isolated region)에 상기 애플리케이션의 제 2 부분을 저장하는 단계 - 상기 애플리케이션의 제 2 부분은 암호화 부분 및 평문 부분을 포함하고, 상기 암호화 부분은 상기 암호화 부분이 복호화될 때까지 상기 애플리케이션의 제 1 부분 및 제 2 부분이 기능하는 것을 방지함 - 와,

상기 평문 부분을 사용하여, 서버와 보안 암호화 통신 채널을 수립하는 단계와,

상기 보안 암호화 통신 채널을 사용하여, 상기 서버로 데이터를 전송하는 단계와,

상기 데이터의 전송에 적어도 부분적으로 기초하여, 상기 보안 암호화 통신 채널을 사용하여, 상기 서버로부터 복호화 키를 수신하는 단계와,

상기 복호화 키를 사용하여 상기 암호화 부분을 복호화하는 단계와,

상기 암호화 부분을 복호화하는 것에 응답하여 상기 전자 장치의 상기 컴퓨터 메모리로부터 상기 애플리케이션의 제 1 부분 및 상기 컴퓨터 메모리의 상기 보안 격리 영역으로부터 상기 애플리케이션의 제 2 부분의 상기 암호화 부분 및 상기 평문 부분 모두를 실행하는 단계를 포함하는

방법.

청구항 2

제 1 항에 있어서,

상기 데이터는 상기 전자 장치가 신뢰되는 CPU 칩 및 상기 보안 격리 영역을 포함하고 있는지를 상기 서버에게 검증하도록 하게 하는 입증 정보(attestation information)를 포함하는

방법.

청구항 3

제 2 항에 있어서,

상기 입증 정보는 상기 CPU 칩에 대한 식별자, 상기 전자 장치가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실행되고 있다는 증거, 또는 상기 보안 격리 영역의 다이제스트(digest) 중 적어도 하나를 포함하는

방법.

청구항 4

제 1 항에 있어서,

상기 보안 격리 영역을 사용하여, 실링 키(sealing key)를 생성하는 단계와,

상기 실링 키를 사용하여 상기 복호화 키를 암호화하는 단계를 더 포함하는

방법.

청구항 5

제 4 항에 있어서,

상기 암호화된 복호화 키를 비휘발성 메모리에 저장하는 단계를 더 포함하는

방법.

청구항 6

제 1 항에 있어서,

상기 평문 부분은 상기 서버로부터 상기 복호화 키를 불러오기 위한 라이센싱 코드를 포함하는

방법.

청구항 7

제 1 항에 있어서,

상기 암호화 부분은 상기 애플리케이션의 사용에 중요한 코드를 포함하는

방법.

청구항 8

제 1 항에 있어서,

상기 서버로부터, 상기 보안 격리 영역이 종료되어야 하는지를 결정하기 위해 상기 보안 격리 영역으로 하여금 상기 서버와 주기적으로 통신하게 하는 인스트럭션을 수신하는 단계를 더 포함하는

방법.

청구항 9

제 1 항에 있어서,

상기 애플리케이션의 제 1 부분은 상기 전자 장치의 상기 컴퓨터 메모리로부터 상기 애플리케이션의 제 1 부분 및 상기 컴퓨터 메모리의 상기 보안 격리 영역으로부터 상기 애플리케이션의 제 2 부분의 상기 암호화 부분 및 상기 평문 부분 모두를 실행하는 동안 상기 보안 격리 영역 내의 상기 애플리케이션의 제 2 부분을 호출하는

방법.

청구항 10

불법 복제 및 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하도록 구성된 전자 장치로서,

적어도 하나의 프로세서 및 메모리를 구비하되,

상기 메모리는,

애플리케이션의 제 1 부분 - 상기 애플리케이션은 상기 애플리케이션의 실행에 필요한 제 2 부분을 더 포함함 - 과,

상기 메모리의 보안 격리 영역 내의 상기 애플리케이션의 제 2 부분

을 저장하되,

상기 제 2 부분은 추출로부터 상기 애플리케이션을 보안화하기 위한 암호화 부분 및 서버와의 통신 채널을 오픈하기 위한 평문 부분을 포함하고, 상기 암호화 부분은 상기 암호화 부분이 복호화될 때까지 상기 애플리케이션의 제 1 부분 및 제 2 부분이 기능하는 것을 방지하며,

상기 평문 부분은, 상기 적어도 하나의 프로세서에 의한 실행시에, 상기 적어도 하나의 프로세서로 하여금,

상기 서버와 상기 통신 채널을 수립하고,

상기 통신 채널을 거쳐서 상기 서버로부터 상기 애플리케이션과 연관된 복호화 키를 수신하며,

상기 복호화 키를 사용하여 상기 암호화 부분을 복호화하고,

상기 암호화 부분을 복호화하는 것에 응답하여 상기 전자 장치의 상기 메모리로부터 상기 애플리케이션의 제 1 부분 및 상기 메모리의 상기 보안 격리 영역으로부터 상기 애플리케이션의 제 2 부분의 상기 암호화 부분 및 상기 평문 부분 모두를 실행

하도록 하게 하는 컴퓨터 판독가능 인스트럭션을 포함하는

전자 장치.

청구항 11

제 10 항에 있어서,

상기 보안 격리 영역은, 상기 적어도 하나의 프로세서에 의한 실행시에, 상기 적어도 하나의 프로세서로 하여금, 상기 통신 채널을 거쳐서 상기 서버로 데이터를 전송하게 하는 컴퓨터 판독가능 인스트럭션을 포함하고, 상기 데이터는 상기 전자 장치가 보안 격리 기술을 포함하는지를 상기 서버에게 검증하도록 하게 하는 입증 정보를 포함하는

전자 장치.

청구항 12

제 11 항에 있어서,

상기 입증 정보는 상기 적어도 하나의 프로세서에 대한 식별자, 상기 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실행되고 있다는 증거, 및 상기 보안 격리 영역의 다이제스트 중 적어도 하나를 포함하는

전자 장치.

청구항 13

제 10 항에 있어서,

상기 컴퓨터 판독가능 인스트럭션은 또한, 상기 적어도 하나의 프로세서에 의한 실행시에, 상기 적어도 하나의 프로세서로 하여금, 상기 보안 격리 영역에 의해 생성된 실링 키를 사용하여 상기 복호화 키를 암호화하도록 하게 하는

전자 장치.

청구항 14

제 13 항에 있어서,

상기 컴퓨터 판독가능 인스트럭션은 또한, 상기 적어도 하나의 프로세서에 의한 실행시에, 상기 적어도 하나의 프로세서로 하여금, 상기 암호화된 복호화 키를 비휘발성 메모리에 저장하도록 하게 하는

전자 장치.

청구항 15

제 10 항에 있어서,

상기 컴퓨터 판독가능 인스트럭션은 또한, 상기 적어도 하나의 프로세서에 의한 실행시에, 상기 적어도 하나의 프로세서로 하여금,

상기 통신 채널을 거쳐서 상기 서버로부터, 상기 서버와 통신하기 위한 시간 간격을 포함하는 인스트럭션을 수신하도록 하게 하고,

상기 시간 간격에 적어도 일부분 기초하여, 상기 애플리케이션에 대한 라이센스가 여전히 유효한지를 결정하기 위해 상기 서버와 통신하도록 하게 하는

전자 장치.

발명의 설명

배 경 기 술

[0001] 전자 장치의 설계시, 개발자들은 악의적인 사용자들로부터 애플리케이션을 보호하는 전자 장치용 불법 복제 방지 수단(예를 들면, 소프트웨어 기술)을 생성하고자 한다. 그러나, 현재의 불법 복제 방지 수단이 존재하더라도, 악의적인 사용자들은 여전히 애플리케이션을 불법 복제하기 위해 전자 장치를 종종 조작할 수 있다. 통상적으로, 전자 장치의 악의적인 사용자는 전자 장치의 오퍼레이팅 시스템, 하이퍼바이저, 및/또는 펌웨어를 변경할 것이다. 변경된 전자 장치를 사용하면, 악의적인 사용자는 전자 장치 상에서 애플리케이션을 악의적으로 실행하는 데 필요한 애플리케이션에 대한 코드를 추출할 수 있다.

발명의 내용

과제의 해결 수단

[0002] 본 발명은 전자 장치의 불법 복제(piracy) 및 불법 행위(cheating)를 방지하기 위해 보안 격리 기술(secure isolated technology)을 사용하는 기법을 기재하고 있다. 일부 예에서, 전자 장치는 전자 장치의 프로세서가 보안 모드에서 동작 가능하게 하고, 및/또는 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역(a hardware based secure isolated region)에 데이터 및/또는 코드를 저장 가능하게 하는 보안 격리 기술을 포함한다. 예컨대, 전자 장치는 컴퓨터 메모리에 애플리케이션의 제 1 부분을 저장하고, 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 애플리케이션의 제 2 부분을 저장할 수 있다. 애플리케이션의 제 2 부분은 평문 부분 및 암호화 부분을 포함할 수 있다. 일부 예에서, 암호화 부분은 애플리케이션의 사용에 중요한 애플리케이션용 코드를 포함한다. 암호화 부분이 정확하게 복호화 및 실행되지 않으면, 애플리케이션은 올바르게 기능하는 데 제한을 받기 때문에 불법 복제가 금지된다.

[0003] 애플리케이션을 실행하기 위해, 전자 장치는 네트워크를 거쳐서 서버와 보안 암호화 통신 채널을 수립하는 데 애플리케이션의 평문 부분을 이용할 수 있다. 전자 장치는 보안 암호화 통신 채널을 거쳐서 서버로부터 복호화 키를 수신하고 또한 서버로 데이터를 전송하는 데 애플리케이션의 평문 부분을 이용할 수 있다. 일부 예에서, 데이터는 전자 장치 상의 CPU 칩에 대한 식별자, 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실제로 실행중이라는 증거, 및/또는 보안 격리 영역의 다이제스트(a digest) 등의 입증 정보(attestation information)를 포함한다. 그러면 전자 장치는 복호화 키를 사용하여 하드웨어 기반 보안 격리 영역 내에서 애플리케이션의 암호화 부분을 복호화할 수 있다. 복호화 후에, 전자 장치는 애플리케이션의 제 1 부분 및 애플리케이션의 제 2 부분을 사용하여 애플리케이션을 실행할 수 있다.

[0004] 프로세서가 보안 모드에서 실행 가능하게 하고, 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에서 코드를 실

행 가능하게 하는 보안 격리 기술을 사용함으로써, 전자 장치의 오퍼레이팅 시스템, 하이퍼바이저, 및/또는 펌웨어는 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서 데이터에 액세스하는 데 제한을 받는다. 이와 같이, 심지어 사용자가 전자 장치를 조작하고 있더라도, 하드웨어 기반 보안 격리 영역 내의 애플리케이션의 부분(예를 들면, 애플리케이션의 중요 코드)은 추출로부터 여전히 안전하다. 또한, 조작된 전자 장치를 사용하는 경우, 사용자는 하드웨어 기반 보안 격리 영역 내에 있는 애플리케이션의 부분을 변경하는 데 제한을 받는다. 따라서, 전자 장치의 사용자는 전자 장치가 애플리케이션을 실행하고 있는 동안에 애플리케이션의 불법 복제 및 불법 행위에 제한을 받는다.

[0005] 이 개요는 상세한 설명에서 이하에 추가로 설명되는 개념들의 모음을 단순화된 형태로 소개하기 위해 제공된 것이다. 이 개요는 청구대상의 핵심 또는 필수 특징들을 식별하기 위한 것이 아니며, 청구대상의 범위를 결정함에 있어서 도움을주기 위한 것도 아니다. 예를 들면, "기법들"의 용어는 상기한 문맥 및 문서 전반에 걸쳐서 허용되는 바와 같이 시스템(들), 방법(들), 컴퓨터 판독가능 인스트럭션, 모듈(들), 알고리즘, 하드웨어 로직, 및/또는 동작(들)을 지칭할 수 있다.

도면의 간단한 설명

[0006] 상세한 설명은 첨부 도면을 참조하여 설명된다. 도면에서, 참조 번호의 가장 왼쪽 번호(들)는 참조 번호가 처음 출현하는 도면을 식별한다. 상이한 도면에서의 동일한 참조 번호는 유사하거나 동일한 항목을 표시한다.

도 1은 전자 장치의 불법 행위 및 불법 복제를 방지하는 데 하드웨어 기반 보안 격리 기술을 사용하는 기법이 구동될 수 있는 예시적인 환경을 도시하는 블록도이다.

도 2는 불법 복제 및 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하도록 구성된 예시적인 클라이언트 컴퓨팅 장치를 도시하는 블록도이다.

도 3은 하드웨어 기반 보안 격리 기술을 이용하는 전자 장치 상에서 불법 복제 및 불법 행위를 방지하는 것과 연관된 기술을 수행하도록 구성된 예시적인 컴퓨팅 장치를 도시하는 블록도이다.

도 4는 애플리케이션의 불법 복제를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하는 전자 장치의 예시적인 방법의 흐름도이다.

도 5는 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서 애플리케이션의 부분을 실행하는 전자 장치의 예시적인 방법의 흐름도이다.

도 6은 복호화 키를 보안화하는 데 하드웨어 기반 보안 격리 기술을 이용하는 예시적인 방법의 흐름도이다.

도 7은 애플리케이션과 연관된 플로팅 권한(a floating right)을 이용하는 전자 장치의 예시적인 방법의 흐름도이다.

도 8은 전자 장치 상에서 하드웨어 기반 보안 격리 기술을 검증하는 서버의 제 1 예시적 방법의 흐름도이다.

도 9는 전자 장치 상에서 하드웨어 기반 보안 격리 기술을 검증하는 서버의 제 2 예시적 방법의 흐름도이다.

도 10은 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하는 제 1 예시적인 방법의 흐름도이다.

도 11은 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하는 제 2 예시적인 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0007] 본 명세서에서 설명되는 예들은 전자 장치의 불법 행위 및 불법 복제를 방지하는 데 보안 격리 기술을 이용하는 기술을 제공한다. 일부 예에서, 전자 장치는 전자 장치 상에서 데이터 및/또는 코드를 보호하는 하드웨어 기반 보안 격리 기술을 포함한다. 보안 격리 기술은 전자 장치의 프로세서가 보안 모드에서 동작 가능하게 하고, 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 데이터 및/또는 코드를 저장 가능하게 함으로써, 데이터 및/또는 코드를 보호한다. 일부 예에서, 전자 장치의 오퍼레이팅 시스템, 하이퍼바이저, 및/또는 펌웨어는 컴퓨터 메모리의 보안 격리 영역 내의 데이터 및/또는 코드에 액세스하는 데 제한을 받는다. 이와 같이, 심지어 사용자가 전자 장치(예를 들면, 전자 장치의 오퍼레이팅 시스템, 하이퍼바이저, 및/또는 펌웨어)를 조작한다고 하더라도, 하드웨어 기반 보안 격리 영역 내의 데이터 및/또는 코드는 추출 및 조작으로부터 여전히 안전하다. 하드웨어 기반 보안 격리 기술의 예는 인텔의 소프트웨어 가드 익스텐션(SGX; Software Guard Extensions)이지만, 이러한 기술은 또한 다른 하드웨어 제조업체로부터 나올 수 있다. 보안 격리 기술의 기능은 이하를 포함한다.

[0008] · OS 감독자 및 하이퍼바이저를 포함한 나머지 컴퓨터 시스템으로부터 하드웨어 기반 보안 격리 영역에서의 코드 및 데이터를 기밀로 유지할 수 있는 기능.

[0009] · 하드웨어 기반 보안 격리 영역을 갖는 머신에서 그 영역이 실제로 실행되고 있음을 하드웨어 기반 보안 격리 영역 내에서 서버에 대해 증명할 수 있는 기능.

[0010] · 현재 실행중인 하드웨어 기반 보안 격리 영역의 암호 다이제스트(cryptographic digest)/측정을 하드웨어 기반 보안 격리 영역 내에서 서버에 대해 입증할 수 있는 기능.

[0011] · 하드웨어 기반 보안 격리 기술을 갖고서 다른 전자 장치와 이 전자 장치를 고유하게 식별하는 고유 ID를 하드웨어 기반 보안 격리 영역 내에서 서버에 대해 입증할 수 있는 기능.

[0012] · 정확히 동일한 하드웨어 기반 보안 격리 영역이 정확히 동일한 하드웨어에서 다시 실행되고 있는 경우에만 재생성될 수 있는 실링 키(a sealing key)로서 사용될 수 있는 키를 하드웨어 기반 보안 격리 영역 내에서 생성할 수 있는 기능.

[0013] 일부 예에서, 전자 장치는 애플리케이션의 제 1 부분(예를 들면, 제 1 코드 부분)을 컴퓨터 메모리에 저장하고, 애플리케이션의 제 2 부분(예를 들면, 제 2 코드 부분)을 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 저장한다. 애플리케이션의 제 2 부분은 평문 부분 및 암호화 부분을 포함할 수 있다. 일부 예에서, 평문 부분은 전자 장치가 서버로부터 복호화 키를 불러오는 데 사용하는 코드를 포함할 수 있다. 예컨대, 평문 부분은 애플리케이션에 대한 라이센스 코드를 포함할 수 있다. 일부 예에서, 암호화 부분은 적절하게 실행하는 애플리케이션에 있어서 중요한 코드를 포함할 수 있다. 예컨대, 게임의 암호화 부분은 애플리케이션에 있어서 AI 휴리스틱, 3D 물리 계산, 커스텀 그래픽 프로세싱 유닛 커맨드 생성, 등을 위한 코드를 포함할 수 있다.

[0014] 일부 예에서, 애플리케이션을 실행하기 위해, 전자 장치는 서버(예를 들면, 라이센싱 서버)와 보안 암호화 통신 채널을 수립하는 데 평문 부분을 사용한다. 전자 장치는 보안 암호화 통신 채널을 통해서 서버로 데이터를 전송하는 데 평문 부분을 추가로 사용할 수 있다. 예컨대, 전자 장치는 특정 데이터(예를 들면, 입증 정보)를 서버로 전송함으로써 서버에 대해 입증할 수 있다. 일부 예에서, 데이터는 전자 장치의 CPU 칩의 식별자(예를 들면, CPU 칩 번호), 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치에서 실제로 실행되고 있다는 증거, 및/또는 하드웨어 기반 보안 격리 영역에서의 코드 및 데이터의 다이제스트를 포함할 수 있다. 이러한 예에서, 보안 격리 영역의 다이제스트는 평문 부분 및 암호화 부분의 양쪽을 포함할 수 있다. 데이터를 사용하는 경우, 서버는 하드웨어 기반 보안 격리 기술을 지원하는 전자 장치에서 하드웨어 기반 보안 격리 영역이 실행되고 있는지를 검증할 수 있다. 또한, 일부 예에서, 서버는 전자 장치 및/또는 전자 장치의 사용자가 애플리케이션에 대한 라이센스를 갖고 있는지를 지불 기록 데이터베이스를 찾아봄으로써 또한 검증할 수 있다. 애플리케이션의 라이센스가 적절히 부여된 경우, 서버는 보안 암호화 통신 채널을 통해 전자 장치로 복호화 키를 전송할 수 있다.

[0015] 일부 예에서, 전자 장치는 하드웨어 기반 보안 격리 영역 내에서 암호화 부분을 복호화하는 데 복호화 키를 사용한다. 복호화 후에, 전자 장치는 애플리케이션을 실행하는 데 제 1 부분, 평문 부분, 및 복호화 부분을 사용할 수 있다. 예컨대, 전자 장치는 컴퓨터 메모리에 저장된 애플리케이션의 제 1 부분을 실행하는 데 CPU를 사용할 수 있다. 전자 장치는 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에 저장된 평문 부분 및 복호화 부분을 실행하는 데 CPU를 추가로 사용할 수 있다.

[0016] 일부 예에서, 전자 장치가 애플리케이션의 실행을 종료하면, 하드웨어 기반 보안 격리 영역은 평문 부분이 복호화 키를 암호화하는 데 사용할 수 있는 실링 키를 생성할 수 있다. 전자 장치는 암호화된 복호화 키를 비휘발성 컴퓨터 판독가능 저장 매체에 저장할 수 있다. 이에 의해 복호화 키는 리부트 후에 복구될 수 있으므로, 복호화 키가 초기에 획득된 후에 애플리케이션이 오프라인(라이센싱 서버로의 액세스 없이)에서 사용할 수 있다. 일부 예에서, 정확히 동일한 실링 키는 정확히 동일한 전자 장치 상에서 다시 실행중인 정확히 동일한 하드웨어 기반 보안 격리 영역에 의해서만 복구될 수 있기 때문에, 다른 전자 장치들의 불법 복제가 방지된다.

[0017] 추가적으로 또는 이와는 달리, 개발자는 사용자가 부정행위를 행할 수 없는 하드웨어 기반 보안 격리 영역에 전자 장치가 코드를 저장하게 할 수 있다. 예컨대, 일부 예에서, 애플리케이션의 암호화 부분은 애플리케이션의 다른 부분들(예를 들면, 애플리케이션의 제 1 부분)이 적절하게 실행중이며 악의적으로 수정되지 않았다는 것을 확인하는 코드를 포함할 수 있다. 예컨대, 암호화 부분은 애플리케이션의 제 1 부분이 손상되지 않았음을 주기적으로 검사 및 확인하는 코드를 포함할 수 있다. 추가적으로 또는 이와는 달리, 일부 예에서, 암호화 부분은 부정행위를 위해 사용자가 조작하는 데이터를 포함할 수 있다. 예컨대, 애플리케이션이 각 플레이어의 건강 상

태를 포함하고 있는 비디오 게임을 포함하는 경우, 암호화 부분은 플레이어의 건강 상태를 계속해서 추적하는 가변 데이터를 포함할 수 있다. 이 건강 상태는 이제 하드웨어 기반 보안 격리 영역에 저장되기 때문에, 게임에서 부정행위를 하고자 하는 사용자에 의해 수정되는 것이 금지된다.

[0018] 다수의 예, 시나리오, 및 측면을 도 1-10을 참조하여 더 설명한다.

[0019] 실례로 되는 환경

[0020] 도 1은 전자 장치의 불법 복제 및 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 사용하는 기법이 구동될 수 있는 예시적인 환경(100)을 도시한다. 일부 예에서, 환경(100)의 다수의 장치 및/또는 구성요소는 하나 이상의 네트워크(104)를 거쳐서 상호 간에 또한 외부 장치와 통신할 수 있는 분산형 컴퓨팅 리소스(102)를 포함한다.

[0021] 네트워크(들)(104)는 예를 들어 인터넷과 같은 공중 네트워크, 기관 및/또는 개인 인트라넷과 같은 사설 네트워크, 또는 사설 및 공중 네트워크의 일부 조합을 포함할 수 있다. 또한, 네트워크(들)(104)는 LAN, WAN, 위성 네트워크, 케이블 네트워크, 와이파이 네트워크, 와이맥스 네트워크, 이동통신 네트워크(예를 들면, 3G, 4G, 등) 또는 이들의 임의의 조합을 포함하지만 이들로 제한되지 않는 임의의 타입의 유선 및/또는 무선 네트워크를 포함할 수 있다. 네트워크(들)(104)는 IP, TCP, UDP, 또는 다른 타입의 프로토콜과 같은 패킷 기반 및/또는 데이터그램 기반 프로토콜을 포함한 통신 프로토콜을 이용할 수 있다. 게다가, 네트워크(들)(104)는 네트워크 통신을 가능하게 하고 및/또는 스위치, 라우터, 게이트웨이, 액세스 포인트, 방화벽, 기지국, 중계기, 백본 장치, 등과 같은 네트워크에서의 하드웨어 기반을 형성하는 다수의 장치를 포함할 수도 있다.

[0022] 일부 예에서, 네트워크(들)(104)는 WAP와 같은 무선 네트워크로의 접속을 가능하게 하는 장치를 더 포함할 수 있다. 예들은 IEEE 802.11 표준(예를 들면, 802.11g, 802.11n, 등) 및 기타 표준을 지원하는 WAP를 포함해서 다수의 전자기 주파수(예를 들면, 무선 주파수)를 통해 데이터를 송신 및 수신하는 WAP를 거친 접속을 지원한다.

[0023] 다수의 예들에서, 분산형 컴퓨팅 리소스(102)는 장치들(106(1)-106(M))을 포함한다. 예들은 장치(들)(106)가 리소스를 공유하기 위해, 부하의 균형을 맞추기 위해, 성능을 증대시키기 위해, 장애 해결 지원 또는 리던던시를 제공하기 위해, 또는 다른 목적을 위해 클러스터에서 또는 다른 그룹화된 구성에서 동작하는 하나 이상의 컴퓨팅 장치를 포함할 수 있다. 장치(들)(106)는 종래의 서버형 장치, 데스크탑 컴퓨터형 장치, 모바일형 장치, 특수 목적형 장치, 내장형 장치, 및/또는 웨어러블형 장치와 같은 다양한 카테고리 또는 클래스의 장치들에 속할 수 있다. 따라서, 단일형의 장치로서 도시되어 있지만, 장치(들)(106)는 매우 다양한 장치 타입을 포함할 수 있고 특정 타입의 장치로 제한되지 않는다. 장치(들)(106)는 데스크탑 컴퓨터, 서버 컴퓨터, 웹-서버 컴퓨터, 퍼스널 컴퓨터, 모바일 컴퓨터, 랩탑 컴퓨터, 태블릿 컴퓨터, 웨어러블 컴퓨터, 매립형 컴퓨팅 장치, 전자 통신 장치, 자동차용 컴퓨터, 네트워크 가능 텔레비전, 씬 클라이언트(thin clients), 단말기, PDA, 게임 콘솔, 게임 장치, IoT 장치, 워크 스테이션, 미디어 플레이어, 퍼스널 비디오 레코더(PVR), 셋탑 박스, 카메라, 컴퓨팅 장치, 전자 기기, 또는 임의의 다른 종류의 컴퓨팅 장치에 포함시키기 위한 통합형 컴포넌트(즉, 주변 장치)로 나타낼 수 있지만, 이로 제한되지 않는다.

[0024] 장치(들)(106)는, 일부 예에서 시스템 버스, 데이터 버스, 어드레스 버스, PCI 버스, 미니-PCI 버스, 및 임의의 다양한 로컬형, 주변형, 및/또는 독립형 버스 중 하나 이상의 포함할 수 있는 버스(112)를 거쳐서, 컴퓨터 판독가능 매체(110)에 동작가능하게 접속된 하나 이상의 프로세싱 유닛(들)(108)을 갖는 임의의 컴퓨팅 장치를 포함할 수 있다. 컴퓨터 판독가능 매체(110)에 저장된 실행가능 인스트럭션은 예를 들어 오퍼레이팅 시스템(114), 보안 격리 기술(SIT; secure isolation technology) 검증 유틸리티(116), 및 프로세싱 유닛(들)(108)에 의해 로드 및 실행 가능한 기타 모듈, 프로그램, 또는 애플리케이션을 포함할 수 있다. 이와 달리 또는 추가로, 본 명세서에서 설명되는 기능은 가속기와 같은 하나 이상의 하드웨어 로직 컴포넌트에 의해 적어도 부분적으로 수행될 수 있다. 예컨대, 제한 없이, 사용될 수 있는 하드웨어 로직 컴포넌트의 예시적 형태로는 FPGA(Field-programmable Gate Arrays), ASIC(Application-specific Integrated Circuits), ASSP(Application-specific Standard Products), SOC(System-on-a-chip systems), CPLD(Complex Programmable Logic Devices), 등이 포함된다. 예컨대, 가속기는 FPGA 패브릭에 내장된 CPU를 포함하는 ZYLEX 또는 ALTERA 중 하나와 같은 하이브리드 장치로 나타낼 수 있다.

[0025] 또한, 장치(들)(106)는 컴퓨팅 장치(들)(106)와 클라이언트 컴퓨팅 장치(들)(120)와 같은 다른 네트워크화된 장치들 간의 통신을 가능하게 하기 위해 하나 이상의 네트워크 인터페이스(118)를 포함할 수 있다. 이러한 네트

워크 인터페이스(들)(118)는 네트워크를 통해 통신을 전송 및 수신하기 위해 하나 이상의 네트워크 인터페이스 제어기(NIC) 또는 다른 형태의 트랜시버 장치를 포함할 수 있다. 단순화를 위해, 다른 구성요소들은 예시적인 장치(들)(106)에서 생략된다.

[0026] 전자 장치에서의 불법 복제 및 불법 행위를 방지하는 데 보안 격리 기술을 사용하는 기법을 구현하도록 구성된 다른 장치들은 클라이언트 컴퓨팅 장치들, 예를 들어 하나 이상의 클라이언트 컴퓨팅 장치(120(1)-120(N))를 포함할 수 있다. 클라이언트 컴퓨팅 장치(들)(120)는 종래의 클라이언트형 장치, 데스크탑 컴퓨터형 장치, 모바일형 장치, 특수 목적형 장치, 내장형 장치, 및/또는 웨어러블형 장치와 같은 장치(들)(106)와 동일하거나 상이할 수 있는 다양한 카테고리 또는 클래스의 장치에 속할 수 있다. 클라이언트 컴퓨팅 장치(들)(120)는 랩탑 컴퓨터(120(1)), 태블릿 컴퓨터(120(2)), 이동 전화(120(3))와 같은 전자 통신 장치, GPS 장치를 포함하는 위성 기반 네비게이션 시스템 및 기타 위성 기반의 네비게이션 시스템과 같은 컴퓨터 네비게이션형 클라이언트 컴퓨팅 장치, 이동 전화/태블릿 하이브리드, PDA, 퍼스널 컴퓨터, 기타 모바일 컴퓨터, 웨어러블 컴퓨터, 매립형 컴퓨팅 장치, 데스크탑 컴퓨터, 자동차용 컴퓨터, 네트워크 가능 텔레비전, 씬 클라이언트, 단말기, 게임 콘솔, 게임 장치(120(4)), 네트워크 접속 차량(120(5)), IoT 장치(120(N)), 워크 스테이션, 미디어 플레이어, PVR, 셋톱 박스, 카메라, 컴퓨팅 장치, 전자 기기, 또는 임의의 다른 종류의 컴퓨팅 장치에 포함시키기 위한 통합형 컴포넌트(즉, 주변 장치)를 포함할 수 있지만, 이로 제한되지 않는다.

[0027] 랩탑 컴퓨터(120(1))와 같이 다양한 카테고리 또는 클래스 및 장치 형태의 클라이언트 컴퓨팅 장치(들)(120)는, 예를 들어 시스템 버스, 데이터 버스, 어드레스 버스, PCI 버스, 미니-PCI 버스, 및 임의의 다양한 로컬형, 주변형, 및/또는 독립형 버스 중 하나 이상의 포함할 수 있는 버스(126)를 거쳐서, 컴퓨터 메모리(124)에 동작가능하게 접속된 하나 이상의 프로세싱 유닛(들)(122)을 갖는 임의 형태의 컴퓨팅 장치를 나타낼 수 있다.

[0028] 컴퓨터 메모리(124)에 저장된 실행가능 인스트럭션은 예를 들어 오퍼레이팅 시스템(128), 애플리케이션(130)의 제 1 부분 및 프로세싱 유닛(들)(122)에 의해 로드 가능하고 실행 가능한 기타 모듈, 프로그램, 또는 애플리케이션을 포함할 수 있다.

[0029] 또한, 클라이언트 컴퓨팅 장치(들)(120)는 클라이언트 컴퓨팅 장치(들)(120)와 다른 네트워크화된 장치들, 예를 들어 네트워크(들)(104)를 통한 다른 클라이언트 컴퓨팅 장치(들)(120) 또는 장치(들)(106) 간의 통신을 가능하게 하기 위해 하나 이상의 네트워크 인터페이스(132)를 포함할 수 있다. 이러한 네트워크 인터페이스(들)(132)는 네트워크를 통해 통신을 전송 및 수신하기 위해 하나 이상의 네트워크 인터페이스 제어기(NIC) 또는 다른 형태의 트랜시버 장치를 포함할 수 있다.

[0030] 도 1의 예에서, 클라이언트 컴퓨팅 장치(들)(120)는 클라이언트 컴퓨팅 장치(들)(120) 상에서의 데이터 및/또는 코드를 보호하는 하드웨어 기반 보안 격리 기술을 포함할 수 있다. 하드웨어 기반 보안 격리 기술은 클라이언트 컴퓨팅 장치(들)(120)의 프로세싱 유닛(들)(122)이 보안 모드에서 동작할 수 있게 하고, 컴퓨터 메모리(124)의 하드웨어 기반 보안 격리 영역(HBSIR; hardware based secure isolated region)(134)에 데이터 및/또는 코드를 저장함으로써 데이터 및/또는 코드를 보호할 수 있다. 일부 예에서, 클라이언트 컴퓨팅 장치(들)(120)의 오퍼레이팅 시스템(128), 하이퍼바이저, 및/또는 펌웨어는 컴퓨터 메모리(124)의 하드웨어 기반 보안 격리 영역(134) 내의 데이터 및/또는 코드에 액세스하는 것을 제한받는다. 이와 같이, 사용자가 클라이언트 컴퓨팅 장치(들)(120)(예를 들면, 컴퓨팅 장치(들)(120)의 오퍼레이팅 시스템(128), 하이퍼바이저, 및/또는 펌웨어)를 조작하더라도, 하드웨어 기반 보안 격리 영역(134) 내의 데이터 및/또는 코드는 추출 및 조작으로부터 여전히 안전하다.

[0031] 예컨대, 일부 예에서, 프로세싱 유닛(들)(122) 및 클라이언트 컴퓨팅 장치(들)(120)는 SECURE GUARD EXTENSIONS(SGX)을 포함하는 INTEL의 SKYLAKE CHIPS을 포함할 수 있다. 이러한 예에서, SGX에 의해, 하드웨어 기반 보안 격리 영역(134)을 포함할 수 있는 ENCLAVE 내의 데이터 및/또는 코드가 악의적인 오퍼레이팅 시스템(128), 하이퍼바이저, 및/또는 펌웨어에도 불구하고 기밀로 유지될 수 있는 "엔클레이브(enclave)" 모드에서 프로세싱 유닛(들)(122)이 실행될 수 있다.

[0032] 도 1의 예에서, 하드웨어 기반 보안 격리 영역(134)은 애플리케이션의 제 2 부분(136)을 저장한다. 예컨대, 도 1의 예에서, 애플리케이션의 제 1 부분(130) 및 애플리케이션의 제 2 부분(136)은 단일 애플리케이션용 코드를 포함할 수 있다. 일부 예에서, 애플리케이션의 제 1 부분(130)은 평문을 포함하고, 애플리케이션의 제 2 부분(136)은 평문 부분 및 암호화 부분을 포함한다. 이와 같이, 클라이언트 컴퓨팅 장치(들)(120)는 컴퓨터 메모리(124)에 저장된 애플리케이션의 제 1 부분(130) 및 하드웨어 기반 보안 격리 영역(134)에 저장된 애플리케이션의 제 2 부분(136)을 사용하여 애플리케이션을 실행할 수 있다.

[0033] 예컨대, 일부 예에서, 클라이언트 컴퓨팅 장치(들)(120)는 장치(들)(106)와 보안 암호화 통신 채널을 수립하기 위해 애플리케이션의 제 2 부분(예를 들면, 평문)을 사용할 수 있다. 예컨대, 프로세싱 유닛(들)(122)으로 하여금 보안 암호화 통신 채널을 수립하게 하는 평문 부분에 포함된 컴퓨터 판독가능 인스트럭션을 프로세싱 유닛(들)(122)이 실행할 수 있다. 보안 암호화 통신 채널을 사용하는 경우, 하드웨어 기반 보안 격리 영역(134)은 클라이언트 컴퓨팅 장치(들)(120)를 거쳐서 장치(들)(106)과 간접적으로 통신할 수 있다.

[0034] 예컨대, 클라이언트 컴퓨팅 장치(들)(120)는 보안 암호화 통신 채널을 거쳐서 장치(들)(106)로 데이터를 전송함으로써 장치(들)(106)에 대해 입증할 수 있다. 일부 예에서, 데이터는 프로세싱 유닛(들)(122)의 식별(예를 들면, CPU 칩 번호), 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 컴퓨팅 장치(들)(120)의 코드가 실제로 실행되고 있다는 증거, 및/또는 하드웨어 기반 보안 격리 영역(134)의 다이제스트를 포함할 수 있다. 이러한 예에서, 하드웨어 기반 보안 격리 영역(134)의 다이제스트는 평문 부분 및 암호화 부분을 포함한다. 데이터를 사용하는 경우, 장치(들)(106)는 하드웨어 기반 보안 격리 기술을 지원하는 클라이언트 컴퓨팅 장치(들)(120) 상에서 하드웨어 기반 보안 격리 영역(134)이 실행되고 있는지를 검증할 수 있다. 추가적으로, 일부 예에서, 장치(들)(106)는 클라이언트 컴퓨팅 장치(들)(120) 및/또는 클라이언트 컴퓨팅 장치(들)(120)의 사용자가 애플리케이션에 대한 라이센스를 포함하고 있는지를 검증할 수 있다. 그 후에 장치(들)(106)는 보안 암호화 통신 채널을 거쳐서 클라이언트 컴퓨팅 장치(들)(120)로 복호화 키(138)를 전송할 수 있다.

[0035] 복호화 키(138)를 수신한 후에, 클라이언트 컴퓨팅 장치(들)(120)는 애플리케이션의 암호화된 부분을 복호화하기 위해 복호화 키(138)를 사용한다. 예컨대, 프로세싱 유닛(들)(122)으로 하여금 암호화된 부분을 복호화 키(138)를 사용하여 복호화하도록 하게 하는 평문 부분에 포함된 컴퓨터 판독가능 인스트럭션을 프로세싱 유닛(들)(122)이 실행할 수 있다. 그 후에 클라이언트 컴퓨팅 장치(들)(120)는 하드웨어 기반 보안 격리 영역(134) 내에서 애플리케이션의 암호화된 제 2 부분을 실행할 수 있다.

[0036] 도 2는 불법 복제 및 불법 행위를 방지하기 위해 하드웨어 기반 보안 격리 기술을 이용하도록 구성된 예시적인 클라이언트 컴퓨팅 장치(200)를 도시하는 블록도이다. 컴퓨팅 장치(200)는 클라이언트 컴퓨팅 장치(들)(120)를 나타낼 수 있다. 예시적인 컴퓨팅 장치(200)는 하나 이상의 프로세싱 유닛(들)(202), 컴퓨터 메모리(204), 입력/출력 인터페이스(206), 및 네트워크 인터페이스(들)(208)를 포함한다. 컴퓨팅 장치(200)의 구성요소들은 예를 들어 버스(126)를 나타낼 수 있는 버스(210)를 거쳐서 동작가능하게 연결되어 있다.

[0037] 예시적인 컴퓨팅 장치(200)에서, 프로세싱 유닛(들)(202)은 프로세싱 유닛(들)(122)에 대응할 수 있고, 또한 예를 들어 CPU 방식 프로세싱 유닛, GPU 방식 프로세싱 유닛, FPGA, 다른 종류의 DSP, 또는 일부 경우에 CPU에 의해 구동될 수 있는 기타 하드웨어 로직 컴포넌트를 나타낼 수 있다. 예컨대, 제한 없이, 사용될 수 있는 예시적인 형태의 하드웨어 로직 컴포넌트는 ASIC, ASSP(Application-Specific Standard Products), SOC(System-on-a-chip systems), CPLD(Complex Programmable Logic Devices), 등을 포함한다.

[0038] 컴퓨터 메모리(204)는 컴퓨터 메모리(124)에 대응할 수 있고, 프로세싱 유닛(들)(202)에 의해 실행가능한 인스트럭션을 저장할 수 있다. 또한, 컴퓨터 메모리(204)는 외부 CPU, 외부 GPU와 같은 외부 프로세싱 유닛에 의해 실행가능한, 및/또는 FPGA 방식 가속기, DSP 방식 가속기와 같은 외부 가속기, 또는 임의의 다른 내부 또는 외부 가속기에 의해 실행가능한 인스트럭션을 저장할 수 있다. 다수의 예에서, CPU, GPU, 및/또는 가속기 중 적어도 하나가 컴퓨팅 장치(100)에 통합되는 반면에, 일부 예에서 CPU, GPU, 및/또는 가속기 중 하나 이상은 컴퓨팅 장치(200) 외부에 있다.

[0039] 컴퓨터 메모리(204)는 컴퓨터 저장 매체를 포함할 수 있다. 컴퓨터 저장 매체는 휘발성 메모리, 비휘발성 메모리, 및/또는 기타 영구적 및/또는 보조적 컴퓨터 저장 매체, 컴퓨터 판독가능 인스트럭션, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현되는 착탈식 및 비착탈식 컴퓨터 메모리 중 하나 이상을 포함할 수 있다. 따라서, 컴퓨터 저장 매체는 RAM, SRAM, DRAM, PRAM, ROM, EPROM, EEPROM, 플래시 메모리, 또는 컴퓨팅 장치에 의한 액세스에 대한 정보를 저장 및 유지하는 데 사용될 수 있는 임의의 다른 저장 메모리, 저장 장치, 및/또는 저장 매체를 포함해서, 장치의 일부이거나 장치 외부에 있는 하드웨어 컴포넌트 및/또는 장치에 포함된 유형적 및/또는 물리적 형태의 매체를 포함한다.

[0040] 입력/출력(I/O) 인터페이스(206)는 주변 입력 장치(예를 들면, 키보드, 마우스, 펜, 게임 콘트롤러, 음성 입력 장치, 터치 입력 장치, 제스처 입력 장치, 등)를 포함한 사용자 입력 장치 및/또는 주변 출력 장치(예를 들면, 디스플레이, 프린터, 오디오 스피커, 햅틱 출력, 등)를 포함한 출력 장치와 같은 입력/출력 장치와 컴퓨팅 장치(200)가 통신하게 한다.

[0041] 네트워크 인터페이스(들)(132)에 대응할 수 있는 네트워크 인터페이스(들)(208)는, 예를 들어 네트워크를 통해 통신을 전송 및 수신하기 위한 네트워크 인터페이스 제어기(NIC) 또는 다른 형태의 트랜시버 장치를 나타낼 수 있다.

[0042] 도시된 예에서, 컴퓨터 메모리(204)는 비휘발성 저장 매체(212)를 포함한다. 비휘발성 저장 매체(212)는 컴퓨터 메모리(204)에 저장되고 및/또는 프로세싱 유닛(들)(202) 및/또는 가속기(들)에 의해 실행되는 프로세스, 애플리케이션, 컴포넌트, 및/또는 모듈의 동작들을 위한 데이터를 저장할 수 있다. 추가적으로, 일부 예에서, 상기한 데이터의 일부 또는 전부는 하나 이상의 프로세싱 유닛(들)(202)에 탑재된 별도의 메모리(214), 예를 들어 CPU 방식 프로세서, GPU 방식 메모리, FPGA 방식 가속기, DSP 방식 가속기, 및/또는 다른 가속기에 탑재된 메모리에 저장될 수 있다.

[0043] 도 2의 도시된 예에서, 컴퓨터 메모리(204)는 오퍼레이팅 시스템(128)을 나타낼 수 있는 오퍼레이팅 시스템(216)을 또한 포함한다. 추가적으로, 컴퓨터 메모리(204)는 하드웨어 기반 보안 격리 영역(134) 및 애플리케이션의 제 1 부분(130)을 각각 나타낼 수 있는 하드웨어 기반 보안 격리 영역(218) 및 애플리케이션의 제 1 부분(220)을 포함한다. 또한, 컴퓨터 메모리(204)는 암호화된 복호화 키(222)를 포함한다.

[0044] 도 2의 예에서, 하드웨어 기반 보안 격리 영역(218)은 애플리케이션의 제 2 부분(224)(애플리케이션의 제 2 부분(136)을 나타낼 수 있음), 복호화 키(226), 및 실링 키(228)를 저장한다. 일부 예에서, 컴퓨터 메모리(204)에 저장된 애플리케이션의 제 1 부분(220) 및 하드웨어 기반 보안 격리 영역(218)에 저장된 애플리케이션의 제 2 부분(224)은 소프트웨어 애플리케이션에 대한 데이터 및 코드를 포함한다. 예컨대, 애플리케이션의 제 1 부분(220)은 애플리케이션에 대한 평문을 포함할 수 있다. 애플리케이션의 제 2 부분(224)은 애플리케이션의 평문 부분(230) 및 애플리케이션의 암호화 부분(232)을 포함할 수 있다. 일부 예에서, 평문 부분(230)은 암호화 부분(232)을 복호화하기 위해 복호화 키(226)를 다운로드하는 표준 라이센싱 코드를 포함한다. 일부 예에서, 암호화 부분(232)은 애플리케이션을 적절하게 실행하는 데 중요한 코드를 포함한다. 예컨대, 게임용 암호화 부분(232)은 AI 휴리스틱, 물리 계산, 커스텀 그래픽 프로세싱 유닛 커맨드 생성, 등을 위한 코드를 포함할 수 있다.

[0045] 하드웨어 기반 보안 격리 영역(218)은 블록들(234, 236, 238, 240, 242)로서 도시되어 있는 하나 이상의 모듈을 더 포함할 수 있지만, 이는 단지 예이며 개수는 더 많거나 더 적게 변할 수 있다. 블록들(234, 236, 238, 240, 242)과 관련되어 설명된 기능은 보다 적은 수의 모듈에 의해 수행되도록 결합될 수 있거나, 보다 많은 수의 모듈에 의해 분할 및 수행될 수 있다. 추가적으로, 일부 예에서, 블록들(234, 236, 238, 240, 242)과 관련된 기능 중 일부는 하드웨어 기반 보안 격리 영역(218)에 포함되지 않는 모듈에 의해 수행될 수 있다.

[0046] 블록(234)은 컴퓨팅 장치(200)에 있어서 본 명세서에서 설명되는 입증 프로세스를 수행하기 위해 컴퓨팅 장치(200)의 프로세싱 유닛(들)(202)을 프로그래밍하는 로직을 포함한다. 예컨대, 프로세싱 유닛(들)(202)은 도 1에서의 장치(들)(106)와 같은 서버에 대해 입증하기 위해 입증 모듈(234)을 실행할 수 있다. 일부 예에서, 서버에 대해 입증하기 위해, 컴퓨팅 장치(200)는 하드웨어 기반 보안 격리 영역(218) 내의 평문 부분(230)을 사용하여 서버와의 보안 암호화 통신 채널을 수립한다. 예컨대, 디피 헬먼(Diffie-Hellman) 키 교환 알고리즘은 이러한 보안 암호화 통신 채널을 셋업하는 데 사용될 수 있다. 예컨대, 프로세싱 유닛(들)(202)은 네트워크 인터페이스(들)(208)를 거쳐서 서버와 보안 암호화 통신 채널을 프로세싱 유닛(들)(202)으로 하여금 수립하게 하는 평문 부분(230)에 포함된 코드를 실행할 수 있다.

[0047] 일부 예에서, 컴퓨팅 장치(200)는 애플리케이션을 실행하는 데 컴퓨팅 장치(200)를 사용하는 사용자에 응답하여 보안 암호화 통신 채널을 수립한다. 보안 암호화 통신 채널을 수립한 후에, 하드웨어 기반 보안 격리 영역(218)은 컴퓨팅 장치(200)를 거쳐서 서버와 간접적으로 통신할 수 있다. 예컨대, 보안 암호화 통신 채널을 통해, 컴퓨팅 장치(200)는 입증을 수행하기 위해 서버로 데이터를 전송하는 데 입증 모듈(234)을 사용할 수 있다. 일부 예에서, 데이터는 전자 장치의 프로세싱 유닛(들)(202)의 식별자(예를 들면, CPU 칩 번호), 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 전자 장치의 코드가 실제로 실행되고 있다는 증거, 및/또는 하드웨어 기반 보안 격리 영역(218)의 다이제스트를 포함한다. 이러한 예에서, 하드웨어 기반 보안 격리 영역(218)의 다이제스트는 평문 부분(230) 및 암호화 부분(232)을 포함한다. 데이터를 사용하는 경우, 서버는 하드웨어 기반 보안 격리 기술을 지원하는 컴퓨팅 장치(200) 상에서 하드웨어 기반 보안 격리 영역(218)이 실행되고 있는지를 검증할 수 있다. 추가적으로, 일부 예에서, 서버는 컴퓨팅 장치(200) 및/또는 컴퓨팅 장치(200)의 사용자가 애플리케이션에 대한 라이센스를 포함하고 있는지를 검증할 수 있다. 그러면 서버는 보안 암호화 통신 채널을 거쳐서 컴퓨팅 장치(200)로 복호화 키(226)를 전송할 수 있다.

[0048] 블록(236)은 서버와 보안 채널을 수립하도록 컴퓨팅 장치(200)의 프로세싱 유닛(들)(202)을 프로그래밍하는 로직을 포함한다. 예컨대, 프로세싱 유닛(들)(202)은 네트워크 인터페이스(들)(208)를 이용할 수 있는 보안 통신 모듈(236)을 실행하여, 도 1의 장치(들)(106)와 같은 서버와 보안 암호화 통신 채널을 수립할 수 있다. 일부 예에서, 보안 통신 모듈(236)은 디피 헬먼 키 교환 알고리즘을 이용하여 서버와 보안 암호화 통신 채널을 셋업할 수 있다. 일부 예에서, 프로세싱 유닛(들)(202)은, 애플리케이션을 실행하는 데 컴퓨팅 장치(200)를 사용하는 사용자에 응답하여, 보안 암호화 통신 채널을 수립하기 위해 보안 통신 모듈을(236)을 실행한다.

[0049] 블록(238)은 하드웨어 기반 보안 격리 영역(218) 내에 있는 데이터 및/또는 코드를 복호화하도록 컴퓨팅 장치(200)의 프로세싱 유닛(들)(202)을 프로그래밍하는 로직을 포함한다. 예컨대, 컴퓨팅 장치(200)는 보안 격리 영역(SIR) 복호화 모듈(238)을 이용하여 하드웨어 기반 보안 격리 영역(218) 내에서의 애플리케이션의 암호화 부분(232)을 복호화할 수 있다. 암호화 부분(232)을 복호화함으로써 애플리케이션의 복호화 부분을 생성할 수 있다. 일부 예에서, 복호화 부분은 애플리케이션의 실행중에 하드웨어 기반 보안 격리 영역(218) 내에서 프로세싱 유닛(들)(202)이 실행하는 코드를 포함할 수 있다. 일부 예에서, 컴퓨팅 장치(200)는 컴퓨팅 장치(200)가 애플리케이션을 실행하고자 시도할 때마다 복호화 키(226)를 사용하여 암호화 부분(232)을 복호화하는 데 SIR 복호화 모듈(238)을 이용한다.

[0050] 컴퓨팅 장치(200)는 하드웨어 기반 보안 격리 영역(218) 내에서 암호화된 복호화 키(222)를 복호화하는 데 SIR 복호화 모듈(238)을 더 이용할 수 있다. 예컨대, 일부 예에서, 컴퓨팅 장치(200)는 실링 키(228)를 사용하여 복호화 키(226)를 암호화하고, 암호화된 복호화 키(222)를 컴퓨터 메모리(204)에 저장한다. 이러한 예에서, 컴퓨팅 장치(200)는, 복호화 키(226)를 불러오기 위해, 실링 키(228)를 사용하여 하드웨어 기반 보안 격리 영역(218) 내에서 암호화된 복호화 키(222)를 복호화하는 데 SIR 복호화 모듈(238)을 이용할 수 있다.

[0051] 블록(240)은 실링 키(228)를 생성하도록 컴퓨팅 장치(200)의 프로세싱 유닛(들)(202)을 프로그래밍하는 로직을 포함한다. 예컨대, 컴퓨팅 장치(200)는 실링 키(228)를 생성하는 데 실링 키 생성 모듈(240)을 이용할 수 있다. 일부 예에서, 실링 키(228)는 프로세싱 유닛(들)(202) 및/또는 하드웨어 기반 보안 격리 영역(218)에 대해 특정적이어야 한다. 예컨대, 이러한 예에서, 프로세싱 유닛(들)(202) 및 하드웨어 기반 보안 격리 영역(218)을 포함하는 컴퓨팅 장치(200)만이 실링 키(228)를 생성할 수 있다. 일부 예에서, 컴퓨팅 장치(200)가 복호화 키(226)를 암호화해야 할 때마다 및/또는 컴퓨팅 장치(200)가 암호화된 복호화 키(222)를 복호화해야 할 때마다, 컴퓨팅 장치(200)는 실링 키(228)를 생성하는 데 실링 키 생성 모듈(240)을 이용한다.

[0052] 블록(242)은 실링 키(228)를 사용하여 복호화 키(226)를 암호화하도록 컴퓨팅 장치(200)의 프로세싱 유닛(들)(202)을 프로그래밍하는 로직을 포함한다. 예컨대, 컴퓨팅 장치(200)는 암호화된 복호화 키(222)를 생성하기 위해 실링 키(228)를 사용하여 복호화 키(226)를 암호화하는 데 보안 격리 영역 암호화 모듈(242)을 이용할 수 있다. 그 후에 일부 예에서, 컴퓨팅 장치(200)는 암호화된 복호화 키(222)를 컴퓨터 메모리(204)에 저장할 수 있다. 예컨대, 일부 예에서, 컴퓨팅 장치(200)는 암호화된 복호화 키(222)를 비휘발성 저장 매체(212)에 저장한다.

[0053] 일부 예에서, 컴퓨팅 장치(200)가 서버로부터 플로팅 라이센스를 수신할 수 있다는 것을 유의해야 한다. 이러한 예에서, 컴퓨팅 장치(200)는 실링 키(228)를 사용하여 복호화 키(226)를 암호화하지 않고, 하드웨어 기반 보안 격리 영역(218)의 외부에 복호화 키(암호화 여부에 상관 없음)를 절대 저장하지 않는다. 대신에, 시스템은 애플리케이션을 사용하기 위한 이 라이센스가 한 번에 하나의 전자 장치에 의해서만 사용되는지를 확인해야 할 필요가 있을 것이다. 이를 행하기 위해, 컴퓨팅 장치(200)가 플로팅 라이센스를 수신하면, 컴퓨팅 장치(200) 및/또는 하드웨어 기반 보안 격리 영역(218)은 서버와 주기적(예를 들면, 매분, 10분마다 등과 같은 시간 간격)으로 통신하라는 인스트럭션을 서버로부터 수신할 수 있다. 그 후에 하드웨어 기반 보안 격리 영역(218)은, (1) 컴퓨팅 장치(200) 및/또는 하드웨어 기반 보안 격리 영역(218)이 서버와 통신할 수 없는 경우에, 또는 (2) 컴퓨팅 장치(200)의 사용자가 컴퓨팅 장치(200)에서 사용되는 사용자와 동일한 라이센스를 갖는 애플리케이션을 허가하는 데 상이한 컴퓨팅 장치를 사용하는 경우에, 평문 부분(230) 및/또는 애플리케이션의 복호화 부분에게 실행을 종료하게 할 수 있다.

[0054] 도 3은 하드웨어 기반 보안 격리 기술을 검증하는 전자 장치 상에서 불법 복제 및 불법 행위를 방지하는 것과 관련된 기술을 수행하도록 구성된 예시적인 서버 컴퓨팅 장치를 도시하는 블록도이다. 컴퓨팅 장치(300)는 장치(들)(106)를 나타낼 수 있다. 예시적인 컴퓨팅 장치(300)는 하나 이상의 프로세싱 유닛(들)(302), 컴퓨터 판독가능 매체(304), 입력/출력 인터페이스(들)(306), 및 네트워크 인터페이스(들)(308)를 포함한다. 컴퓨팅 장치(300)의 구성요소들은, 예를 들어 버스(112)를 나타낼 수 있는 버스(310)를 거쳐서 동작가능하게 연결될 수

있다.

[0055] 예시적인 컴퓨팅 장치(300)에서, 프로세싱 유닛(들)(302)은 프로세싱 유닛(들)(108)에 대응할 수 있고, 또한 예를 들면 CPU 방식 프로세싱 유닛, GPU 방식 프로세싱 유닛, FPGA, 다른 부류의 DSP, 또는 일부 경우에 CPU에 의해 구동될 수 있는 기타 하드웨어 로직 컴포넌트를 나타낼 수 있다. 예컨대, 제한 없이, 사용될 수 있는 하드웨어 로직 컴포넌트의 예시적인 형태로는 ASIC, ASSP, SOC, CPLD, 등이 포함된다.

[0056] 컴퓨터 판독가능 매체(304)는 컴퓨터 판독가능 매체(110)에 대응할 수 있고, 프로세싱 유닛(들)(302)에 의해 실행가능한 인스트럭션을 저장할 수 있다. 또한, 컴퓨터 판독가능 매체(304)는 외부 CPU, 외부 GPU와 같은 외부 프로세싱 유닛에 의해 실행가능한 인스트럭션, 및/또는 FPGA 방식 가속기, DSP 방식 가속기와 같은 외부 가속기, 혹은 임의의 다른 내부 또는 외부 가속기에 의해 실행가능한 인스트럭션을 저장할 수 있다. 다수의 예에서, CPU, GPU, 및/또는 가속기 중 적어도 하나가 컴퓨팅 장치(300)에 통합되는 반면에, 일부 예에서 CPU, GPU, 및/또는 가속기 중 하나 이상은 컴퓨팅 장치(300)의 외부에 있다.

[0057] 컴퓨터 판독가능 매체(304)는 컴퓨터 저장 매체 및/또는 통신 매체를 포함할 수 있다. 컴퓨터 저장 매체는 휘발성 메모리, 비휘발성 메모리, 및/또는 기타 영구적 및/또는 보조적 컴퓨터 저장 매체, 컴퓨터 판독 가능 인스트럭션, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현되는 착탈식 및 비착탈식 컴퓨터 저장 매체 중 하나 이상을 포함할 수 있다. 따라서, 컴퓨터 저장 매체는 이로 제한되진 않지만 RAM, SRAM, DRAM, PRAM, ROM, EPROM, EEPROM, 플래시 메모리, 광학 카드 또는 기타 광학 저장 매체, 자기 카세트, 자기 테이프, 자기 디스크 스토리지, 자기 카드 또는 기타 자기 저장 장치 또는 매체, 고체 상태 메모리 장치, 스토리지 어레이, 네트워크 접속된 스토리지, 스토리지 영역 네트워크, 호스트 컴퓨터 스토리지 또는 임의의 다른 스토리지 메모리, 스토리지 장치, 및/또는 컴퓨팅 장치에 의한 액세스용 정보를 저장 및 유지하는 데 사용될 수 있는 스토리지 매체를 포함해서, 장치의 일부이거나 장치 외부에 있는 하드웨어 컴포넌트 및/또는 장치에 포함된 유형적 및/또는 물리적 형태의 매체를 포함한다.

[0058] 컴퓨터 저장 매체와 달리, 통신 매체는 컴퓨터 판독가능 인스트럭션, 데이터 구조, 프로그램 모듈, 혹은 반송파와 같은 변조된 데이터 신호 또는 다른 전송 메카니즘에서의 다른 데이터를 구현할 수 있다. 본 명세서에서 정의된 바와 같이, 컴퓨터 저장 매체는 통신 매체를 포함하지 않는다. 즉, 컴퓨터 저장 매체는 변조된 데이터 신호, 반송파, 또는 전파 신호만으로 구성된 통신 매체를 포함하지 않는다.

[0059] 입력/출력(I/O) 인터페이스(306)는 주변 입력 장치(예를 들면, 키보드, 마우스, 펜, 게임 콘트롤러, 음성 입력 장치, 터치 입력 장치, 제스처 입력 장치, 등)를 포함한 사용자 입력 장치 및/또는 주변 출력 장치(예를 들면, 디스플레이, 프린터, 오디오 스피커, 햅틱 출력, 등)를 포함한 출력 장치와 같은 입력/출력 장치와 통신 장치(300)가 통신하게 한다.

[0060] 네트워크 인터페이스(들)(118)에 대응할 수 있는 네트워크 인터페이스(들)(308)는, 예를 들면 네트워크 인터페이스 제어기(NIC), 또는 네트워크를 통해 통신을 전송 및 수신하는 다른 형태의 트랜시버 장치를 나타낼 수 있다.

[0061] 도시된 예에서, 프로세싱 유닛(들)(312)은 별도의 메모리(312)를 포함한다. 일부 예에서, 상기한 데이터의 일부 또는 전부는 하나 이상의 프로세싱 유닛(들)(302)에 탑재된 별도의 메모리(312), 예를 들어 CPU 방식 프로세서, GPU 방식 메모리, FPGA 방식 가속기, DSP 방식 가속기, 및/또는 다른 가속기에 탑재된 메모리에 저장될 수 있다.

[0062] 도 3의 도시된 예에서, 컴퓨터 판독가능 매체(304)는 오퍼레이팅 시스템(114)을 나타낼 수 있는 오퍼레이팅 시스템(134)을 포함한다. 추가적으로, 컴퓨터 판독가능 매체(304)는 보안 격리 기술 검증 유틸리티(316)를 포함한다. 보안 격리 기술 검증 유틸리티(316)는 블록들(318, 320, 322, 324)로 표시되는 하나 이상의 모듈을 포함할 수 있지만, 이는 단지 예이며, 개수가 더 많거나 더 적게 변할 수 있다. 블록들(318, 320, 322, 324)과 관련되어 설명되는 기능은 보다 적은 수의 모듈에 의해 수행되도록 결합될 수 있거나, 보다 많은 수의 모듈에 의해 분할 및 수행될 수 있다. 추가적으로, 일부 예에서, 블록들(318, 320, 322, 324)과 관련된 기능 중 일부는 보안 격리 기술 검증 유틸리티(316)에 포함되지 않는 모듈에 의해 수행될 수 있다.

[0063] 블록(318)은 컴퓨팅 장치(300)에 대해서 본 명세서에서 설명되는 입증 프로세스를 수행하도록 컴퓨팅 장치(300)의 프로세싱 유닛(들)(302)을 프로그래밍하는 로직을 포함한다. 예컨대, 컴퓨팅 장치(300)는 보안 암호화 통신 채널을 거쳐서 도 1의 클라이언트 컴퓨팅 장치(120)와 같은 전자 장치로부터 데이터(예를 들면, 입증 정보)를 수신할 수 있다. 컴퓨팅 장치(300)는 전자 장치가 데이터를 사용하여 하드웨어 기반 보안 격리 기술을 실행

하고 있는지를 검증하기 위해 입증 검증을 수행하는 데 입증 검증 모듈(318)을 이용할 수 있다. 일부 예에서, 데이터는 전자 장치의 CPU 칩의 식별자(예를 들면, CPU 칩 번호), 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 전자 장치의 코드가 실제로 실행되고 있다는 증거, 및/또는 하드웨어 기반 보안 격리 영역의 다이제스트 값을 포함할 수 있다.

[0064] 예컨대, 컴퓨팅 장치(300)는 전자 장치가 신뢰적인 CPU 칩을 포함하는지 및 하드웨어 기반 보안 격리 기술을 포함하는지를 검증함으로써 입증을 수행할 수 있다. 예컨대, 서버는 보안 격리 기술(SIT) 데이터베이스(326)를 사용하여 CPU 칩의 아이덴티티 및 하드웨어 기반 보안 격리 영역의 아이덴티티를 검증할 수 있다. SIT 데이터베이스(326)는 하드웨어 기반 보안 격리 기술과 전자 장치를 연관시키는 데이터를 포함할 수 있다. 이와 같이, 컴퓨팅 장치(300)는 전자 장치의 CPU 칩이 전자 장치 상에서 하드웨어 기반 보안 격리 기술에 매칭되는지를 검증하는 데 SIT 데이터베이스(326)를 사용할 수 있다. 일부 예에서, CPU 칩이 전자 장치 상에서 하드웨어 보안 격리 기술에 매칭된다고 컴퓨팅 장치(300)가 결정하면, 컴퓨팅 장치(300)는 전자 장치 상에서 하드웨어 기반 보안 격리 기술을 검증할 수 있다. 그러나, CPU 칩이 전자 장치 상에서 하드웨어 기반 보안 격리 기술에 매칭되지 않는다고 컴퓨팅 장치가 결정하면, 컴퓨팅 장치(300)는 전자 장치 상에서 하드웨어 기반 보안 격리 기술을 검증하지 않는다.

[0065] 블록(320)은 전자 장치와 관련해서 애플리케이션과 연관된 권한을 결정하도록 컴퓨팅 장치(300)의 프로세싱 유닛(들)(302)을 프로그래밍하는 로직을 포함한다. 예컨대, 일부 예에서, 전자 장치를 검증한 후에, 컴퓨팅 장치(300)는 전자 장치가 애플리케이션을 실행할 권한을 포함하는지를 결정하기 위해 권한 모듈(320)을 실행할 수 있다.

[0066] 예컨대, 일부 예에서, 컴퓨팅 장치(300)는 전자 장치가 애플리케이션을 실행할 권한을 포함하는지를 결정하는 데 권한 데이터베이스(328)를 이용할 수 있다. 권한 데이터베이스(328)는 다양한 애플리케이션과 연관된 권한을 포함하는 사용자 및/또는 전자 장치를 표시하는 데이터를 포함할 수 있다. 이와 같이, 컴퓨팅 장치(300)는 전자 장치 및/또는 전자 장치의 사용자가 애플리케이션과 연관된 권한을 포함하고 있는지를 결정하는 데 권한 데이터베이스(328)를 사용할 수 있다. 일부 예에서, 컴퓨팅 장치(300)는 전자 장치가 애플리케이션과 연관된 라이센싱 권한을 갖는지를 결정하는 데 CPU 칩의 아이덴티티를 사용할 수 있다. 일부 예에서, 컴퓨팅 장치(300)가 데이터와 함께 사용자에 대한 인증서(예를 들면, 사용자 계정 정보)를 수신하면, 컴퓨팅 장치(300)는 사용자가 애플리케이션과 연관된 라이센싱 권한을 갖는지를 결정할 수 있다.

[0067] 일부 예에서, 애플리케이션과 연관된 권한으로는 애플리케이션에 대한 영구 라이센스 또는 플로팅 라이센스를 포함할 수 있다. 애플리케이션에 대한 영구 라이센스를 포함하는 사용자 및/또는 전자 장치에 기초하여, 컴퓨팅 장치(300)는 애플리케이션에 대한 복호화 키(330)(복호화 키(138)를 나타낼 수 있음)를 전자 장치에 전송할 수 있다. 애플리케이션에 대한 플로팅 라이센스를 포함하는 사용자 및/또는 전자 장치에 기초하여, 컴퓨팅 장치(300)는 애플리케이션에 대한 복호화 키(330) 및 플로팅 라이센스와 연관된 플로팅 라이센스 인스트럭션(332)의 양쪽을 전자 장치에 전송할 수 있다.

[0068] 일부 예에서, 플로팅 라이센스 인스트럭션(332)은, 전자 장치의 하드웨어 기반 보안 격리 기술에 의해, 컴퓨팅 장치(300)와 플로팅 라이센스를 주기적으로 검증하게 할 수 있다. 예컨대, 플로팅 라이센스 인스트럭션(332)은, 하드웨어 기반 보안 격리 기술에 의해, 주어진 시간 간격(예를 들면, 30초마다, 매분, 매시간, 등)으로 컴퓨팅 장치(300)와 통신하여 전자 장치의 애플리케이션에 대한 플로팅 라이센스가 여전히 유효한지를 검증하게 할 수 있다. 일부 예에서, 컴퓨팅 장치(300)는 추가적인 전자 장치의 사용자로부터 유사한 인증서(예를 들어, 사용자 계정 정보)를 수신하는 컴퓨팅 장치(300)에 기초하여 플로팅 라이센스가 더이상 유효하지 않다고 결정할 수 있다. 이러한 예에서, 컴퓨팅 장치(300)는 플로팅 라이센스가 전자 장치 상에서 더이상 유효하지 않음을 표시하는 메시지를 전자 장치에 전송할 수 있다.

[0069] 블록(322)은 컴퓨팅 장치(300)와 전자 장치 간의 통신을 암호화하도록 컴퓨팅 장치(300)의 프로세싱 유닛(들)(302)을 프로그래밍하는 로직을 포함한다. 추가적으로, 블록(324)은 컴퓨팅 장치(300)와 전자 장치 간의 통신을 복호화하도록 컴퓨팅 장치(300)의 프로세싱 유닛(들)(302)을 프로그래밍하는 로직을 포함한다. 예컨대, 일부 예에서, 컴퓨팅 장치(300)는 보안 암호화 통신 채널을 사용하여 전자 장치와 통신한다. 이와 같이, 컴퓨팅 장치(300)는 보안 암호화 통신 채널을 거쳐서 전자 장치로 통신을 전송하기 전에 통신을 암호화하는 데 암호화 모듈(322)을 이용할 수 있다. 추가적으로, 컴퓨팅 장치(300)는 보안 암호화 통신 채널을 거쳐서 전자 장치로부터 수신되는 통신을 복호화하는 데 복호화 모듈(324)을 이용할 수 있다.

[0070] 일부 예에서, 보안 격리 기술 검증 유틸리티(316)가 암호화 모듈(322) 또는 복호화 모듈(324) 중 하나 이상을

포함하지 않을 수 있음을 유의해야 한다. 예컨대, 일부 예에서, 컴퓨팅 장치(300)는 암호화 모듈 및/또는 복호화 모듈을 컴퓨팅 장치(300)의 컴퓨터 판독가능 매체(304)에 저장할 수 있다. 이러한 예에서, 컴퓨팅 장치(300)는 컴퓨터 판독가능 매체(304)에서의 암호화 모듈 및 복호화 모듈을 사용하여 통신을 암호화 및/또는 복호화할 수 있다.

[0071] 도 4-10은 전자 장치의 불법 복제 및 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 사용하는 예시적인 프로세스를 도시한다. 예시적인 프로세스는 하드웨어, 소프트웨어, 또는 그 조합으로 구현될 수 있는 일련의 동작들을 나타낼 수 있는 논리적 흐름 그래프에서 블록들의 집합으로서 도시된다. 블록들은 번호로 참조된다. 소프트웨어와 관련하여, 블록들은 하나 이상의 프로세싱 유닛(예를 들어, 하드웨어 마이크로 프로세서)에 의해 실행될 때에 열거되는 동작들을 수행하는 하나 이상의 컴퓨터 메모리에 저장된 컴퓨터 실행가능 인스트럭션을 나타낸다. 일반적으로, 컴퓨터 실행가능 인스트럭션은 특정한 기능을 수행하거나 특정한 추상 데이터 형태를 구현하는 루틴, 프로그램, 오브젝트, 컴포넌트, 데이터 구조 등을 포함한다. 동작들이 설명되는 순서는 제한적으로 해석되지 말아야 하고, 임의의 개수의 설명되는 블록들은 프로세스를 구현하기 위해 임의의 순서로 및/또는 병렬로 결합될 수 있다.

[0072] 도 4는 애플리케이션의 불법 복제를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하는 전자 장치의 예시적인 방법의 흐름도(400)이다. 블록 402에서, 전자 장치는 애플리케이션의 제 1 부분을 컴퓨터 메모리에 저장할 수 있다. 예컨대, 애플리케이션의 개발자는 전자 장치가 전자 장치의 컴퓨터 메모리로부터 애플리케이션의 어떤 부분을 실행할지, 또한 전자 장치가 전자 장치의 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역으로부터 애플리케이션의 어떤 부분을 실행하지를 특정할 수 있다. 이와 같이, 애플리케이션을 실행할 준비를 할 때, 전자 장치는 컴퓨터 메모리에 애플리케이션의 제 1 부분(예를 들면, 전자 장치가 컴퓨터 메모리로부터 실행하는 애플리케이션의 부분)을 저장할 수 있다. 일부 예에서, 애플리케이션의 제 1 부분은 평문을 포함한다.

[0073] 블록 404에서, 전자 장치는 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 애플리케이션의 제 2 부분을 저장할 수 있다. 예컨대, 전자 장치는 하드웨어 기반 보안 격리 영역에 애플리케이션의 제 2 부분을 저장할 수 있고, 여기서 제 2 부분은 평문 부분 및 암호화 부분을 포함한다. 일부 예에서, 평문 부분은 전자 장치가 서버로부터 복호화 키를 불러오는 데 사용하는 코드를 포함한다. 예컨대, 평문 부분은 복호화 키를 다운로드하는 표준 라이센싱 코드를 포함할 수 있다. 일부 예에서, 암호화 부분은 애플리케이션이 적절하게 실행되는 데 중요한 코드를 포함한다. 예컨대, 암호화 부분은 AI 휴리스틱, 물리 계산, 커스텀 그래픽 프로세싱 유닛 커맨드 생성, 등을 위한 코드를 포함할 수 있다.

[0074] 블록 406에서, 전자 장치는 평문 부분을 사용하여 서버와 보안 암호화 통신 채널을 수립할 수 있다. 예컨대, 전자 장치(예를 들면, 프로세서)는 서버와의 보안 암호화 통신 채널을 전자 장치에게 수립하게 하는 평문 부분에 포함된 컴퓨터 판독가능 인스트럭션을 실행할 수 있다. 일부 예에서, 하드웨어 기반 보안 격리 영역은 전자 장치를 거쳐서 서버와 데이터를 전송 및 수신하는 데 보안 암호화 통신 채널을 간접적으로 사용할 수 있다.

[0075] 블록 408에서, 전자 장치는 보안 암호화 통신 채널을 거쳐서 서버로 데이터를 전송할 수 있다. 예컨대, 전자 장치(예를 들면, 프로세서)는 보안 암호화 통신 채널을 거쳐서 서버로 입증 정보를 전자 장치에게 전송하게 하는 하드웨어 기반 보안 격기 영역에 포함된 컴퓨터 판독가능 인스트럭션(예를 들면, 코드)을 실행할 수 있다. 일부 예에서, 입증 정보는 전자 장치의 프로세서의 식별자(예를 들면, CPU 칩 번호), 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치에서 실제로 실행되고 있다는 증거, 및/또는 하드웨어 기반 보안 격리 영역의 다이제스트 값을 포함할 수 있다. 일부 예에서, 서버는 전자 장치, 프로세서, 및/또는 하드웨어 기반 보안 격리 영역 중 하나 이상을 검증하는 데 입증 정보를 사용하여 입증을 수행할 수 있다. 추가적으로, 일부 예에서, 서버는 전자 장치 및/또는 전자 장치의 사용자가 애플리케이션과 관련해서 갖고 있는 하나 이상의 권한을 결정할 수 있다. 예컨대, 서버는 전자 장치 및/또는 전자 장치의 사용자가 영구 라이센스 또는 플로팅 라이센스를 포함하는지를 결정할 수 있다.

[0076] 블록 410에서, 전자 장치는 보안 암호화 통신 채널을 거쳐서 서버로부터 복호화 키를 수신할 수 있고, 블록 412에서, 전자 장치는 복호화 키를 사용하여 제 2 부분의 암호화 부분을 복호화할 수 있다. 예컨대, 서버에 의한 권한의 검증 및 결정에 기초하여, 전자 장치는 보안 암호화 통신 채널을 거쳐서 서버로부터 복호화 키를 수신할 수 있다. 그 후에 전자 장치는 복호화 키를 사용하여 하드웨어 기반 보안 격리 영역 내에서 암호화 부분을 복호화할 수 있다. 예컨대, 전자 장치(예를 들면, 프로세서)는 복호화 키를 사용하여 전자 장치에게 암호화 부분을 복호화하게 하는 평문 부분에 포함된 컴퓨터 판독가능 인스트럭션을 실행할 수 있다.

[0077] 그 후에, 일부 예에서, 전자 장치가 애플리케이션을 실행할 수 있음을 유의해야 한다. 예컨대, 전자 장치(예를

들면, 프로세서)는 컴퓨터 메모리로부터 애플리케이션의 제 1 부분을 실행하고, 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서 평문 부분 및 복호화 부분의 양쪽을 실행할 수 있다. 일부 예에서, 애플리케이션의 제 1 부분은 실행시에 하드웨어 기반 보안 격리 영역 내에서 애플리케이션의 제 2 부분에 대한 호출을 행할 수 있다.

[0078] 일부 예에서, 애플리케이션의 실행시에 애플리케이션의 제 2 부분이 불법 행위를 방지할 수 있음을 또한 유의해야 한다. 예컨대, 애플리케이션의 제 2 부분(예를 들면, 암호화 부분)은 애플리케이션의 제 1 부분의 코드가 올바르게 실행되고 있는지를 주기적으로 결정하는 코드를 포함할 수 있다. 제 1 부분의 코드가 올바르게 실행되고 있는지를 결정하는 것은 전자 장치의 사용자에 의해 코드가 수정되었었는지를 결정하는 것을 포함할 수 있다. 추가적으로 또는 이와는 달리, 일부 예에서, 애플리케이션의 제 2 부분(예를 들면, 암호화 부분)은 애플리케이션의 악의적인 사용자가 불법 행위시에 수정하는 코드를 포함할 수 있다. 하드웨어 기반 보안 격리 영역에 코드를 배치함으로써, 악의적인 사용자가 불법 행위를 위해 코드를 수정하는 데 제한을 받는다.

[0079] 도 5는 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서 애플리케이션의 부분을 실행하는 전자 장치의 예시적인 방법의 흐름도(500)이다. 블록 502에서, 전자 장치는 서버와 통신 채널을 수립할 수 있다.

[0080] 블록 504에서, 전자 장치는 통신 채널을 거쳐서 서버로부터 복호화 키를 수신할 수 있다. 예컨대, 전자 장치는 서버와 통신 채널을 수립하는 데 애플리케이션의 부분을 사용할 수 있다. 애플리케이션의 부분은 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 저장된 평문 부분을 포함할 수 있다. 일부 예에서, 평문 부분은 서버로부터 복호화 키를 다운로드하기 위해 전자 장치가 사용하는 표준 라이센스 코드를 포함한다.

[0081] 블록 506에서, 전자 장치는 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서, 복호화 키를 사용하여 애플리케이션의 암호화 부분을 복호화할 수 있다. 예컨대, 전자 장치는 하드웨어 기반 보안 격리 영역에 애플리케이션의 암호화 부분을 저장할 수 있다. 그 후에 전자 장치는 하드웨어 기반 보안 격리 영역 내에서 암호화 부분을 복호화하는 데 복호화 키를 사용할 수 있다. 일부 예에서, 전자 장치의 오퍼레이팅 시스템, 하이퍼바이저, 및/또는 펌웨어가 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서 애플리케이션의 복호화 부분을 액세스하는 데 제한을 받는다.

[0082] 그 후에, 일부 예에서, 전자 장치가 애플리케이션을 실행할 수 있음을 유의해야 한다. 예컨대, 암호화 부분을 복호화한 후에, 전자 장치는 하드웨어 기반 보안 격리 영역 내에서 애플리케이션의 부분을 실행할 수 있다. 추가적으로, 전자 장치는 하드웨어 기반 보안 격리 영역의 외부에 저장되는 애플리케이션의 임의의 부분을 실행할 수 있다.

[0083] 도 6은 복호화 키를 보안화하는 데 하드웨어 기반 보안 격리 기술을 이용하는 예시적인 방법의 흐름도(600)이다. 전자 장치는 서버로부터 영구 라이센스를 전자 장치가 수신할 때에 도 6의 방법을 수행할 수 있다. 복호화 키를 안전하게 저장함으로써, 전자 장치는 오프라인 모드에서 애플리케이션을 실행할 수 있다.

[0084] 블록 602에서, 하드웨어 기반 보안 격리 기술은 전자 장치로 하여금 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서 실링 키를 생성하게 할 수 있다. 예컨대, 전자 장치의 프로세서는 프로세서로 하여금 하드웨어 기반 보안 격리 영역 내에서 실링 키를 생성하게 하는 하드웨어 기반 보안 격리 영역에 포함된 컴퓨터 판독가능 인스트럭션(예를 들면, 코드)을 실행할 수 있다. 일부 예에서, 전자 장치는 전자 장치의 프로세서 및/또는 하드웨어 기반 보안 격리 영역에 기초하여 실링 키를 생성한다. 이러한 예에서, 프로세서 및 하드웨어 기반 보안 격리 영역을 포함하는 전자 장치만이 동일한 실링 키를 생성할 수 있다.

[0085] 블록 604에서, 전자 장치의 하드웨어 기반 보안 격리 기술은 실링 키를 사용하여 복호화 키를 암호화할 수 있고, 블록 606에서, 하드웨어 기반 보안 격리 기술은 전자 장치로 하여금 암호화된 복호화 키를 컴퓨터 메모리에 저장하게 할 수 있다. 예컨대, 전자 장치는 하드웨어 기반 보안 격리 영역 내에 저장되는 애플리케이션의 평문 부분 내에 포함된 컴퓨터 판독가능 인스트럭션을 실행할 수 있고, 여기서 컴퓨터 판독가능 인스트럭션은 전자 장치로 하여금 하드웨어 기반 보안 격리 영역 내에서 복호화 키를 암호화하도록 하게 한다. 그 후에 전자 장치는 암호화된 복호화 키를 컴퓨터 메모리에 저장할 수 있다. 일부 예에서, 전자 장치는 암호화된 복호화 키를 비휘발성 메모리에 저장한다.

[0086] 오프라인 모드에서 애플리케이션을 실행하기 위해, 하드웨어 기반 보안 격리 기술이 저장 및 암호화된 복호화 키를 컴퓨터 메모리로부터 불러올 수 있음을 유의해야 한다. 그러면 전자 장치는 실링 키를 사용하여 하드웨어 기반 보안 격리 영역 내에서 암호화된 복호화 키를 복호화할 수 있고, 또한 애플리케이션의 암호화 부분을 복호화하는 데 복호화 키를 사용할 수 있다.

[0087] 도 7은 애플리케이션과 연관된 플로팅 권한을 이용하는 전자 장치의 예시적인 방법의 흐름도(700)이다. 일부 예에서, 플로팅 권한은 전자 장치의 사용자를 따르는 플로팅 라이센스를 포함할 수 있다. 예컨대, 사용자가 전자 장치를 사용하여 서버에 인증서(예를 들면, 사용자명 및 패스워드)를 제공할 때마다, 서버는 애플리케이션을 실행하기 위해 플로팅 라이센스를 전자 장치에 전송할 수 있다.

[0088] 블록 702에서, 전자 장치는 애플리케이션에 대한 플로팅 권한과 연관된 인스트럭션을 서버로부터 수신할 수 있다. 예컨대, 전자 장치는 애플리케이션에 대한 복호화 키와 함께 인스트럭션을 서버로부터 수신할 수 있다. 일부 예에서, 플로팅 권한은 애플리케이션에 대한 플로팅 라이센스를 포함한다. 이러한 예에서, 인스트럭션은 전자 장치의 하드웨어 기반 보안 격리 영역이 서버와 연속적으로 및/또는 주기적으로 통신하게 하여 플로팅 라이센스가 여전히 유효한지를 결정할 수 있다.

[0089] 블록 704에서, 전자 장치는 컴퓨터 메모리에 저장된 애플리케이션의 제 1 부분 및 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 저장된 애플리케이션의 제 2 부분을 사용하여 애플리케이션을 실행할 수 있다. 일부 예에서, 애플리케이션의 제 1 부분은 평문을 포함하고, 애플리케이션의 제 2 부분은 평문 부분 및 암호화 부분을 포함한다. 이러한 예에서, 평문 부분은 복호화 키를 사용하여 암호화 부분을 복호화함으로써, 전자 장치는 애플리케이션을 실행할 수 있다.

[0090] 블록 706에서, 하드웨어 기반 보안 격리 영역은 플로팅 권한이 여전히 유효한지를 결정하기 위해 서버와 통신할 수 있다. 예컨대, 일부 예에서, 플로팅 권한은 전자 장치의 사용자가 한 번에 단일 전자 장치에서만 애플리케이션을 실행할 수 있음을 특정할 수 있다. 이러한 예에서, 하드웨어 기반 보안 격리 영역은 서버와 주기적으로(예를 들면, 매분, 매시간, 등) 통신하여 사용자가 애플리케이션을 실행하는 데 다른 전자 장치를 사용하고 있는지를 결정할 수 있다. 사용자가 애플리케이션을 실행하는 데 다른 전자 장치를 사용하고 있다고 서버가 결정하면, 서버는 전자 장치에 대한 플로팅 권한이 더이상 유효하지 않다고 결정할 수 있다. 그러나, 사용자가 애플리케이션 실행을 위해 다른 전자 장치를 사용하고 있지 않으면, 서버는 전자 장치에 대한 플로팅 권한이 여전히 유효하다고 결정할 수 있다.

[0091] 블록 708에서, 하드웨어 기반 보안 격리 영역은 플로팅 권한이 유효하지 않다는 것에 기초하여 전자 장치로 하여금 제 2 부분의 실행을 종료하게 할 수 있고, 블록 710에서, 하드웨어 기반 보안 격리 영역은 플로팅 권한이 여전히 유효하다는 것에 기초하여 전자 장치로 하여금 애플리케이션의 제 2 부분을 계속해서 실행하게 할 수 있다.

[0092] 추가적으로, 플로팅 라이센스가 여전히 유효하면, 블록 712에서, 하드웨어 기반 보안 격리 영역은 서버와 계속해서 통신하여 플로팅 권한이 지연 후에 여전히 유효한지를 결정할 수 있다. 일부 예에서, 지연은 매분, 매시간, 등과 같은 주기적인 지연을 포함할 수 있다. 서버와 통신하고 있는 경우, 하드웨어 기반 보안 격리 영역은 플로팅 권한이 더는 유효하지 않다는 것에 기초하여 애플리케이션의 실행을 종료할 수 있거나(블록 708), 플로팅 권한이 유효하다는 것에 의해 애플리케이션의 실행을 계속할 수 있다(블록 710).

[0093] 도 8은 본 명세서에서 설명되는 전자 장치에서 하드웨어 기반 보안 격리 기술을 검증하는 서버의 제 1 예시적 방법에 대한 흐름도(800)이다. 블록 802에서, 서버는 전자 장치로부터 데이터를 수신할 수 있다. 예컨대, 일부 예에서, 서버는 전자 장치의 CPU 칩에 대한 식별자, 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실제로 실행되고 있다는 증거, 및/또는 하드웨어 기반 보안 격리 영역의 다이제스트와 같은 입증 정보를 전자 장치로부터 수신할 수 있다.

[0094] 블록 804에서, 서버는 데이터를 사용하여, 전자 장치가 하드웨어 기반 보안 격리 기술을 실행하도록 구성되어 있는지를 결정할 수 있다. 예컨대, 서버는 전자 장치가 CPU에 대한 식별자를 사용하여 보안 격리 기술을 갖는 신뢰되는 CPU를 포함하고 있는지를 결정할 수 있다. 일부 예에서, 전자 장치가 하드웨어 기반 보안 격리 기술을 포함하는지를 결정하기 위해, 서버는 정보를 저장하는 데이터베이스를 사용하여 하드웨어 기반 보안 격리 기술과 CPU 칩을 연관시킬 수 있다.

[0095] 블록 806에서, 서버는 데이터를 사용하여, 전자 장치의 하드웨어 기반 보안 격리 영역이 애플리케이션의 적어도 일부를 포함하는지를 결정할 수 있다. 예컨대, 서버는 하드웨어 기반 보안 격리 영역의 다이제스트가 허가받은 애플리케이션에 매칭되는지를 결정할 수 있다. 일부 예에서, 서버는 애플리케이션(및/또는 애플리케이션의 일부)이 하드웨어 기반 보안 격리 기술(예를 들면, 하드웨어 기반 보안 격리 영역)로 실제로 실행되고 있는지를 결정하기 위해 (데이터로부터의) 하드웨어 기반 보안 격리 기술의 다이제스트를 사용할 수 있다.

[0096] 블록 808에서, 서버는 애플리케이션과 연관된 복호화 키를 전자 장치에 전송한다. 일부 예에서, 서버는 라이센

스가 플로팅 라이센스를 포함하는 경우에 애플리케이션에 대응하는 인스트럭션을 전자 장치에 추가로 전송할 수 있다.

[0097] 도 9는 전자 장치 상에서 하드웨어 기반 보안 격리 기술을 검증하는 서버의 예시적인 방법에 대한 흐름도(900)이다. 블록 902에서, 서버는 전자 장치로부터 데이터를 수신할 수 있다. 예컨대, 일부 예에서, 서버는 전자 장치로부터 입증 정보, 예를 들어 전자 장치의 CPU 칩에 대한 식별자, 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실제로 실행되고 있다는 증거, 및/또는 하드웨어 기반 보안 격리 영역의 다이제스트를 수신할 수 있다.

[0098] 블록 904에서, 서버는 전자 장치가 하드웨어 기반 보안 격리 기술을 갖는 신뢰되는 CPU를 포함하고 있는지를 결정한다. 일부 예에서, 서버는 전자 장치가 데이터베이스를 사용하여 하드웨어 기반 보안 격리 기술을 갖는 신뢰되는 CPU를 포함하고 있는지를 결정한다. 데이터베이스는 정보를 저장하여, 전자 장치 상에서 하드웨어 기반 보안 격리 기술과 CPU 칩을 연관시킬 수 있다. 블록 904에서 서버가 아니오라고 결정하면, 방법은 서버가 애플리케이션과 연관된 복호화 키를 전자 장치로 전송하지 않는 블록 906으로 진행된다. 그러나, 블록 904에서 서버가 예라고 결정하면, 방법은 블록 908로 진행된다.

[0099] 블록 908에서, 서버는 전자 장치 상의 하드웨어 기반 보안 격리 기술의 다이제스트가 허가받은 애플리케이션에 매칭되는지를 결정한다. 예컨대, 서버는 애플리케이션(및/또는 애플리케이션의 일부)이 하드웨어 기반 보안 격리 기술(예를 들면, 하드웨어 기반 보안 격리 영역)로 실제로 실행되고 있는지를 결정하는 데 (데이터로부터의) 하드웨어 기반 보안 격리 기술의 다이제스트를 사용할 수 있다. 블록 908에서 서버가 아니로로 결정하면, 방법은 서버가 애플리케이션과 연관된 복호화 키를 전자 장치로 전송하지 않는 블록 906으로 진행된다. 그러나, 블록 908에서 서버가 예라고 결정하면, 방법은 블록 910으로 진행된다.

[0100] 블록 910에서, 서버는 전자 장치의 사용자 및/또는 전자 장치가 애플리케이션을 사용하기 위한 라이센스를 갖고 있는지를 결정한다. 예컨대, 일부 예에서, 서버는 전자 장치의 사용자 및/또는 전자 장치가 애플리케이션에 대한 라이센스를 포함하는지를 결정한다. 일부 예에서, 서버는 전자 장치의 사용자 및/또는 전자 장치가 영구 라이센스를 포함하고 있다고 결정할 수 있는 반면에, 다른 예에서 서버는 전자 장치의 사용자 및/또는 전자 장치가 플로팅 라이센스를 포함하고 있다고 결정할 수 있다. 블록 910에서 서버가 아니오라고 결정하면, 방법은 서버가 애플리케이션과 연관된 복호화 키를 전자 장치로 전송하지 않는 블록 906으로 진행된다. 그러나, 블록 910에서 서버가 예로 결정하면, 방법은 블록 912로 진행된다.

[0101] 블록 912에서 서버는 애플리케이션과 연관된 복호화 키를 전자 장치에 전송한다. 일부 예에서, 서버는 라이센스가 플로팅 라이센스를 포함하는 경우에 애플리케이션에 대응하는 인스트럭션을 전자 장치에 추가로 전송할 수 있다.

[0102] 도 10은 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하는 제 1 예시적 방법에 대한 흐름도(1000)이다. 블록 1002에서, 전자 장치는 전자 장치의 하드웨어 기반 보안 격리 영역 내부에 보안 코드를 저장할 수 있다. 예컨대, 전자 장치는 전자 장치 상에서 실행되고 있는 애플리케이션의 코드를 모니터링하는 데 전자 장치가 사용하는 보안 코드를 저장할 수 있다. 일부 예에서, 보안 코드는 전자 장치가 모니터링하고 있는 애플리케이션의 일부를 포함할 수 있다.

[0103] 블록 1004에서, 전자 장치는 애플리케이션을 실행할 수 있고, 블록 1006에서, 전자 장치는 보안 코드를 사용하여 애플리케이션의 코드를 모니터링할 수 있다. 예컨대, 전자 장치는 (1) 애플리케이션이 적절하게 실행되고 있는지를 결정하고, (2) 코드 변수를 검사하여 변수가 올바른지를 결정하고, 및/또는 (3) 애플리케이션의 코드의 상이한 부분을 검사하는 데 보안 코드를 사용할 수 있다. 일부 예에서, 전자 장치는 주기적인 실행시에 애플리케이션을 모니터링할 수 있다. 예컨대, 전자 장치는 애플리케이션이 매초, 매분, 등 적절하게 실행되고 있는지를 결정할 수 있다.

[0104] 도 11은 불법 행위를 방지하는 데 하드웨어 기반 보안 격리 기술을 이용하는 제 2 예시적 방법에 대한 흐름도이다. 블록 1102에서, 전자 장치 및/또는 개발자는 전자 장치의 하드웨어 기반 보안 격리 영역에 저장할 애플리케이션의 데이터 부분을 결정할 수 있고, 블록 1104에서, 전자 장치는 애플리케이션의 데이터 부분을 하드웨어 기반 보안 격리 영역에 저장할 수 있다. 예컨대, 애플리케이션의 데이터 부분은 악의적인 사용자가 불법 행위를 위해 조작할 가능성이 높은 데이터를 포함할 수 있다. 일부 예에서, 애플리케이션의 데이터 부분은 애플리케이션의 변수 데이터를 포함할 수 있다. 예컨대, 게임의 상태가 사용자의 건강 레벨을 포함하는 게임을 애플리케이션이 포함하고 있으면, 전자 장치는 건강 레벨과 연관된 변수 데이터를 하드웨어 기반 보안 격리 영역에

저장할 수 있다.

[0105] 예시적인 조항

[0106] A: 전자 장치의 컴퓨터 메모리에 애플리케이션의 제 1 부분을 저장하는 단계와; 전자 장치의 컴퓨터 메모리의 보안 격리 영역에 애플리케이션의 제 2 부분을 저장하는 단계 - 상기 애플리케이션의 제 2 부분은 암호화 부분 및 평문 부분을 포함함 - 와; 평문 부분을 사용하여, 서버와 보안 암호화 통신 채널을 수립하는 단계와; 보안 암호화 통신 채널을 사용하여, 서버로 데이터를 전송하는 단계와; 데이터 전송에 적어도 부분적으로 기초하여, 보안 암호화 통신 채널을 사용하여, 서버로부터 복호화 키를 수신하는 단계와; 복호화 키를 사용하여 암호화 부분을 복호화하는 단계를 포함하는 방법.

[0107] B: 단락 A에 기재된 방법으로서, 데이터는 전자 장치가 신뢰되는 CPU 칩 및 보안 격리 영역을 포함하고 있는지를 서버에게 검증하도록 하게 하는 입증 정보(attestation information)를 포함한다.

[0108] C: 단락 B에 기재된 방법으로서, 입증 정보는 CPU 칩에 대한 식별자, 전자 장치가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실제 실행되고 있다는 증거, 또는 보안 격리 영역의 다이제스트 중 적어도 하나를 포함한다.

[0109] D: 단락 A-C 중 어느 하나에 기재된 방법으로서, 애플리케이션의 제 1 부분, 제 2 부분의 평문 부분, 및 제 2 부분의 복호화 부분을 사용하여 애플리케이션을 실행하는 단계를 더 포함한다.

[0110] E: 단락 A-D 중 어느 하나에 기재된 방법으로서, 보안 격리 영역을 사용하여, 실링 키를 생성하는 단계와; 실링 키를 사용하여 복호화 키를 암호화하는 단계를 더 포함한다.

[0111] F: 단락 E에 기재된 방법으로서, 암호화된 복호화 키를 비휘발성 메모리에 저장하는 단계를 더 포함한다.

[0112] G: 단락 A-F 중 어느 하나에 기재된 방법으로서, 평문 부분은 서버로부터 복호화 키를 불러오기 위한 라이센싱 코드를 포함한다.

[0113] H: 단락 A-G 중 어느 하나에 기재된 방법으로서, 암호화된 부분은 애플리케이션의 사용에 중요한 코드를 포함한다.

[0114] I: 단락 A-H 중 어느 하나에 기재된 방법으로서, 서버로부터 인스트럭션을 수신하는 단계를 더 포함하고, 상기 인스트럭션은 보안 격리 영역이 종료되어야 하는지를 결정하기 위해 보안 격리 영역으로 하여금 서버와 주기적으로 통신하게 한다.

[0115] J: 저장된 컴퓨터 실행가능 인스트럭션을 갖는 메모리로서, 컴퓨터 실행가능 인스트럭션은 단락 A-J 중 어느 하나에 기재된 방법을 수행하도록 전자 장치를 구성한다.

[0116] K: 적어도 하나의 프로세싱 유닛과; 적어도 하나의 프로세싱 유닛에 의한 실행시에, 단락 A-J 중 어느 하나에 기재된 방법을 수행하도록 장치를 구성하는 컴퓨터 실행가능 인스트럭션을 갖는 컴퓨터 메모리를 포함하는 장치.

[0117] L: 적어도 하나의 프로세서와; 메모리를 포함하는 전자 장치로서, 상기 메모리는 애플리케이션의 제 1 부분, 및 애플리케이션의 제 2 부분을 메모리의 보안 격리 영역에 저장하고, 상기 제 2 부분은 추출로부터 애플리케이션을 안전하게 하기 위한 암호화 부분 및 서버와의 통신 채널을 오픈하기 위한 평문 부분을 포함하고, 상기 평문 부분은, 적어도 하나의 프로세서에 의한 실행시에, 적어도 하나의 프로세서로 하여금, 서버와 통신 채널을 수립하고; 통신 채널을 거쳐서 서버로부터 애플리케이션과 연관된 복호화 키를 수신하며; 암호화 부분을 복호화 키를 사용하여 복호화하도록 하게 하는 컴퓨터 판독가능 인스트럭션을 포함한다.

[0118] M: 단락 L에 기재된 장치로서, 보안 격리 영역은, 적어도 하나의 프로세서에 의한 실행시에, 적어도 하나의 프로세서로 하여금, 통신 채널을 거쳐서 서버로 데이터를 전송하도록 하게 하는 컴퓨터 판독가능 인스트럭션을 포함하고, 데이터는 전자 장치가 보안 격리 기술을 포함하는지를 서버가 검증할 수 있게 하는 입증 정보를 포함한다.

[0119] N: 단락 M에 기재된 장치로서, 입증 정보는 프로세서에 대한 식별자, 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실제로 실행되고 있다는 증거, 및 보안 격리 영역의 다이제스트 중 적어도 하나를 포함한다.

[0120] O: 단락 L-N 중 어느 하나에 기재된 장치로서, 컴퓨터 판독가능 인스트럭션은 또한, 적어도 하나의 프로세서에

의한 실행시에, 적어도 하나의 프로세서로 하여금, 보안 격리 영역에 의해 생성된 실링 키를 사용하여 복호화 키를 암호화하도록 하게 한다.

[0121] P: 단락 O에 기재된 장치로서, 컴퓨터 판독가능 인스트럭션은 또한, 적어도 하나의 프로세서에 의한 실행시에, 적어도 하나의 프로세서로 하여금, 암호화된 복호화 키를 비휘발성 메모리에 저장하도록 하게 한다.

[0122] Q: 단락 L-P 중 어느 하나에 기재된 장치로서, 컴퓨터 판독가능 인스트럭션은 또한, 적어도 하나의 프로세서에 의한 실행시에, 적어도 하나의 프로세서로 하여금, 통신 채널을 거쳐서 서버로부터 인스트럭션을 수신 - 상기 인스트럭션은 서버와 통신하기 위한 시간 간격을 포함함 - 하도록 하게 하고; 시간 간격에 적어도 일부 기초하여, 애플리케이션에 대한 라이센스가 여전히 유효한지를 결정하기 위해 서버와 통신하도록 하게 한다.

[0123] R: 하나 이상의 프로세서와; 하나 이상의 프로세서에 의한 실행시에, 하나 이상의 프로세서로 하여금, 전자 장치로부터 데이터를 수신 - 상기 데이터는 적어도 전자 장치의 CPU 칩의 식별자, 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실제로 실행되고 있다는 증거, 및 보안 격리 영역의 다이제스트를 포함함 - 하고: 전자 장치의 코드가 하드웨어 기반 보안 격리 기술을 지원하는 장치 상에서 실제로 실행되고 있다는 증거를 사용하여, 전자 장치가 보안 격리 기술을 실행하도록 구성되어 있는지를 결정하고: 보안 격리 영역의 다이제스트를 사용하여, 전자 장치의 보안 격리 영역이 적어도 애플리케이션의 일부를 포함하는지를 결정하고, 전자 장치로 복호화 키를 전송하도록 하게 하는 컴퓨터 실행가능 인스트럭션을 저장하는 메모리를 포함하는 시스템.

[0124] S: 단락 R에 기재된 시스템으로서, 컴퓨터 판독가능 인스트럭션은 또한, 하나 이상의 프로세서에 의한 실행시에, 하나 이상의 프로세서로 하여금, 전자 장치가 애플리케이션을 실행하기 위한 라이센스를 갖고 있는지를 결정하도록 하게 한다.

[0125] T: 단락 S에 기재된 시스템으로서, 동작들에 전자 장치로 인스트럭션을 전송하는 것이 더 포함되고, 인스트럭션은 라이센스가 전자 장치에서 여전히 유효한지를 보안 격리 영역에 대해 주기적으로 검사하도록 하게 한다.

[0126] U: 단락 R-T 중 어느 하나에 기재된 시스템으로서, 데이터를 수신하는 것은 보안 격리 영역과 서버 간의 보안 암호화 통신 채널을 거쳐서 데이터를 수신하는 것을 포함하고, 복호화 키를 전송하는 것은 보안 암호화 통신 채널을 거쳐서 복호화 키를 전송하는 것을 포함한다.

[0127] V: 단락 R-U 중 어느 하나에 기재된 시스템으로서, 보안 격리 영역의 다이제스트는 애플리케이션의 평문 부분 및 애플리케이션의 암호화 부분을 포함한다.

[0128] W: 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역 내에서 실링 키를 생성하는 단계와; 하드웨어 기반 보안 격리 영역 내에서 실링 키를 사용하여 복호화 키를 암호화하는 단계와; 암호화된 복호화 키를 컴퓨터 메모리에 저장하는 단계를 포함하는 방법.

[0129] X: 단락 W에 기재된 방법을 수행하도록 전자 장치를 구성하는 컴퓨터 실행가능 인스트럭션을 갖는 메모리.

[0130] Y: 적어도 하나의 프로세싱 유닛과; 적어도 하나의 프로세싱 유닛에 의한 실행시에, 단락 W에 기재된 방법을 장치가 수행하도록 구성하는 컴퓨터 실행가능 인스트럭션을 갖는 메모리를 포함하는 장치.

[0131] Z: 서버로부터, 애플리케이션에 대한 플로팅 권한과 연관된 인스트럭션을 수신하는 단계와; 컴퓨터 메모리에 저장된 애플리케이션의 제 1 부분 및 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 저장된 애플리케이션의 제 2 부분을 사용하여 애플리케이션을 실행하는 단계와; 플로팅 권한이 여전히 유효한지를 결정하기 위해 서버와 통신하는 단계와; 플로팅 권한이 유효하지 않다는 것에 적어도 일부 기초하여 애플리케이션의 제 2 부분의 실행을 종료하는 것, 또는 플로팅 권한이 유효하다는 것에 적어도 일부 기초하여 애플리케이션을 계속해서 실행하는 것 중 적어도 하나를 수행하는 단계를 포함하는 방법.

[0132] AA: 단락 Z에 기재된 방법을 수행하도록 전자 장치를 구성하는 컴퓨터 실행가능 인스트럭션을 갖는 메모리.

[0133] AB: 적어도 하나의 프로세싱 유닛과; 적어도 하나의 프로세싱 유닛에 의한 실행시에, 단락 Z에 기재된 방법을 수행하도록 장치를 구성하는 컴퓨터 실행가능 인스트럭션을 갖는 메모리를 포함하는 장치.

[0134] AC: 전자 장치의 하드웨어 기반 보안 격리 영역 내부에 보안 코드를 저장하는 단계와; 애플리케이션을 실행하는 단계와; 보안 코드를 사용하여 애플리케이션의 코드를 모니터링하는 단계를 포함하는 방법.

[0135] AD: 단락 AC에 기재된 방법을 수행하도록 전자 장치를 구성하는 컴퓨터 실행가능 인스트럭션을 갖는 메모리.

[0136] AE: 적어도 하나의 프로세싱 유닛과; 적어도 하나의 프로세싱 유닛에 의한 실행시에, 단락 AC에 기재된 방법을 수행하도록 장치를 구성하는 컴퓨터 실행가능 인스트럭션을 갖는 메모리를 포함하는 장치.

[0137] 결론

[0138] 본 기술은 구조적 특징들 및/또는 방법론적 행위들에 대해 특정한 언어로 설명되었지만, 첨부된 청구범위가 설명되는 특징들 또는 행위들로 반드시 제한되지 않음 이해해야 한다. 또한, 특징들 및 행위들은 이러한 기술의 예시적인 구현예로서 설명된다.

[0139] 예시적인 프로세스들의 동작은 개별적인 블록들에서 도시되고, 그 블록들을 참조하여 요약된다. 프로세스들은 블록들의 논리적 흐름들로서 도시되고, 각 블록은 하드웨어, 소프트웨어, 또는 그 조합으로 구현될 수 있는 하나 이상의 동작을 나타낼 수 있다. 소프트웨어와 관련하여, 동작들은, 하나 이상의 프로세서에 의한 실행시에, 하나 이상의 프로세서들로 하여금, 상기한 동작들을 수행하게 할 수 있는 하나 이상의 컴퓨터 메모리에 저장된 컴퓨터 실행가능 인스트럭션을 나타낸다. 일반적으로, 컴퓨터 실행가능 인스트럭션은 특정한 기능을 수행하거나 특정한 추상적 데이터 형태를 구현하는 루틴, 프로그램, 오브젝트, 모듈, 컴포넌트, 데이터 구조, 등을 포함한다. 동작들이 설명되는 순서는 제한적으로 해석되도록 의도되지 않으며, 임의의 개수의 설명되는 동작들은 임의의 순서로 실행되고, 임의의 순서로 조합되고, 다수의 서브 동작들로 세분화되고, 및/또는 설명되는 프로세스들을 구현하기 위해 병렬로 실행될 수 있다. 설명되는 프로세스들은 하나 이상의 내부 또는 외부 CPU 또는 GPU와 같은 하나 이상의 장치(들)(106, 120, 200, 및/또는 300)와 연관된 리소스, 및/또는 FPGA, DSP, 또는 다른 형태의 가속기와 같은 하드웨어 로직의 하나 이상의 부품들에 의해 수행될 수 있다.

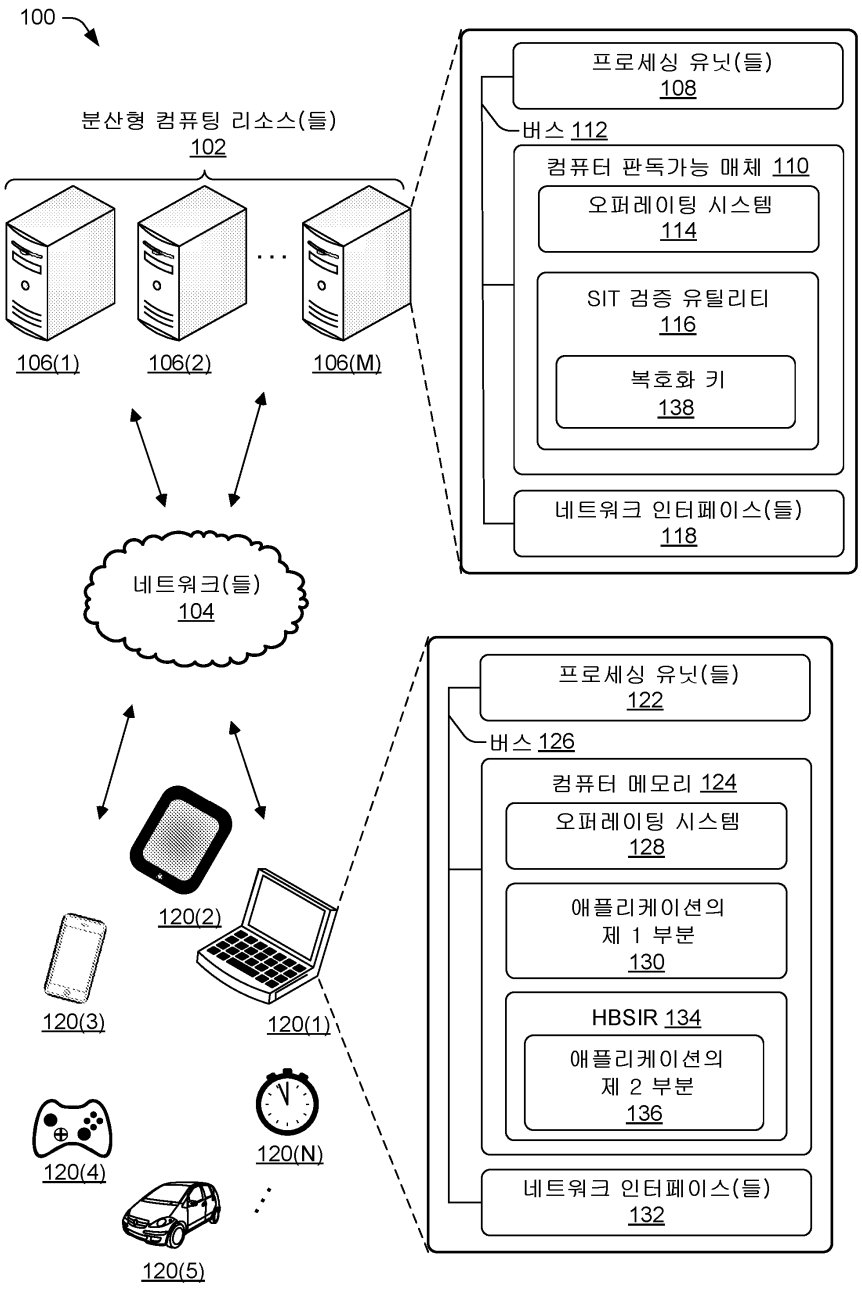
[0140] 상기한 모든 방법들 및 프로세스들은 하나 이상의 범용 컴퓨터 또는 프로세서에 의해 실행되는 소프트웨어 코드 모듈을 통해 실시될 수 있고, 또한 완전히 자동화될 수 있다. 코드 모듈은 임의의 형태의 컴퓨터 판독가능 저장 매체 또는 기타 컴퓨터 저장 장치에 저장될 수 있다. 방법들의 일부 또는 전부는 이와는 달리 특수한 컴퓨터 하드웨어로 실시될 수 있다.

[0141] "~할 수 있다", "~할 수 있었다", "~일 수도 있었다" 또는 "~일 수도 있다"와 같은 조건부 언어는, 달리 특별하게 언급되지 않는 한, 소정의 예들이 소정의 특징, 요소 및/또는 단계를 포함하지만 다른 예들에는 이들이 포함되지 않음을 나타내기 위한 문맥 내에서 이해된다. 따라서, 이러한 조건부 언어는, 소정의 특징, 요소 및/또는 단계가 하나 이상의 예들에 대해 임의의 방식으로 요구되는 것, 혹은 사용자 입력 또는 프롬프팅을 이용하거나 이용하지 않고서 소정의 특징, 요소 및/또는 단계가 임의의 특정한 예에 포함되거나 수행되는지 여부를 결정하기 위한 로직을 하나 이상의 예들이 반드시 포함한다는 것을 의미하도록 일반적으로 의도되지 않는다. "X, Y 또는 Z 중 적어도 하나"라는 구절과 같은 결합 언어는, 달리 특별하게 언급되지 않는 한, 항목, 용어 등이 X, Y 또는 Z 또는 이들의 조합일 수 있음을 나타내는 것으로 이해되어야 한다.

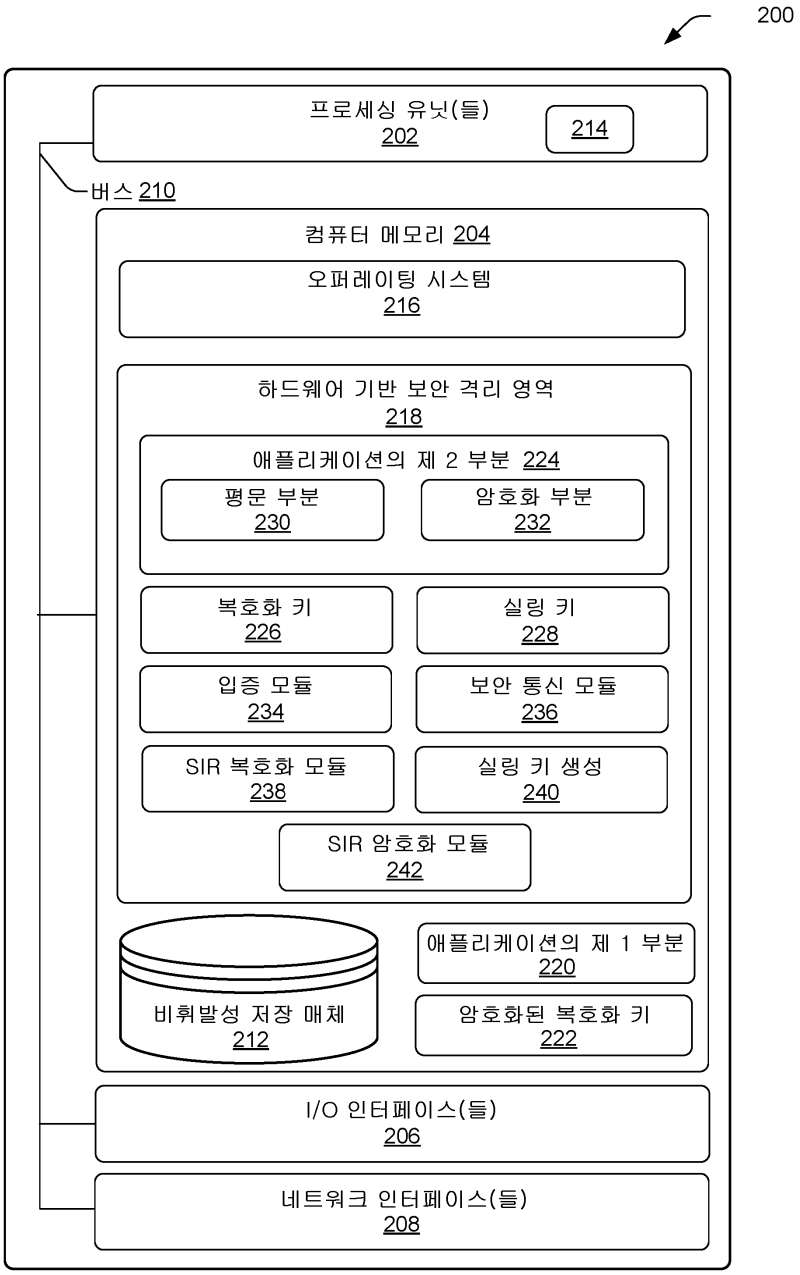
[0142] 본 명세서에서 설명되고 및/또는 첨부 도면에 도시되는 흐름도에서의 임의의 통상적인 설명, 요소 또는 블록은 특정한 논리적 기능 또는 요소를 관례에 따라 구현하기 위한 하나 이상의 실행가능 인스트럭션을 포함하는 모듈, 세그먼트, 또는 코드 부분을 잠재적으로 나타내는 것으로 이해되어야 한다. 다른 구현예들은, 당업자가 이해할 수 있는 바와 같이 관련 기능에 따라 실질적으로 동기적으로 또는 역순을 포함해서, 도시되거나 논의되는 것과는 다른 순서로 요소들 또는 기능들이 삭제 또는 실행될 수 있는 본 명세서에서 설명되는 예들의 범위 내에 포함된다. 다수의 변경 및 수정이 상기한 예들에 대해 이루어질 수 있는 것이 강조되어야 하고, 그 요소들은 다른 허용가능한 예들 중에 있는 것으로 이해되어야 한다. 이러한 모든 수정 및 변경은 본 발명의 범위 내에서 포함되고, 이하의 청구범위에 의해 보호되도록 의도된다.

도면

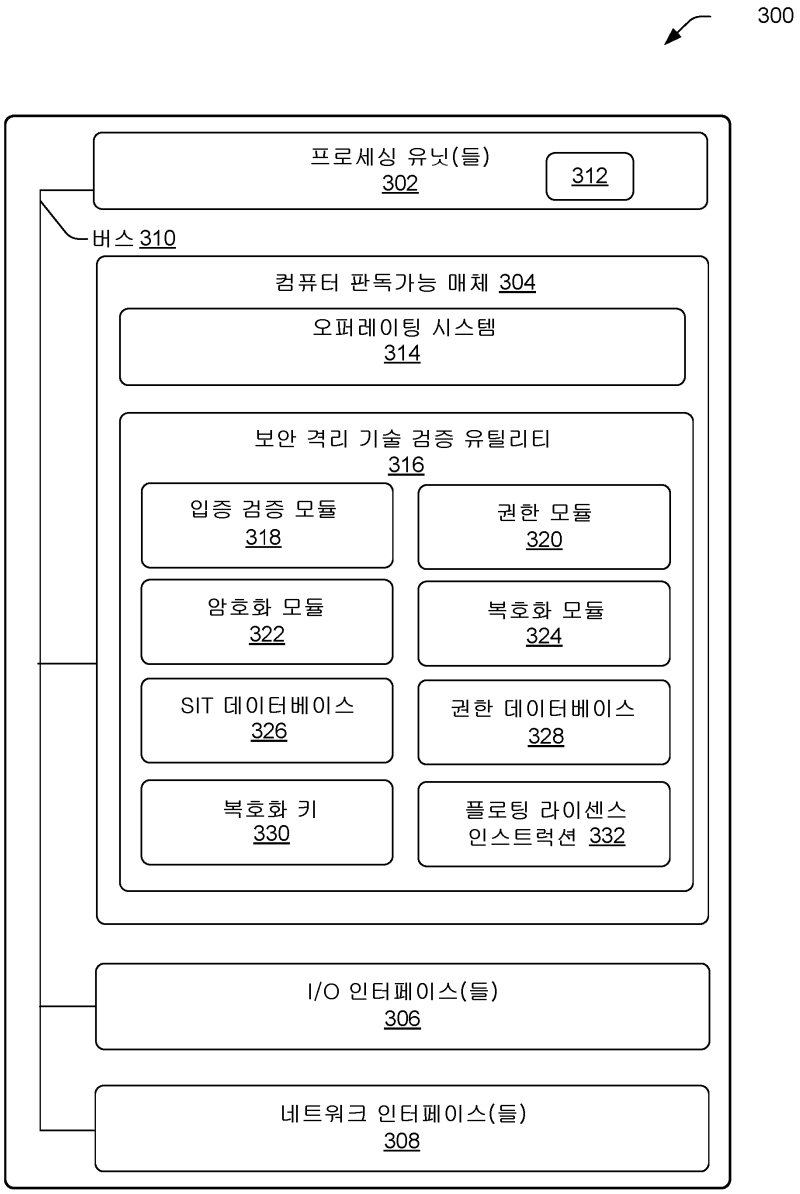
도면1


100
분산형 컴퓨팅 리소스(들)
102
106(1)
106(2)
106(M)
네트워크(들)
104
프로세싱 유닛(들)
108
버스 112
컴퓨터 판독가능 매체 110
오퍼레이팅 시스템
114
SIT 검증 유틸리티
116
복호화 키
138
네트워크 인터페이스(들)
118
120(1)
120(2)
120(3)
120(4)
120(5)
120(N)
프로세싱 유닛(들)
122
버스 126
컴퓨터 메모리 124
오퍼레이팅 시스템
128
애플리케이션의
제 1 부분
130
HBSIR 134
애플리케이션의
제 2 부분
136
네트워크 인터페이스(들)
132

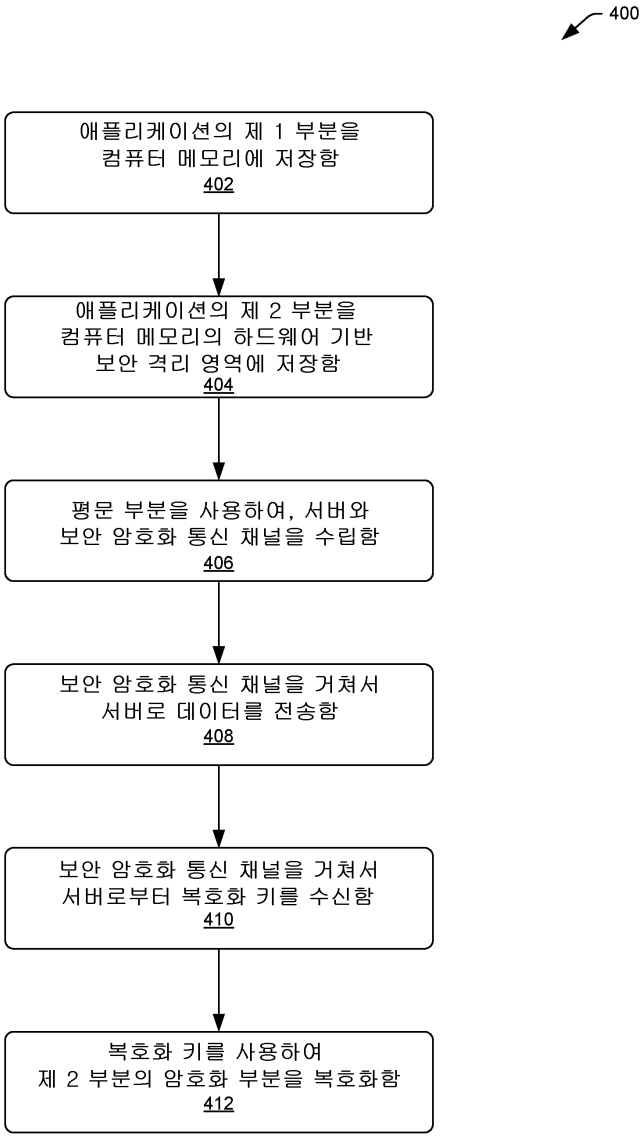
도면2


200
프로세싱 유닛(들)
202
214
버스 210
컴퓨터 메모리 204
오퍼레이팅 시스템
216
하드웨어 기반 보안 격리 영역
218
애플리케이션의 제 2 부분 224
평문 부분
230
암호화 부분
232
복호화 키
226
실링 키
228
입증 모듈
234
보안 통신 모듈
236
SIR 복호화 모듈
238
실링 키 생성
240
SIR 암호화 모듈
242
비휘발성 저장 매체
212
애플리케이션의 제 1 부분
220
암호화된 복호화 키
222
I/O 인터페이스(들)
206
네트워크 인터페이스(들)
208

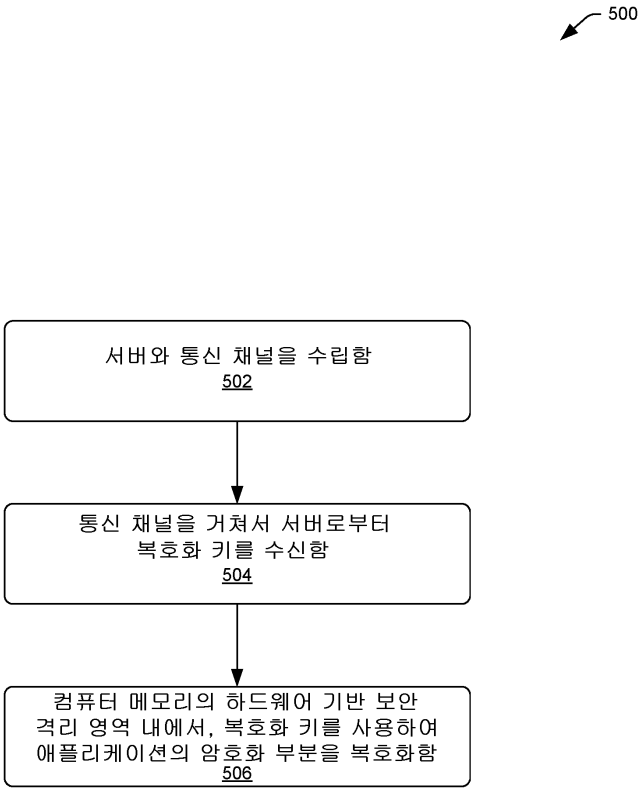
도면3


300
프로세싱 유닛(들)
302
312
버스 310
컴퓨터 판독가능 매체 304
오퍼레이팅 시스템
314
보안 격리 기술 검증 유틸리티
316
입증 검증 모듈
318
권한 모듈
320
암호화 모듈
322
복호화 모듈
324
SIT 데이터베이스
326
권한 데이터베이스
328
복호화 키
330
플로팅 라이센스
인스트럭션 332
I/O 인터페이스(들)
306
네트워크 인터페이스(들)
308

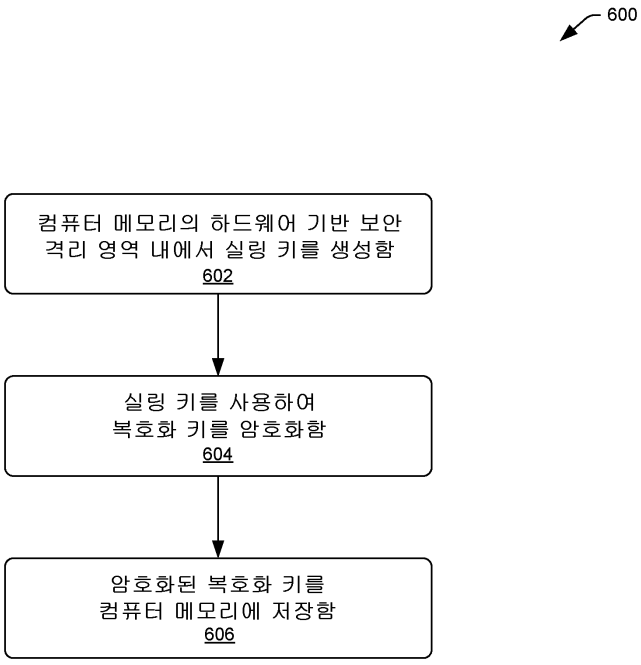
도면4


400
애플리케이션의 제 1 부분을
컴퓨터 메모리에 저장함
402
애플리케이션의 제 2 부분을
컴퓨터 메모리의 하드웨어 기반
보안 격리 영역에 저장함
404
평문 부분을 사용하여, 서버와
보안 암호화 통신 채널을 수립함
406
보안 암호화 통신 채널을 거쳐서
서버로 데이터를 전송함
408
보안 암호화 통신 채널을 거쳐서
서버로부터 복호화 키를 수신함
410
복호화 키를 사용하여
제 2 부분의 암호화 부분을 복호화함
412

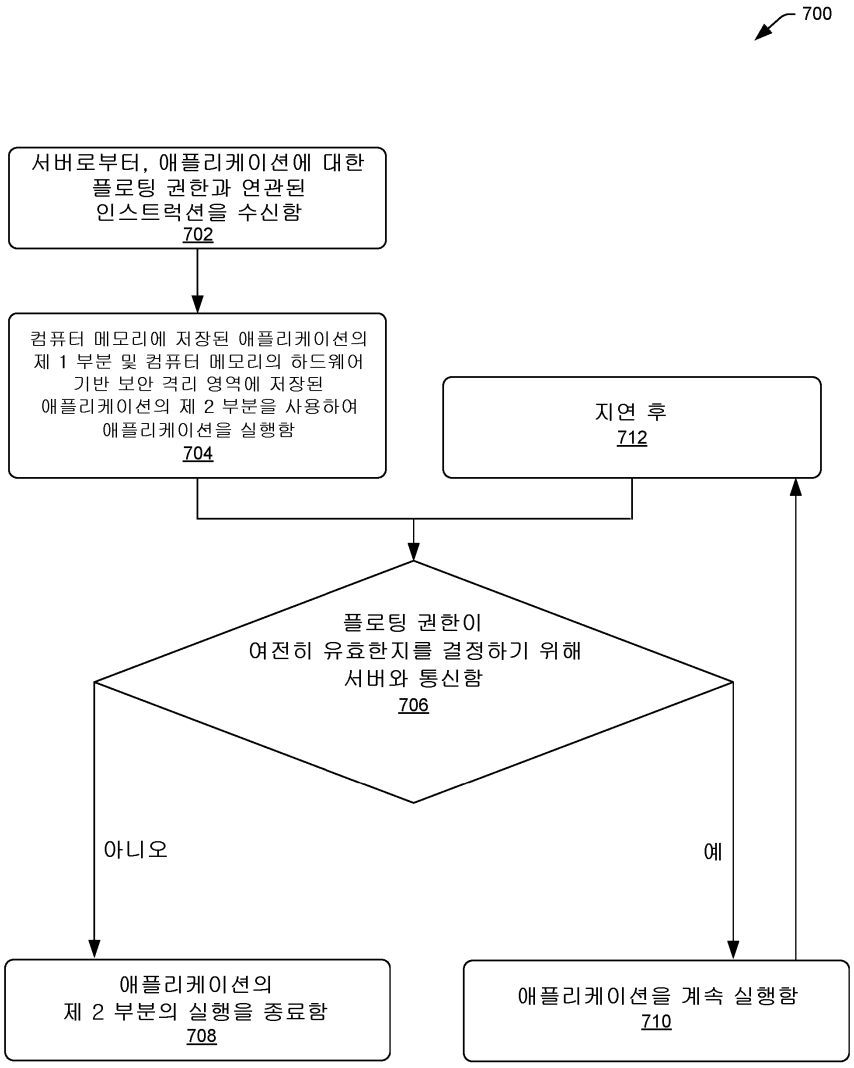
도면5


500
서버와 통신 채널을 수립함
502
통신 채널을 거쳐서 서버로부터
복호화 키를 수신함
504
컴퓨터 메모리의 하드웨어 기반 보안
격리 영역 내에서, 복호화 키를 사용하여
애플리케이션의 암호화 부분을 복호화함
506

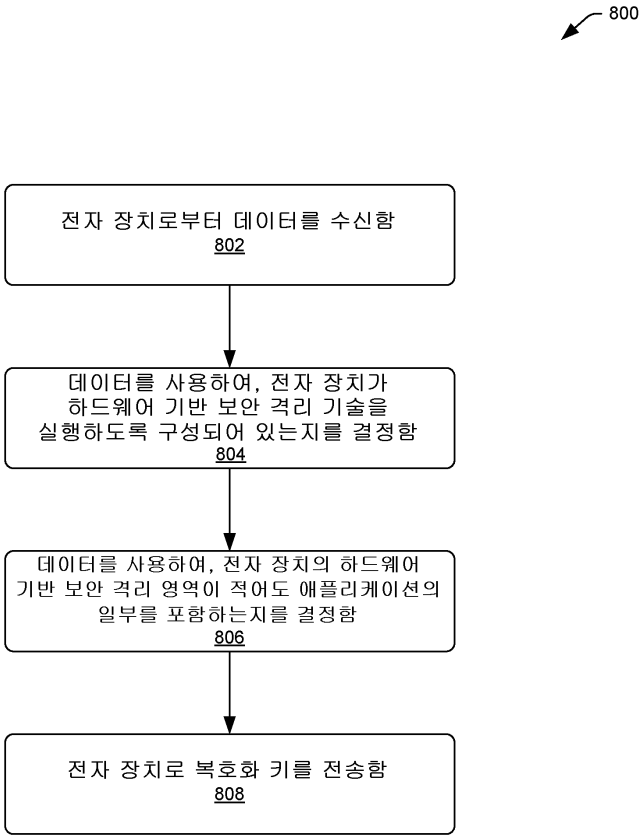
도면6


600
컴퓨터 메모리의 하드웨어 기반 보안
격리 영역 내에서 실링 키를 생성함
602
실링 키를 사용하여
복호화 키를 암호화함
604
암호화된 복호화 키를
컴퓨터 메모리에 저장함
606

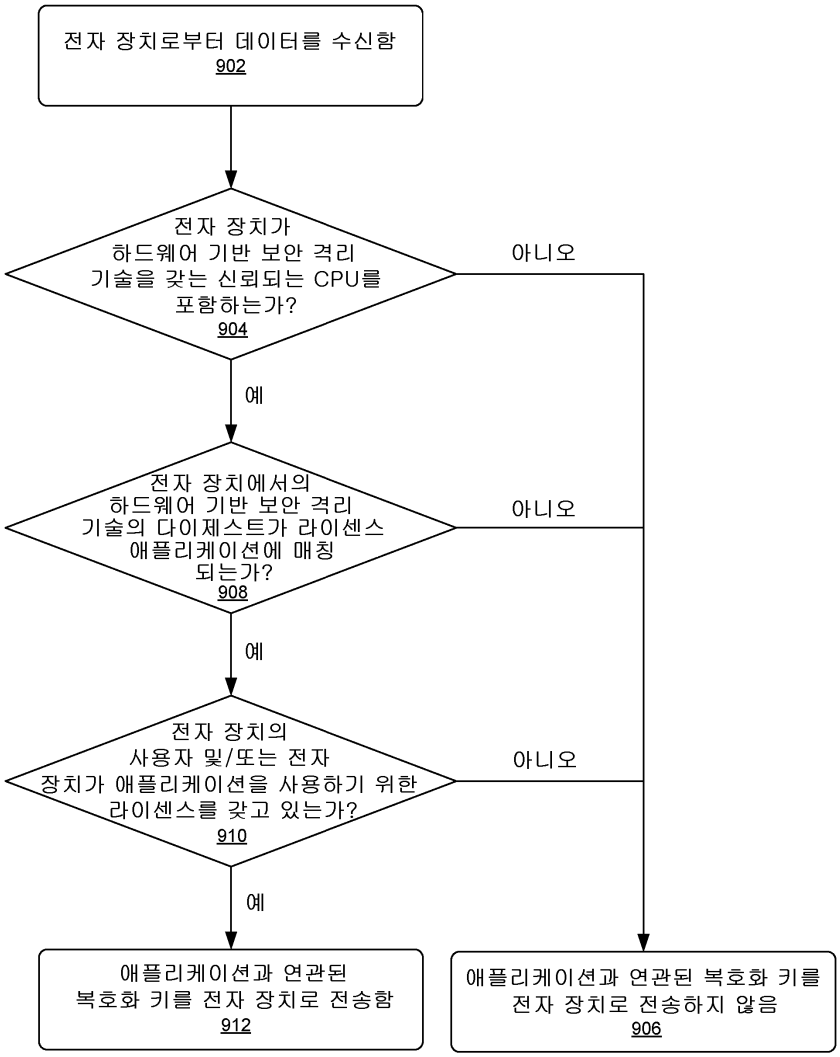
도면7


700
서버로부터, 애플리케이션에 대한 플로팅 권한과 연관된 인스트럭션을 수신함
702
컴퓨터 메모리에 저장된 애플리케이션의 제 1 부분 및 컴퓨터 메모리의 하드웨어 기반 보안 격리 영역에 저장된 애플리케이션의 제 2 부분을 사용하여 애플리케이션을 실행함
704
지연 후
712
플로팅 권한이 여전히 유효한지를 결정하기 위해 서버와 통신함
706
아니오
예
애플리케이션의 제 2 부분의 실행을 종료함
708
애플리케이션을 계속 실행함
710

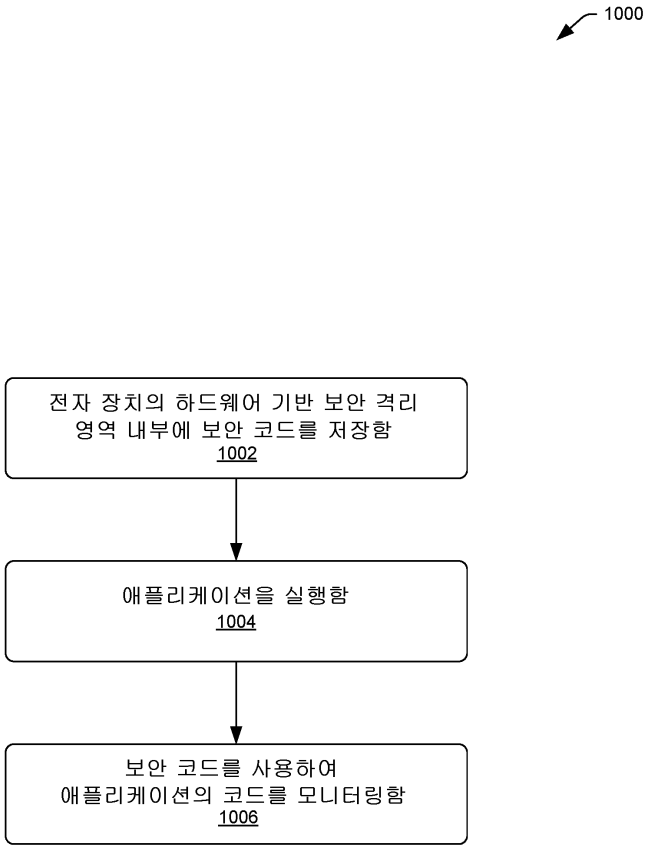
도면8


800
전자 장치로부터 데이터를 수신함
802
데이터를 사용하여, 전자 장치가 하드웨어 기반 보안 격리 기술을 실행하도록 구성되어 있는지를 결정함
804
데이터를 사용하여, 전자 장치의 하드웨어 기반 보안 격리 영역이 적어도 애플리케이션의 일부를 포함하는지를 결정함
806
전자 장치로 복호화 키를 전송함
808

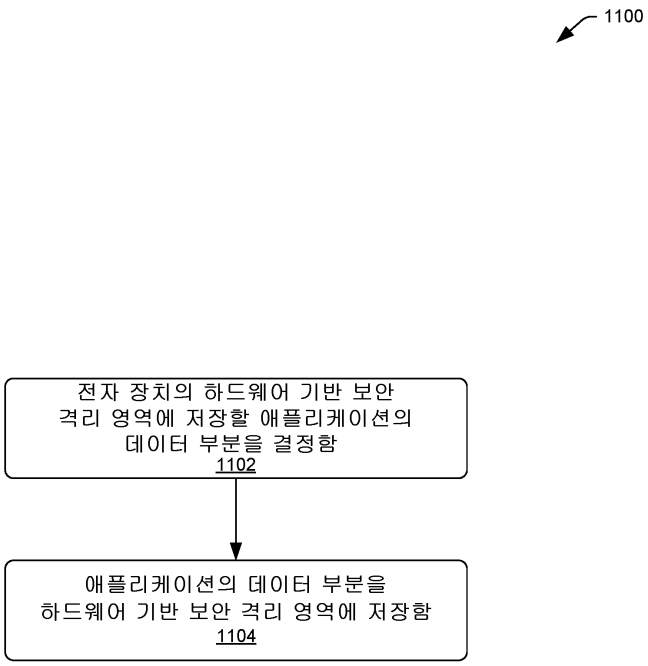
도면9


전자 장치로부터 데이터를 수신함
902
전자 장치가
하드웨어 기반 보안 격리
기술을 갖는 신뢰되는 CPU를
포함하는가?
904
아니오
예
전자 장치에서의
하드웨어 기반 보안 격리
기술의 다이제스트가 라이센스
애플리케이션에 매칭
되는가?
908
아니오
예
전자 장치의
사용자 및/또는 전자
장치가 애플리케이션을 사용하기 위한
라이센스를 갖고 있는가?
910
아니오
예
애플리케이션과 연관된
복호화 키를 전자 장치로 전송함
912
애플리케이션과 연관된 복호화 키를
전자 장치로 전송하지 않음
906

도면10


1000
전자 장치의 하드웨어 기반 보안 격리 영역 내부에 보안 코드를 저장함
1002
애플리케이션을 실행함
1004
보안 코드를 사용하여 애플리케이션의 코드를 모니터링함
1006

도면11


1100
전자 장치의 하드웨어 기반 보안 격리 영역에 저장할 애플리케이션의 데이터 부분을 결정함
1102
애플리케이션의 데이터 부분을 하드웨어 기반 보안 격리 영역에 저장함
1104