(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년03월12일
(11) 등록번호 10-1837678
(24) 등록일자 2018년03월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 15/16* (2018.01)
G06F 9/54 (2018.01)
(52) CPC특허분류
G06F 21/62 (2013.01)
G06F 15/16 (2013.01)
(21) 출원번호 10-2016-0076524
(22) 출원일자 2016년06월20일
심사청구일자 2016년06월20일
(65) 공개번호 10-2017-0142672
(43) 공개일자 2017년12월28일
(56) 선행기술조사문헌
KR1020130143263 A*
KR1020160053814 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 씨오티커넥티드
서울특별시 강남구 논현로 616, 3층(논현동)
(72) 발명자
권영주
경기도 화성시 금반1길 14-28, 401동 1호 (청도솔리움 타운하우스)
이경일
경기도 용인시 기흥구 한보라1로 91, 606동 1402호 (한보라마을휴먼시아6단지아파트)
(뒷면에 계속)
(74) 대리인
정부연

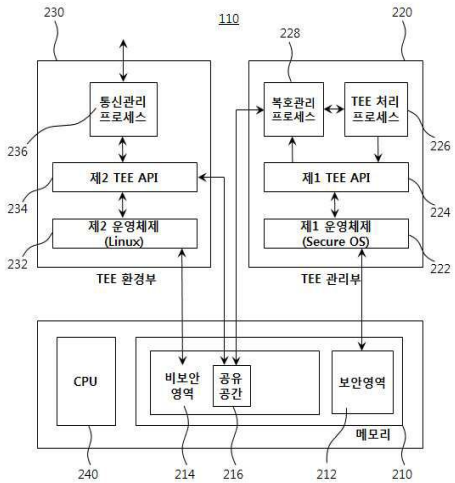
전체 청구항 수 : 총 7 항 심사관 : 구대성

(54) 발명의 명칭 **신뢰실행환경 기반의 컴퓨팅 장치**

(57) 요 약

본 발명은 보안영역에 대한 액세스를 용이하게 하는 신뢰실행환경 기반의 컴퓨팅 기술에 관한 것으로, 보안영역 및 공유공간을 포함하는 비보안영역으로 구성된 메모리, 상기 보안영역을 관리하며 상기 보안영역의 접근을 위한 제1 TEE API(Application Programming Interface)를 제공하는 제1 운영체제에 의하여 구축되고, 상기 제1 운영체제 상에서 TEE 처리 프로세스를 실행시키는 TEE 관리부 및 상기 보안영역에 대한 제2 TEE API를 제공하며 특정 프로세스가 상기 제2 TEE API를 통해 상기 보안영역을 접근하고자 하는 경우 상기 공유공간을 통해 상기 TEE 처리 프로세스와 통신하도록 하는 제2 운영체제에 의하여 구축된 TEE 환경부를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
G06F 9/544 (2013.01)
G06F 9/546 (2013.01)
G06F 2211/007 (2013.01)
(72) 발명자
안재용
서울특별시 관악구 은천로 93, 106동 1001호(봉천동, 벽산블루밍아파트)
김동현
서울특별시 영등포구 도신로 31, 304동 2406호(현대3차아파트)
엄윤호
경기도 부천시 소사구 경인로484번길 68-7, 102동 504호 (신일해피트리아파트)

명 세 서

청구범위

청구항 1

보안영역 및 공유공간을 포함하는 비보안영역으로 구성된 메모리;

상기 보안영역을 관리하며 상기 보안영역의 접근을 위한 제1 TEE API(Application Programming Interface)를 제공하는 제1 운영체제에 의하여 구축되고, 상기 제1 운영체제 상에서 TEE 처리 프로세스를 실행시키는 TEE 관리부; 및

상기 보안영역에 대한 제2 TEE API를 제공하며 특정 프로세스가 상기 제2 TEE API를 통해 상기 보안영역을 접근하고자 하는 경우 상기 공유공간을 통해 상기 TEE 처리 프로세스와 통신하도록 하는 제2 운영체제에 의하여 구축된 TEE 환경부를 포함하고,

상기 TEE 환경부는 상기 특정 프로세스가 상기 제2 TEE API를 호출하여 상기 보안영역을 접근하는 경우 상기 제2 TEE API가 암호화 메시지를 상기 공유공간에 저장하도록 하는 TEE(Trusted Execution Environment) 기반의 컴퓨팅 장치.

청구항 2

삭제

청구항 3

제1항에 있어서, 상기 TEE 환경부는

상기 특정 프로세스가 상기 공유공간으로부터 획득된 제1 보안정보를 상기 암호화 메시지로서 외부의 서버에 송신하도록 하는 것을 특징으로 하는 TEE 기반의 컴퓨팅 장치.

청구항 4

제1항에 있어서, 상기 TEE 환경부는

상기 특정 프로세스가 외부의 서버로부터 획득된 제2 보안정보를 상기 암호화 메시지로서 상기 공유공간에 저장하도록 하는 것을 특징으로 하는 TEE 기반의 컴퓨팅 장치.

청구항 5

제1항에 있어서, 상기 TEE 관리부는

외부의 서버와 통신을 수행하기 위하여 적어도 하나의 DRM(Digital Rights Management) 복호화 키를 관리하는 것을 특징으로 하는 TEE 기반의 컴퓨팅 장치.

청구항 6

제5항에 있어서, 상기 TEE 관리부는

상기 DRM 복호화 키를 통해 상기 공유공간에 저장된 암호화 메시지를 복호화하고 상기 TEE 처리 프로세스를 통해 상기 보안영역을 접근하는 것을 특징으로 하는 TEE 기반의 컴퓨팅 장치.

청구항 7

제6항에 있어서,

상기 메모리는 휘발성 메모리와 비휘발성 메모리로 구성되고,

상기 TEE 관리부는 메모리 매핑 테이블을 통해 상기 보안영역을 상기 비휘발성 메모리로 연관시키는 것을 특징으로 하는 TEE 기반의 컴퓨팅 장치.

청구항 8

제1항에 있어서, 상기 TEE 처리 프로세스는

상기 제1 운영체제 상에서 일정 주기마다 상호 통신하는 메인 및 보조 데몬들로 구성된 이중화 데몬으로 동작되고,

제1 데몬이 비정상적으로 동작되면 제2 데몬은 상기 제1 데몬을 복구시키면서 상기 공유공간에 저장된 암호화 메시지를 기초로 작업을 수행하는 것을 특징으로 하는 TEE 기반의 컴퓨팅 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 신뢰실행환경 기반의 컴퓨팅 기술에 관한 것으로, 보다 상세하게는, 보안영역 접근을 제어하는 전용 프로세스를 구비하여 보안영역에 대한 액세스를 용이하게 하고, 사용자 인터페이스 및 환경에 따라 소프트웨어 플랫폼의 설계를 일일이 변경하지 않아도 간편하게 적용할 수 있는 TEE 기반의 컴퓨팅 장치에 관한 것이다.

배 경 기 술

[0003] TEE(Trusted Execution Environment: 신뢰가 보장된 실행 환경)는 안전성을 높이기 위하여 프로세서, 주변장치 및 저장장치를 대상으로 보안 서비스를 제공하는 소프트웨어 플랫폼을 말한다. TEE는 일반적으로 보안 영역과 비보안 영역의 분리를 지원하는 하드웨어 기능과 이를 이용하여 보안 서비스를 제공하는 소프트웨어로 구성된다.

[0004] TEE는 개방형 운영체제에 하드웨어 기반의 독립적으로 격리된 실행 환경을 제공할 수 있기 때문에 소프트웨어 공격에 대한 방어가 가능하여 보안 수준을 향상시킬 수 있다. 이로 인해, TEE는 장치 및 사용자의 정보에 대한 보안기술을 필요로 하는 다양한 컴퓨팅 장치들에 적용되고 있다.

[0005] 종래의 TEE는 보안 수준이 강력한 만큼 상시로 요구되는 보안영역에 대한 접근이 용이하지 않고, 보안영역 내의 정보를 송수신하기 위한 운영체제 내의 통신 인터페이스를 환경에 따라 일일이 설계해주어야 하는 단점이 있다.

[0006] 한국 공개특허공보 제10-2015-0033368호는 신뢰하는 실행 환경(Trusted Execution Environment; TEE)에서의 보안 도메인 관리 방법 및 장치에 관한 것으로, 적어도 하나의 보안 도메인을 포함하는 TEE에서 적어도 하나의 보안 도메인을 관리하기 위한 보안 도메인 관리 방법에 있어서, 임의의 보안 도메인에 대한 이벤트가 발생하면, 상기 이벤트에 관한 정보를 획득하는 단계, 상기 이벤트에 관한 정보를 적어도 하나의 다른 보안 도메인으로 전달하는 단계를 포함하되, 상기 이벤트에 관한 정보는 TEE 커널을 통하여 전달되는 것을 특징으로 한다.

[0007] 한국 공개특허공보 제10-2014-0111943호는 보안 환경 장치 및 구현 방법에 관한 것으로, 일반 환경은 데이터를 보안 환경으로 요청하는 클라이언트 애플리케이션을 포함하고, 보안 환경은 상기 클라이언트 애플리케이션으로부터 상기 데이터의 요청을 수신하는 신뢰된 실행 환경 소프트웨어를 포함하고, 상기 신뢰된 실행 환경 소프트웨어는 상기 데이터의 요청과는 상이한 경로로 요청된 데이터를 상기 클라이언트 애플리케이션으로 전송하고, 상기 클라이언트 애플리케이션은 상기 요청된 데이터를 수신하는 것을 특징으로 한다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국 공개특허공보 제10-2015-0033368호 (2015.04.01 공개)

(특허문헌 0002) 한국 공개특허공보 제10-2014-0111943호 (2014.09.22 공개)

발명의 내용

해결하려는 과제

[0010] 본 발명의 일 실시예는 보안영역 접근 요청을 수신하면 비보안영역 내의 공유공간을 두고 별도의 전용 프로세스와 통신하도록 하여 보안영역에 대한 액세스를 용이하게 하는 TEE 기반의 컴퓨팅 장치를 제공하고자 한다.

[0011] 본 발명의 일 실시예는 보안영역 접근을 제어하는 전용 프로세스를 구비하여 사용자 인터페이스 및 환경에 따라 소프트웨어 플랫폼의 설계를 일일이 변경하지 않아도 간편하게 적용할 수 있는 TEE 기반의 컴퓨팅 장치를 제공하고자 한다.

[0012] 본 발명의 일 실시예는 보안영역 접근에 대하여 복호화 키 관리를 통해 외부 단말기 및 서버에 대한 인증을 수행하여 보안 수준을 높게 유지하는 TEE 기반의 컴퓨팅 장치를 제공하고자 한다.

과제의 해결 수단

[0014] 실시예들 중에서, TEE(Trusted Execution Environment) 기반의 컴퓨팅 장치는 보안영역 및 공유공간을 포함하는 비보안영역으로 구성된 메모리, 상기 보안영역을 관리하며 상기 보안영역의 접근을 위한 제1 TEE API(Application Programming Interface)를 제공하는 제1 운영체제에 의하여 구축되고, 상기 제1 운영체제 상에서 TEE 처리 프로세스를 실행시키는 TEE 관리부 및 상기 보안영역에 대한 제2 TEE API를 제공하며 특정 프로세스가 상기 제2 TEE API를 통해 상기 보안영역을 접근하고자 하는 경우 상기 공유공간을 통해 상기 TEE 처리 프로세스와 통신하도록 하는 제2 운영체제에 의하여 구축된 TEE 환경부를 포함한다.

[0015] TEE 기반의 컴퓨팅 장치에서 상기 TEE 환경부는 상기 특정 프로세스가 상기 제2 TEE API를 호출하여 상기 보안영역을 접근하는 경우 상기 제2 TEE API가 암호화 메시지를 상기 공유공간에 저장하도록 하는 것을 특징으로 할 수 있다.

[0016] TEE 기반의 컴퓨팅 장치에서 상기 TEE 환경부는 상기 특정 프로세스가 상기 공유공간으로부터 획득된 제1 보안정보를 상기 암호화 메시지로서 외부의 서버에 송신하도록 하는 것을 특징으로 할 수 있다.

[0017] TEE 기반의 컴퓨팅 장치에서 상기 TEE 환경부는 상기 특정 프로세스가 상기 외부의 서버로부터 획득된 제2 보안정보를 상기 암호화 메시지로서 상기 공유공간에 저장하도록 하는 것을 특징으로 할 수 있다.

[0018] TEE 기반의 컴퓨팅 장치에서 상기 TEE 관리부는 외부의 서버와 통신을 수행하기 위하여 적어도 하나의 DRM(Digital Rights Management) 복호화 키를 관리하는 것을 특징으로 할 수 있다.

[0019] TEE 기반의 컴퓨팅 장치에서 상기 TEE 관리부는 상기 DRM 복호화 키를 통해 상기 공유공간에 저장된 암호화 메시지를 복호화하고 상기 TEE 처리 프로세스를 통해 상기 보안영역을 접근하는 것을 특징으로 할 수 있다.

[0020] TEE 기반의 컴퓨팅 장치에서 상기 메모리는 휘발성 메모리와 비휘발성 메모리로 구성되고, 상기 TEE 관리부는 메모리 매핑 테이블을 통해 상기 보안영역을 상기 비휘발성 메모리로 연관시키는 것을 특징으로 할 수 있다.

[0021] TEE 기반의 컴퓨팅 장치에서, 상기 TEE 처리 프로세스는 상기 제1 운영체제 상에서 일정 주기마다 상호 통신하는 메인 및 보조 데몬들로 구성된 이중화 데몬으로 동작되고, 제1 데몬이 비정상적으로 동작되면 제2 데몬은 상기 제1 데몬을 복구시키면서 상기 공유공간에 저장된 암호화 메시지를 기초로 작업을 수행하는 것을 특징으로 할 수 있다.

발명의 효과

[0023] 개시된 기술은 다음의 효과를 가질 수 있다. 다만, 특정 실시예가 다음의 효과를 전부 포함하여야 한다거나 다음의 효과만을 포함하여야 한다는 의미는 아니므로, 개시된 기술의 권리범위는 이에 의하여 제한되는 것으로 이해되어서는 아니 될 것이다.

[0024] 본 발명의 일 실시예에 따른 TEE 기반의 컴퓨팅 장치는 보안영역 접근 요청을 수신하면 비보안영역 내의 공유공

간을 두고 별도의 전용 프로세스와 통신하도록 하여 보안영역에 대한 액세스를 용이하게 할 수 있다.

[0025] 본 발명의 일 실시예에 따른 TEE 기반의 컴퓨팅 장치는 보안영역 접근을 제어하는 전용 프로세스를 구비하여 사용자 인터페이스 및 환경에 따라 소프트웨어 플랫폼의 설계를 일일이 변경하지 않아도 간편하게 적용할 수 있다.

[0026] 본 발명의 일 실시예에 따른 TEE 기반의 컴퓨팅 장치는 보안영역 접근에 대하여 복호화 키 관리를 통해 외부 단말기 및 서버에 대한 인증을 수행하여 보안 수준을 높게 유지할 수 있다.

도면의 간단한 설명

[0028] 도 1은 본 발명의 일 실시예에 따른 TEE 기반의 컴퓨팅 시스템을 설명하는 도면이다.

도 2는 도 1에 있는 TEE 기반의 컴퓨팅 장치의 하드웨어 및 소프트웨어의 구성을 개략적으로 나타내는 도면이다.

도 3은 도 1에 있는 TEE 기반의 컴퓨팅 장치의 동작의 실시예를 설명하는 순서도이다.

도 4는 도 1에 있는 TEE 기반의 컴퓨팅 장치의 동작의 다른 실시예를 설명하는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 발명에 관한 설명은 구조적 내지 기능적 설명을 위한 실시예에 불과하므로, 본 발명의 권리범위는 본문에 설명된 실시예에 의하여 제한되는 것으로 해석되어서는 아니 된다. 즉, 실시예는 다양한 변경이 가능하고 여러 가지 형태를 가질 수 있으므로 본 발명의 권리범위는 기술적 사상을 실현할 수 있는 균등물들을 포함하는 것으로 이해되어야 한다. 또한, 본 발명에서 제시된 목적 또는 효과는 특정 실시예가 이를 전부 포함하여야 한다거나 그러한 효과만을 포함하여야 한다는 의미는 아니므로, 본 발명의 권리범위는 이에 의하여 제한되는 것으로 이해되어서는 아니 될 것이다.

[0030] 한편, 본 출원에서 서술되는 용어의 의미는 다음과 같이 이해되어야 할 것이다.

[0031] "제1", "제2" 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하기 위한 것으로, 이들 용어들에 의해 권리범위가 한정되어서는 아니 된다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[0032] 어떤 구성요소가 다른 구성요소에 "연결되어"있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결될 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어"있다고 언급된 때에는 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 한편, 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0033] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함하다"또는 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이며, 하나 또는 그 이상의 다른 특징이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0034] 각 단계들에 있어 식별부호(예를 들어, a, b, c 등)는 설명의 편의를 위하여 사용되는 것으로 식별부호는 각 단계들의 순서를 설명하는 것이 아니며, 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않는 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 단계들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0035] 본 발명은 컴퓨터가 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현될 수 있고, 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 데이터 저장 장치 등이 있으며, 또한, 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0036] 여기서 사용되는 모든 용어들은 다르게 정의되지 않는 한, 본 발명이 속하는 분야에서 통상의 지식을 가진 자에

의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한 이상적이거나 과도하게 형식적인 의미를 지니는 것으로 해석될 수 없다.

[0038] 도 1은 본 발명의 일 실시예에 따른 TEE 기반의 컴퓨팅 시스템을 설명하는 도면이다.

[0039] 도 1을 참조하면, TEE 기반의 컴퓨팅 시스템(100)은 TEE 기반의 컴퓨팅 장치(110) 및 클라우드 서버(120)를 포함한다.

[0040] TEE 기반의 컴퓨팅 장치(110)는 보안영역 접근을 제어하는 전용 프로세스를 구비하여 사용자 인터페이스 및 환경이 바뀌어도 간편하게 적용할 수 있는 TEE 기반의 소프트웨어 플랫폼을 제공한다. 여기에서, TEE(Trusted Execution Environment)는 일반적으로 안전성을 높이기 위하여 프로세서, 주변장치 및 저장장치를 대상으로 보안 서비스를 제공하는 소프트웨어 플랫폼을 말하는 것으로, 보안 영역과 비보안 영역의 분리를 지원하는 하드웨어 기능과 이를 이용하여 보안 서비스를 제공하는 소프트웨어로 구성된다. 또한, 여기에서, 소프트웨어 플랫폼이란, 다양한 어플리케이션이 작동하는 기반이 되는 운영체제 소프트웨어를 말한다.

[0041] TEE 기반의 컴퓨팅 장치(110)는 보안영역 접근 요청을 수신하면 비보안영역 내의 공유공간을 통해 별도의 전용 프로세스인 TEE 처리 프로세스(226)를 진행하도록 하여 보안영역에 대한 액세스를 용이하게 할 수 있다. 예를 들어, N-스크린 진행 시, TEE 기반의 컴퓨팅 장치(110)는 수시로 즉각적인 데이터 처리를 필요로 하는 민감한 정보들의 보안을 유지하면서 보안영역에 대한 엑세스를 용이하게 할 수 있다. 이에 따라, TEE 기반의 컴퓨팅 장치(110)는 VOD(Video On Demand) 구매목록이나 결제내역처럼 보안을 필요로 하는 사용자의 정보 처리를 보안영역 안에서 진행할 수 있다. 여기에서, N-스크린은 여러 개의 화면을 통해 콘텐츠를 제공하는 서비스를 말한다. 예를 들어, N-스크린은 영화나 음악을 구입한 후 셋톱박스, TV, PC, 태블릿 및 스마트폰 등의 다양한 단말기에서 공통으로 콘텐츠를 향유할 수 있도록 한다.

[0042] TEE 기반의 컴퓨팅 장치(110)는 클라우드 서버(120)와 네트워크를 통해 연결될 수 있다. TEE 기반의 컴퓨팅 장치(110)는 중앙처리장치, 메모리 장치 및 입출력 수단을 구비한 셋톱박스, PC, 스마트폰, 태블릿 PC와 같은 컴퓨팅 장치에 해당할 수 있고, 클라우드 서버(120)에 의해 제공되는 서비스를 사용하는 사용자 혹은 사용자의 단말기에 해당할 수 있다.

[0043] 클라우드 서버(120) 클라우드 컴퓨팅을 제공할 수 있는 가상 사설 서버로, 하나의 물리적 서버를 나누어 여러 개의 가상 서버로 이용하는 가상화 기술방법의 한 형태이다. 여기에서, 클라우드 컴퓨팅이란, 인터넷 기반의 컴퓨터 기술로, 인터넷 상의 유틸리티 데이터 서버에 프로그램을 두고, 그때 그때 필요할 때마다 컴퓨터나 휴대폰, 셋톱박스 등에 불러와서 사용하는 웹 기반 소프트웨어 서비스를 말한다. 클라우드 서버(120)는 네트워크를 통해 TEE 기반의 컴퓨팅 장치(110)에 다양한 서비스 및 기능을 제공할 수 있다.

[0045] 도 2는 도1에 있는 TEE 기반의 컴퓨팅 장치의 하드웨어 및 소프트웨어의 구성을 개략적으로 나타내는 도면이다.

[0046] 도 2를 참조하면, TEE 기반의 컴퓨팅 장치(110)는 메모리(210), TEE 관리부(220), TEE 환경부(230) 및 CPU(240)를 포함한다.

[0047] 메모리(210)는 TEE 기반의 컴퓨팅 장치(110)에 설치된 로컬 저장장치에 해당하고, 휘발성 메모리와 비휘발성 메모리로 구성될 수 있다. 여기에서, 휘발성 메모리는 저장된 정보를 유지하기 위해 전기를 요구하는 컴퓨터 메모리로서, 동적 램(DRAM), 정적 램(SRAM)을 포함한 랜덤 액세스 메모리(RAM)로 구현될 수 있고, 비휘발성 메모리는 시스템에서 전원이 공급되지 않아도 내부 정보가 지워지지 않는 메모리로서, 플래시 메모리, 롬, 마그네틱 컴퓨터 기억장치 등으로 구현될 수 있다.

[0048] 메모리(210)는 보안영역(212) 및 공유공간(216)을 포함하는 비보안영역(214)으로 구성된다. 보안영역(212)과 비보안영역(214)은 TEE 기반의 컴퓨팅 장치(110)의 소프트웨어 플랫폼에 의해 엄격하게 분리되도록 지원 받는다.

[0049] 보안영역(212)은 제1 운영체제(222)에 의해 관리될 수 있고, 비보안영역(214)은 제2 운영체제(232)에 의해 관리된다. 공유공간(216)은 제2 TEE API(234) 및 복호키 관리부(228)에 의해 접근될 수 있고, 클라우드 서버(120)를 대상으로 한 복호화 및 인증 과정에 사용되는 암호화 메시지들이 저장될 수 있다.

[0050] TEE 관리부(220)는 보안영역(212)을 관리하며 보안영역(212)의 접근을 위한 제1 TEE API(Application Programming Interface)(224)를 제공하는 제1 운영체제(222)에 의하여 구축되고, 제1 운영체제(222) 상에서 TEE 처리 프로세스(226)를 실행시킨다. 여기에서, API는 응용 프로그램에서 사용할 수 있도록, 운영 체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 응용 프로그램 프로그래밍 인터페이스를 의미하고, 이러

한 API는 주로 파일 제어, 창 제어, 화상 처리, 문자 제어 등을 위한 인터페이스를 제공한다. 제1 운영체제(222)는 보안영역을 관리하는 운영체제이기 때문에 보안을 강화시킨 운영체제 소프트웨어를 필요로 한다. 일 실시예에서, 제1 운영체제(222)는 Secure OS(Operating System, 운영체제)를 통해 구현될 수 있다. 여기에서, Secure OS는 컴퓨터 운영체제 상에 내재된 보안상의 결함으로 인하여 발생할 수 있는 각종 해킹과 내부 공격자로부터 시스템을 보호하기 위한 솔루션으로, 기본적인 보안 계층을 파일시스템, 디바이스, 프로세스에 대한 접근 권한 결정이 이루어지는 운영체제의 커널 레벨로 낮춘 통합된 보안 커널(Security Kernel)을 이식한 운영체제이다. 이와 같은 Secure OS는 컴퓨터 시스템 자체를 통제하는 운영체제에 보안기능을 부여하였기 때문에 다른 보안 어플리케이션보다 보안 기능이 우수한 특징이 있다.

[0051] TEE 관리부(220)는 외부의 서버와 통신을 수행하기 위하여 적어도 하나의 DRM(Digital Rights Management) 복호화 키를 관리할 수 있다. 여기에서, DRM은 전자장치 상의 디지털 콘텐츠에 대해 사용을 제어하여 콘텐츠가 정해진 규칙 내에서만 사용되도록 특정 사람 및 기기에서 사용권한을 제어하는 기술을 의미한다. TEE 관리부(220)는 DRM 복호화 키를 통해 공유공간에 저장된 암호화 메시지를 복호화하고 TEE 처리 프로세스를 통해 보안영역을 접근할 수 있다. 이러한 복호화 키 관리는 복호관리 프로세스(228)을 통해 진행될 수 있다.

[0052] TEE 관리부(220)는 메모리 매핑 테이블을 통해 보안영역(212)을 비휘발성 메모리(미도시됨)로 연관시키는 것을 특징으로 할 수 있다. 여기에서, 메모리 매핑 테이블은 프로그램에 의해 작성 된 코드를 실행파일로 만들어 운영체제를 실행할 때, 메모리에 각각의 데이터 영역을 분리하여 할당된 지도를 말한다. 예를 들어, 메모리 매핑 테이블은 헤더와 바디를 포함하는 바이너리 이미지로 구현될 수 있고, 헤더는 바디에 있는 보안영역(212)의 정보와 비휘발성 메모리의 위치(즉, 주소 정보)를 기록할 수 있다. TEE 관리부(220)는 이와 같은 방법을 통해 제1 운영체제(222)를 통해 보안영역(212) 내에서 비휘발성 메모리를 관리할 수 있다.

[0053] TEE 관리부(220)에서 TEE 처리 프로세스(226)는 제1 운영체제(222) 상에서 일정 주기마다 상호 통신하는 메인 및 보조 데몬들로 구성된 이중화 데몬으로 동작되고, 제1 데몬이 비정상적으로 동작되면 제2 데몬은 제1 데몬을 복구시키면서 공유공간(216)에 저장된 암호화 메시지를 기초로 작업을 수행할 수 있다. 여기에서, 데몬은 사용자에 의해 직접적으로 제어되지 않고 백그라운드에서 돌면서 여러 작업을 하는 프로그램을 말한다. 일반적으로 시스템은 시동할 때 데몬을 시작하는 경우가 많으며, 이런 데몬들은 네트워크 요청, 하드웨어 동작, 여타 프로그램에 반응하는 기능을 담당하게 된다. TEE 처리 프로세스(226)는 이러한 이중화 데몬을 통해 데몬의 동작 오류에 대비할 수 있고, 공유공간(216)에 저장된 암호화 메시지를 기초로 한 작업이 중단되지 않고 수행될 수 있도록 한다.

[0054] TEE 환경부(230)는 보안영역(212)에 대한 제2 TEE API(234)를 제공하며 특정 프로세스가 제2 TEE API(234)를 통해 보안영역(212)을 접근하고자 하는 경우 공유공간(216)을 통해 TEE 처리 프로세스(226)와 통신하도록 하는 제2 운영체제(232)에 의하여 구축된다. 일 실시예에서, 제2 운영체제(232)는 리눅스(Linux)에 의해 구현될 수 있다. 여기에서, 리눅스는 컴퓨터를 위한 운영 체제 중 하나로서, 자유 소프트웨어와 오픈 소스 개발의 가장 유명한 표본으로 들 수 있다.

[0055] TEE 환경부(230)는 특정 프로세스가 제2 TEE API(234)를 호출하여 보안영역(212)을 접근하는 경우 제2 TEE API(234)가 암호화 메시지를 공유공간(216)에 저장하도록 할 수 있다. TEE 환경부(230)는 특정 프로세스가 공유공간(216)으로부터 획득된 제1 보안정보를 암호화 메시지로서 외부의 클라우드 서버(120)에 송신하도록 할 수 있고, 특정 프로세스가 클라우드 서버(120)로부터 획득된 제2 보안정보를 암호화 메시지로서 공유공간(216)에 저장하도록 할 수 있다. 클라우드 서버(120)와의 통신 과정은 통신관리 프로세스(236)을 통해 진행될 수 있다.

[0056] TEE 환경부(230)는 특정 프로세스가 제2 TEE API(234)를 호출하는 횟수를 카운트하여 이를 기초로 공유공간(216)의 크기를 동적으로 할당할 수 있다. 여기에서, 메모리의 동적 할당은 컴퓨터 프로그래밍에서 실행 시간 동안 사용할 메모리 공간을 할당하는 것을 말하고, 사용 종료 시 운영체제가 쓸 수 있도록 반납하며 다음 요청이 있을 때 재 할당을 받을 수 있다. 일 실시예에서, TEE 환경부(230)는 수식 1을 적용하여 공유공간(216)의 크기를 동적으로 할당할 수 있다.

[0057] [수식 1]

[0058] $$SIZE = \log\left(\sum Count\right)$$

[0059] (SIZE는 공유공간(216)의 크기에 해당하고, Count는 특정 프로세스가 제2 TEE API(234)를 호출하는 횟수를 일정

시간 구간 동안 카운트한 수치에 해당함)

[0060] CPU(Central Processing Unit)(240)는 메모리(210), TEE 관리부(220), TEE 환경부(230) 및 기타 주변 장치들의 동작 전반을 제어하는 컴퓨터 내의 중앙 처리 장치로서, 외부에서 정보를 입력 받고, 기억하고, 컴퓨터 프로그램의 명령어를 해석하여 연산하고, 외부로 출력하는 역할을 수행한다.

[0062] 도 3은 도 1에 있는 TEE 기반의 컴퓨팅 장치의 동작의 실시예를 설명하는 순서도이다.

[0063] 도 3을 참조하면, TEE 기반의 컴퓨팅 장치(110)는 특정 프로세스가 제2 TEE API(234)를 통해 보안영역(212)을 접근하고자 하는 경우, 공유공간(216)을 통해 TEE 처리 프로세스(226)와 통신하도록 한다(단계 S310-S330).

[0064] TEE 기반의 컴퓨팅 장치(110)는 제1 운영체제(222)에 의하여 구축되는 TEE 관리부(220)와 제2 운영체제(232)에 의하여 구축되는 TEE 환경부(230)를 포함한다. 제1 운영체제(222)는 보안영역(212)을 관리하며 보안영역(212)의 접근을 위한 제1 TEE API(224)를 제공하고, 제2 운영체제(232)는 보안영역(212)에 대한 제2 TEE API(234)를 제공한다.

[0065] 우선, 특정 프로세스가 제2 TEE API(234)를 통해 보안영역(212)을 접근하고자 하는 경우(단계S310), TEE 관리부(220)는 제1 운영체제(222) 상에서 TEE 처리 프로세스(226)를 실행시킬 수 있다(단계 S320). 다음, 제2 운영체제(232)는 해당 특정 프로세스와 TEE 처리 프로세스(226)의 통신이 공유공간(216)을 통해 진행되도록 할 수 있다(단계S330). 이와 같은 통신의 과정에서, TEE 처리 프로세스(226)는 해당 특정 프로세스에 의해 공유공간(216)에 저장된 암호화 메시지를 기초로 보안영역(212)에 대한 접근 여부에 대해 결정할 수 있고, 이를 기초로 TEE 관리부(220)는 외부 클라우드 서버(120)와의 통신에 있어서 보안영역(212)에 대한 액세스를 제어할 수 있다.

[0067] 도 4는 도 1에 있는 TEE 기반의 컴퓨팅 장치의 동작의 다른 실시예를 설명하는 순서도이다.

[0068] 도 4를 참조하면, 우선, 앞서 서술한 바와 같이, 특정 프로세스가 제2 TEE API(234)를 통해 보안영역(212)을 접근하고자 하는 경우(단계S410), TEE 관리부(220)는 제1 운영체제(222) 상에서 TEE 처리 프로세스(226)를 실행시킬 수 있다(단계S420). 예를 들어, 클라우드 서버(120)와의 통신을 통해 클라우드 서버(120)의 보안 정보를 포함한 통신관리 프로세스(236)가 제2 TEE API(234)를 통해 보안영역(212)에 접근하고자 할 수 있고, 이에 대해 TEE 관리부(220)는 TEE 처리 프로세스(226)를 실행시키어 이후의 보안영역(212)의 접근과 관련한 통신에 대하여 제어할 수 있다.

[0069] 해당 특정 프로세스가 제2 TEE API(234)를 호출하여 보안영역(212)에 접근함에 따라, 제2 TEE API(234)는 암호화 메시지를 공유공간(216)에 저장할 수 있다(단계S430). 예를 들어, 제2 TEE API(234)는 사전에 접근을 인가받은 서버 혹은 단말기인지 확인하기 위하여 고유의 디바이스 정보를 요청하는 암호화 메시지를 공유공간(216)에 저장할 수 있다. 이후, TEE 환경부(230)는 해당 특정 프로세스가 공유공간(216)으로부터 획득한 제1 보안정보를 암호화 메시지로서 외부의 클라우드 서버(120)에 송신하도록 할 수 있다(단계S440).

[0070] 다음, TEE 환경부(230)는 해당 특정 프로세스로 하여금 외부의 클라우드 서버(120)로부터 획득한 제2 보안정보를 암호화 메시지로서 공유공간(216)에 저장하도록 할 수 있다(단계S450). 예를 들어, 해당 특정 프로세스는 단계S430에서 공유공간(216)에 암호화 메시지로 저장되어 요청된 바 있는 고유의 디바이스 정보를 제2 보안정보로서 외부의 클라우드 서버(120)로부터 획득하여 암호화 메시지로서 공유공간(216)에 저장할 수 있다.

[0071] 이후, TEE 관리부(220)는 이와 같이 외부의 클라우드 서버(120)로부터 획득하여 공유공간(216)에 저장된 암호화 메시지를 복호화하는 작업을 진행하도록 할 수 있다(단계S460). TEE 관리부(220)는 외부의 클라우드 서버(120)와 통신을 수행하기 위하여 적어도 하나의 DRM 복호화 키를 관리할 수 있고, 이와 같은 DRM 복호화 키를 통해 공유공간(216)에 저장된 암호화 메시지를 복호화할 수 있다. 실시예에서, TEE 관리부(220)는 복호관리 프로세스(228)를 통해 적어도 하나의 DRM 복호화 키 정보를 저장 및 관리할 수 있고, TEE 처리 프로세스(226)에 의해 복호화 과정 전반이 제어되도록 할 수 있다.

[0072] TEE 관리부(220)는 복호화 과정이 정상적으로 통과되면, TEE 처리 프로세스(226)를 통해 보안영역(212)을 접근하도록 할 수 있다(단계S470). 예를 들어, 외부의 클라우드 서버(120)로부터 획득하여 공유공간(216)에 저장된 암호화 메시지를 복호화하여 사전에 저장된 DRM 복호화 키와 일치됨을 확인하면, TEE 처리 프로세스(226)를 통해 보안영역(212)에 접근하도록 할 수 있고, 이를 기초로 하여 외부와의 통신을 수행하도록 제어할 수 있다(단계S480)

[0073] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특

허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0075] 100: TEE 기반의 컴퓨팅 시스템

110: TEE 기반의 컴퓨팅 장치 120: 클라우드 서버

210: 메모리

212: 보안영역 214: 비보안영역

216: 공유공간

220: TEE 관리부

222: 제1 운영체제 224: 제1 TEE API

226: TEE 처리 프로세스 228: 복호관리 프로세스

230: TEE 환경부

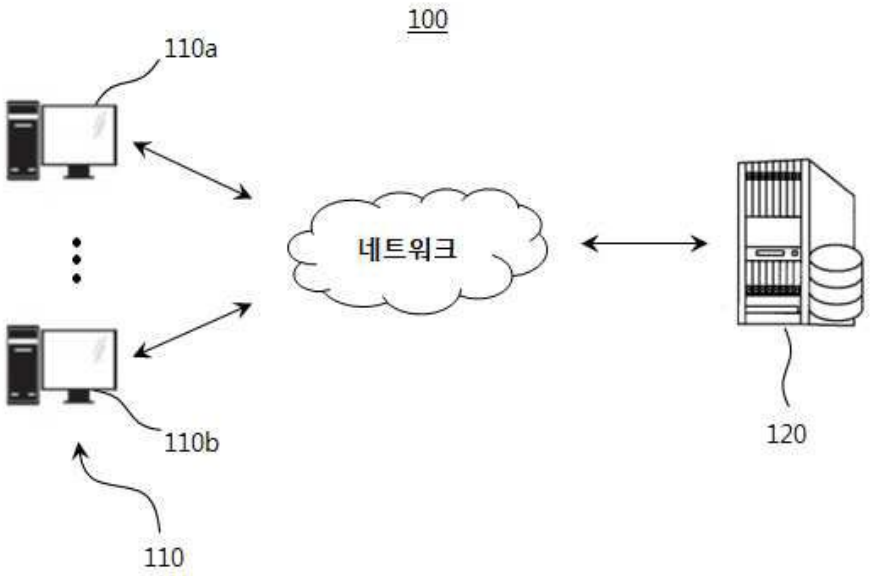
232: 제2 운영체제 234: 제2 TEE API

236: 통신관리 프로세스

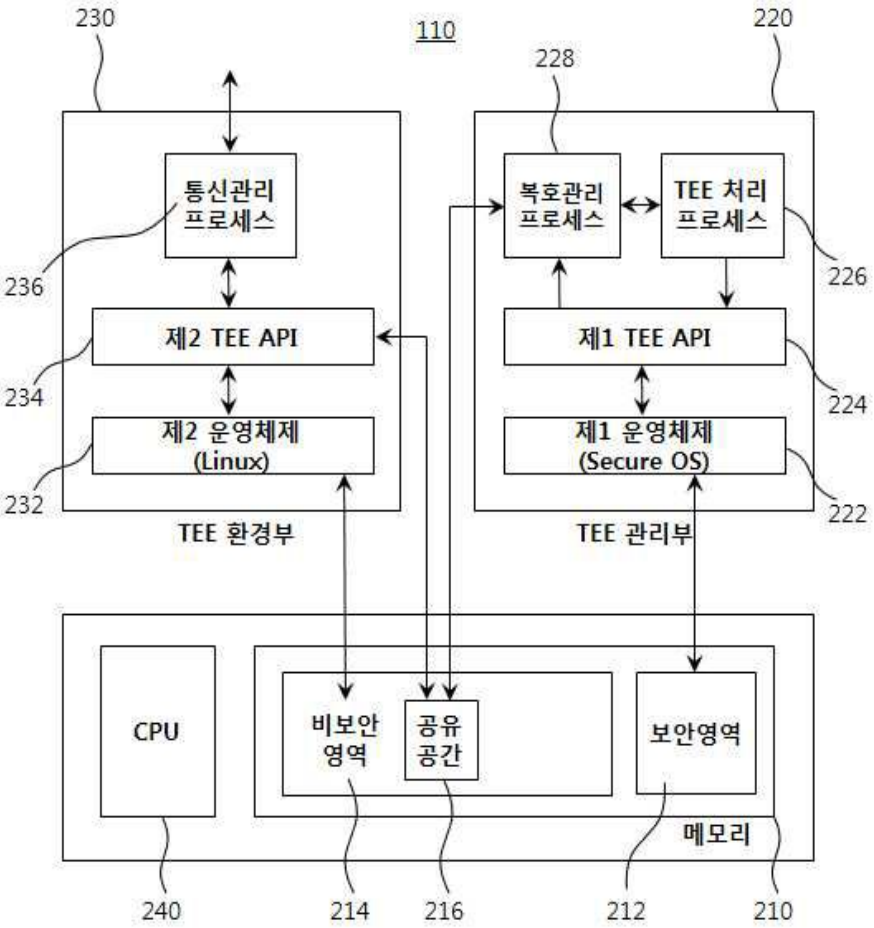
240: CPU

도면

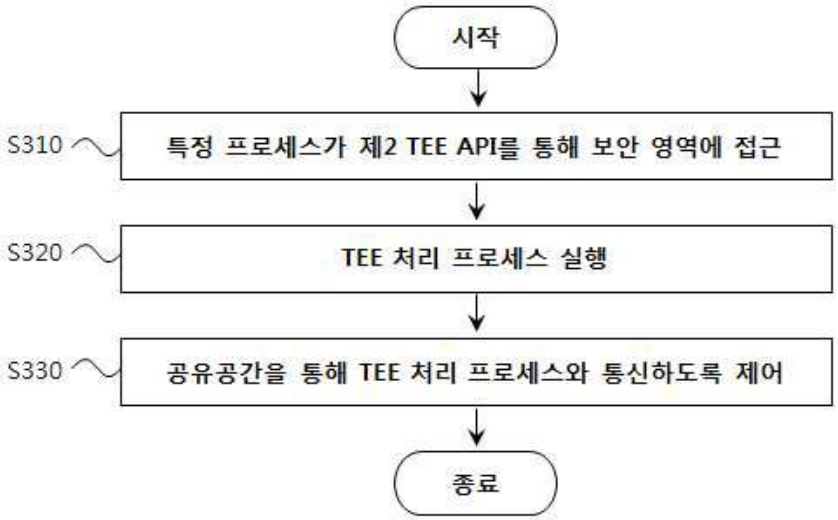
도면1



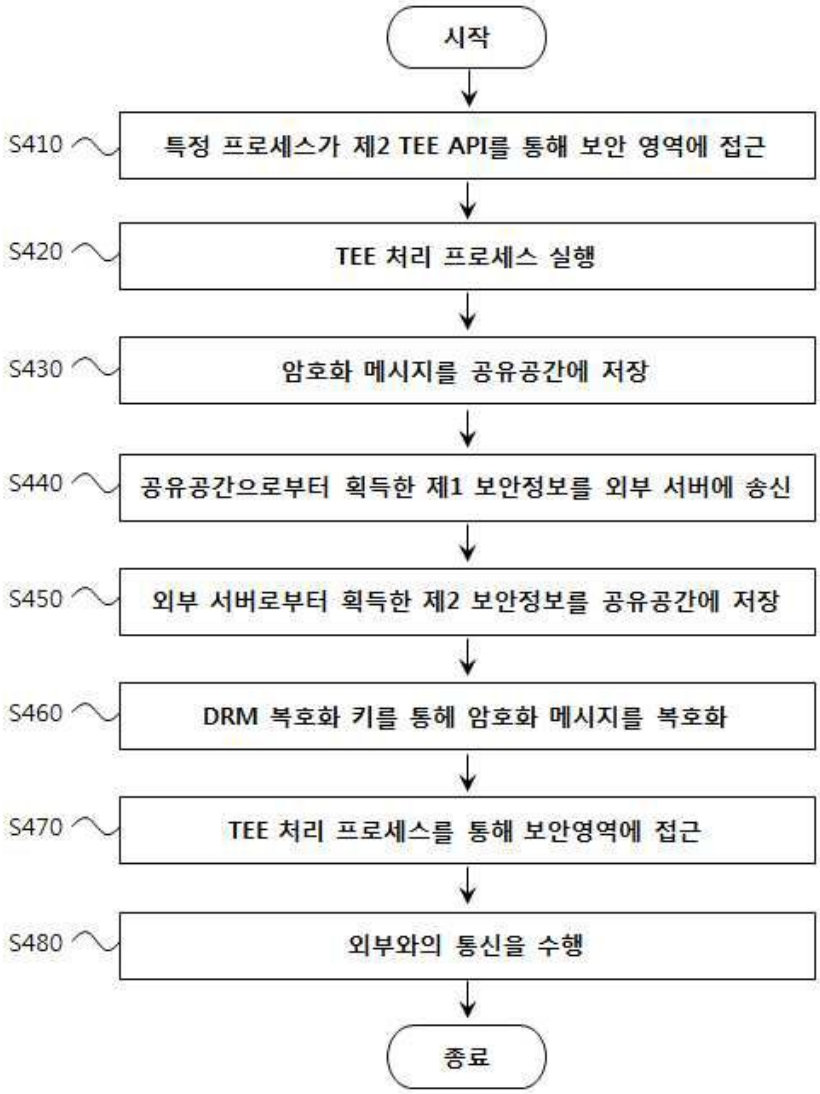
도면2


230
110
220
228
통신관리
프로세스
복호관리
프로세스
TEE 처리
프로세스
236
226
제2 TEE API
제1 TEE API
234
224
제2 운영체제
(Linux)
제1 운영체제
(Secure OS)
232
222
TEE 환경부
TEE 관리부
CPU
비보안
영역
공유
공간
보안영역
메모리
240
214
216
212
210

도면3


시작
S310
특정 프로세스가 제2 TEE API를 통해 보안 영역에 접근
S320
TEE 처리 프로세스 실행
S330
공유공간을 통해 TEE 처리 프로세스와 통신하도록 제어
종료

도면4


시작
S410
특정 프로세스가 제2 TEE API를 통해 보안 영역에 접근
S420
TEE 처리 프로세스 실행
S430
암호화 메시지를 공유공간에 저장
S440
공유공간으로부터 획득한 제1 보안정보를 외부 서버에 송신
S450
외부 서버로부터 획득한 제2 보안정보를 공유공간에 저장
S460
DRM 복호화 키를 통해 암호화 메시지를 복호화
S470
TEE 처리 프로세스를 통해 보안영역에 접근
S480
외부와의 통신을 수행
종료