

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2022년 5월 5일 (05.05.2022)



(10) 국제공개번호
WO 2022/092869 A1

(51) 국제특허분류:

G06F 21/53 (2013.01)

G06F 21/30 (2013.01)

G06F 21/60 (2013.01)

G06F 12/08 (2006.01)

(21) 국제출원번호: PCT/KR2021/015343

(22) 국제출원일: 2021년 10월 28일 (28.10.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2020-0141764 2020년 10월 29일 (29.10.2020) KR

(71) 출원인: 삼성전자 주식회사 (SAMSUNG ELECTRONICS CO., LTD.) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND

BUSINESS FOUNDATION) [KR/KR]; 02841 서울시 성북구 안암로 145, Seoul (KR).

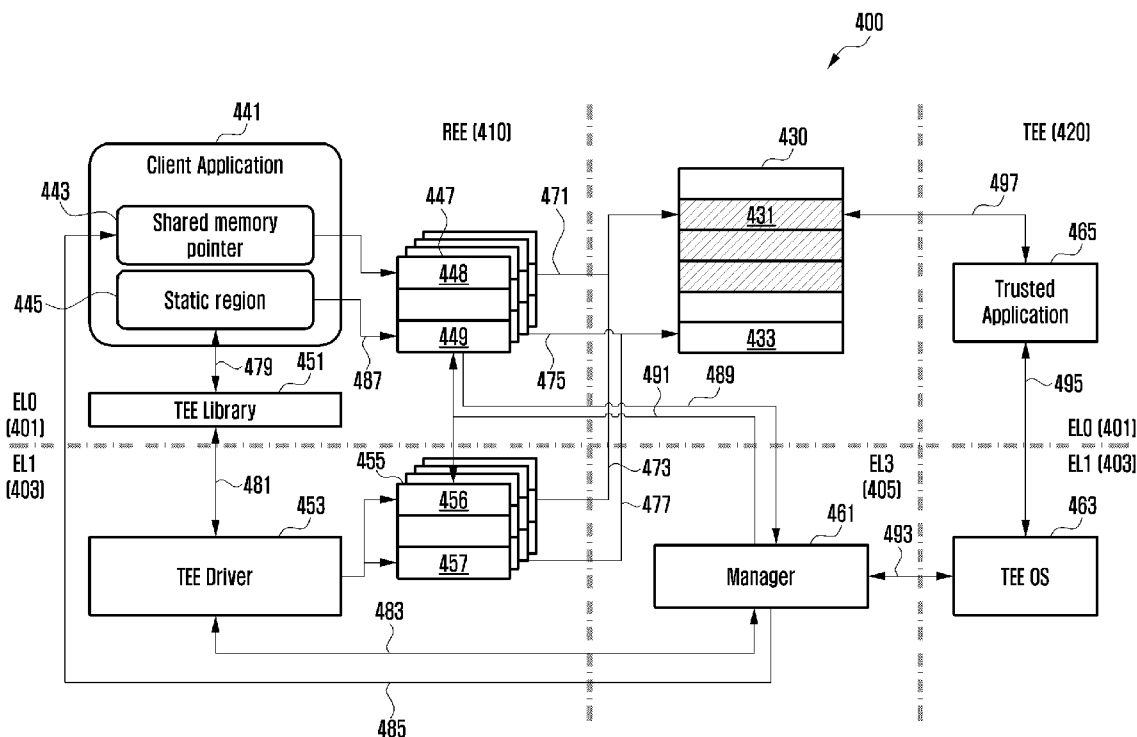
(72) 발명자: 심동욱 (SHIM, Dongwook); 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 이동훈 (LEE, Donghoon); 02841 서울시 성북구 안암로 145, Seoul (KR).

(74) 대리인: 윤앤리특허법인(유한) (YOON & LEE INTERNATIONAL PATENT & LAW FIRM); 08502 서울시 금천구 가산디지털1로 226, 에이스 하이엔드타워 5차 3층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW,

(54) Title: ELECTRONIC DEVICE AND MEMORY PROTECTION METHOD USING SAME

(54) 발명의 명칭: 전자 장치 및 이를 이용한 메모리 보호 방법



(57) Abstract: According to various embodiments disclosed herein, an electronic device comprises memory and a processor operatively connected to the memory, wherein the memory may store instructions which, upon execution, cause the processor to: allocate a first address space and a second address space to the memory in a rich execution environment on the basis of detecting a request to write data to the memory; write the data to the first address space of the memory and then detect access to the second address space in the rich execution environment; set the access permission of a first user virtual memory address space, mapped to the first address space in the memory, in the rich execution environment so that write access is deactivated by a trusted execution environment manager on the basis of detecting access to the second address space; set the access permission of a second user virtual memory address space, mapped to



KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK,
MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA,
PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,
SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역
내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE,
LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM,
ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유
럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK,
MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML,
MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

the second address space, in the rich execution environment so that read access is activated and write access is deactivated; and set the access permission of a first kernel virtual memory address space, mapped to the first address space in the memory, in the rich execution environment so that write access is deactivated by the trusted execution environment manager. Various other embodiments in addition to those disclosed in the present document are also possible.

(57) 요약서: 본 개시의 다양한 실시예들에 따르면, 전자 장치는, 메모리 및 상기 메모리와 작동적으로 연결된 프로세서를 포함하며, 상기 메모리는, 실행될 때, 상기 프로세서가, 상기 메모리에 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 일반 환경에서, 상기 메모리에 제1 주소 공간 및 제2 주소 공간을 할당하고, 상기 일반 환경에서, 상기 메모리의 상기 제1 주소 공간에 데이터를 쓴 후, 상기 제2 주소 공간으로의 접근을 검출하고, 상기 제2 주소 공간으로의 접근을 검출하는 것에 기반하여, 보안 환경의 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 사용자 가상 메모리 주소 공간의 접근 권한에 대한 쓰기 접근이 비활성화되게 설정하고, 상기 제2 주소 공간에 매핑된 상기 일반 환경의 및 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대한 읽기 접근(read access)이 활성화되고, 쓰기 접근(write access)이 비활성화되게 설정하고, 및 상기 보안 환경의 상기 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 커널 가상 메모리 주소 공간의 접근 권한에 대한 쓰기 접근이 비활성화되게 설정하도록 하는 인스트럭션들(instructions)을 저장할 수 있다. 본 문서에 개시된 다양한 실시예들 이외의 다른 다양한 실시예가 가능하다.

명세서

발명의 명칭: 전자 장치 및 이를 이용한 메모리 보호 방법

기술분야

- [1] 본 개시의 다양한 실시예들은, 전자 장치 및 이를 이용한 메모리 보호 방법에 관한 것이다.

배경기술

- [2] 보안 어플리케이션의 안전한 실행을 위하여, ARM 트러스트존(TrustZone) 기술과 같이 보안 환경(trusted execution environment, TEE)을 제공하는 기술이 개발되고 있다. 이러한 기술에서, 일반 환경(rich execution environment, REE) 또는 일반 영역(normal world)에서 일반 어플리케이션을 실행하고, 일반 영역으로부터 격리된(isolated) 보안 환경 또는 보안 영역(secure world)에서 보안 어플리케이션을 실행함으로써, 보안 어플리케이션의 안전한 실행을 보장할 수 있다. 또한, 일반 환경의 일반 어플리케이션은 보안 어플리케이션과 통신하기 위해 필요한 데이터를 공유 메모리(shared memory)에 저장하여 전달할 수 있으며, 보안 어플리케이션 또한 처리 결과를 공유 메모리에 저장하여 일반 어플리케이션에게 알려줄 수 있다.

발명의 상세한 설명

기술적 과제

- [3] 공유 메모리의 데이터 무결성(data integrity)을 보장하지 않고, 보안 어플리케이션의 호출에 대한 호출자 인증을 수행하지 않음에 따라, 공격자는 공유 메모리에 접근하여 데이터를 조작할 수 있다. 이를 방지하기 위해, 공유 메모리의 데이터를 암호화하는 방법을 통해 공격자가 데이터를 조작할 수 없도록 할 수 있다. 하지만, 공유 메모리의 데이터 암호화를 위해서는 일반 환경에서 대칭 키를 가지고 있어야 하기 때문에, 암호화가 수행되는 동안 대칭 키가 일반 환경의 메모리에 로딩될 수 있다. 이에 따라, 커널 권한을 가진 공격자가 일반 환경의 메모리에 접근함으로써 키 유출이 가능할 수 있다.
- [4] 본 개시의 다양한 실시예들에 따른 전자 장치는, 일반 환경의 일반 어플리케이션을 통해 공유 메모리에 데이터를 쓴(write) 후, 공유 메모리의 접근 권한을 읽기 접근만이 가능하도록 제어할 수 있다.

과제 해결 수단

- [5] 본 개시의 다양한 실시예들에 따른 전자 장치는, 메모리 및 상기 메모리와 작동적으로 연결된 프로세서를 포함하며, 상기 메모리는, 실행될 때, 상기 프로세서가, 상기 메모리에 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 일반 환경에서, 상기 메모리에 제1 주소 공간 및 제2 주소 공간을 할당하고, 상기 일반 환경에서, 상기 메모리의 상기 제1 주소 공간에 데이터를 쓴(write) 후, 상기 제2 주소 공간으로의 접근(access)을 검출하고, 상기 제2 주소 공간으로의 접근을

검출하는 것에 기반하여, 보안 환경의 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 사용자 가상 메모리 주소 공간의 접근 권한에 대한 쓰기 접근이 비활성화되게 설정하고, 상기 제2 주소 공간에 매핑된 상기 일반 환경의 제1 사용자 가상 메모리 주소 공간 및 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대한 읽기 접근(read access)이 활성화되고, 쓰기 접근(write access)이 비활성화되게 설정하고, 및 상기 보안 환경의 상기 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 커널 가상 메모리 주소 공간의 접근 권한에 대한 읽기 접근이 활성화되고, 쓰기 접근이 비활성화되게 설정하도록 하는 인스트럭션들(instructions)을 저장할 수 있다.

- [6] 본 개시의 다양한 실시예들에 따른 전자 장치의 메모리 보호 방법은, 메모리에 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 일반 환경에서, 상기 메모리에 제1 주소 공간 및 제2 주소 공간을 할당하는 동작, 상기 일반 환경에서, 상기 메모리의 상기 제1 주소 공간에 데이터를 쓴(write) 후, 상기 제2 주소 공간으로의 접근을 검출하는 동작, 상기 제2 주소 공간으로의 접근을 검출하는 것에 기반하여, 보안 환경의 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 사용자 가상 메모리 주소 공간의 접근 권한에 대한 쓰기 접근이 비활성화되게 설정하고, 상기 제2 주소 공간에 매핑된 상기 일반 환경의 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대한 읽기 접근(read access)이 활성화되고, 쓰기 접근(write access)이 비활성화되게 설정하는 동작, 및 상기 보안 환경의 상기 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 커널 가상 메모리 주소 공간의 접근 권한에 대한 쓰기 접근이 비활성화되게 설정하는 동작을 포함할 수 있다.

발명의 효과

- [7] 본 개시의 다양한 실시예들에 따른 전자 장치는, 일반 환경의 일반 어플리케이션을 통해 공유 메모리에 데이터를 쓴(write) 후, 공유 메모리의 접근 권한을 읽기 접근만이 가능하도록 변경함에 따라, 커널 권한을 가지는 공격자가 공유 메모리의 데이터를 조작할 수 없도록 할 수 있다. 이에 따라, 공유 메모리의 보안을 강화시킬 수 있다.

도면의 간단한 설명

- [8] 도 1은, 다양한 실시예들에 따른, 네트워크 환경 내의 전자 장치의 블록도이다.
 [9] 도 2는, 다양한 실시예들에 따른, 전자 장치에서 운용되는 REE(rich execution environment) 및 TEE(trusted execution environment)를 도시하는 블록도이다.
 [10] 도 3은, 다양한 실시예들에 따른, 전자 장치를 도시한 블록도이다.
 [11] 도 4는, 다양한 실시예들에 따른, 전자 장치에서 운용되는 REE(rich execution environment) 및 TEE(trusted execution environment) 간 신호 흐름을 도시하는 도면이다.

[12] 도 5는, 다양한 실시예들에 따른, 페이지 디스크립터(page descriptor)를 도시한 도면이다.

[13] 도 6은, 다양한 실시예들에 따른, 메모리 보호 방법을 설명하기 위한 흐름도이다.

발명의 실시를 위한 최선의 형태

[14] 도 1은, 다양한 실시예들에 따른, 네트워크 환경(100) 내의 전자 장치(101)의 블록도이다.

[15] 도 1을 참조하면, 네트워크 환경(100)에서 전자 장치(101)는 제1 네트워크(198)(예: 근거리 무선 통신 네트워크)를 통하여 전자 장치(102)와 통신하거나, 또는 제2 네트워크(199)(예: 원거리 무선 통신 네트워크)를 통하여 전자 장치(104) 또는 서버(108)와 통신할 수 있다. 일 실시예에 따르면, 전자 장치(101)는 서버(108)를 통하여 전자 장치(104)와 통신할 수 있다. 일 실시예에 따르면, 전자 장치(101)는 프로세서(120), 메모리(130), 입력 모듈(150), 음향 출력 모듈(155), 디스플레이 모듈(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 연결 단자(178), 햅틱 모듈(179), 카메라 모듈(180), 전력 관리 모듈(188), 배터리(189), 통신 모듈(190), 가입자 식별 모듈(196), 또는 안테나 모듈(197)을 포함할 수 있다. 어떤 실시예에서는, 전자 장치(101)에는, 이 구성요소들 중 적어도 하나(예: 연결 단자(178))가 생략되거나, 하나 이상의 다른 구성요소가 추가될 수 있다. 어떤 실시예에서는, 이 구성요소들 중 일부들(예: 센서 모듈(176), 카메라 모듈(180), 또는 안테나 모듈(197))은 하나의 구성요소(예: 디스플레이 모듈(160))로 통합될 수 있다.

[16] 프로세서(120)는, 예를 들면, 소프트웨어(예: 프로그램(140))를 실행하여 프로세서(120)에 연결된 전자 장치(101)의 적어도 하나의 다른 구성요소(예: 하드웨어 또는 소프트웨어 구성요소)를 제어할 수 있고, 다양한 데이터 처리 또는 연산을 수행할 수 있다. 일 실시예에 따르면, 데이터 처리 또는 연산의 적어도 일부로서, 프로세서(120)는 다른 구성요소(예: 센서 모듈(176) 또는 통신 모듈(190))로부터 수신된 명령 또는 데이터를 휘발성 메모리(132)에 저장하고, 휘발성 메모리(132)에 저장된 명령 또는 데이터를 처리하고, 결과 데이터를 비휘발성 메모리(134)에 저장할 수 있다. 일 실시예에 따르면, 프로세서(120)는 메인 프로세서(121)(예: 중앙 처리 장치 또는 어플리케이션 프로세서) 또는 이와는 독립적으로 또는 함께 운영 가능한 보조 프로세서(123)(예: 그래픽 처리 장치, 신경망 처리 장치(NPU: neural processing unit), 이미지 시그널 프로세서, 센서 허브 프로세서, 또는 커뮤니케이션 프로세서)를 포함할 수 있다. 예를 들어, 전자 장치(101)가 메인 프로세서(121) 및 보조 프로세서(123)를 포함하는 경우, 보조 프로세서(123)는 메인 프로세서(121)보다 저전력을 사용하거나, 지정된 기능에 특화되도록 설정될 수 있다. 보조 프로세서(123)는 메인 프로세서(121)와 별개로, 또는 그 일부로서 구현될 수 있다.

- [17] 보조 프로세서(123)는, 예를 들면, 메인 프로세서(121)가 인액티브(예: 슬립) 상태에 있는 동안 메인 프로세서(121)를 대신하여, 또는 메인 프로세서(121)가 액티브(예: 어플리케이션 실행) 상태에 있는 동안 메인 프로세서(121)와 함께, 전자 장치(101)의 구성요소들 중 적어도 하나의 구성요소(예: 디스플레이 모듈(160), 센서 모듈(176), 또는 통신 모듈(190))와 관련된 기능 또는 상태들의 적어도 일부를 제어할 수 있다. 일 실시예에 따르면, 보조 프로세서(123)(예: 이미지 시그널 프로세서 또는 커뮤니케이션 프로세서)는 기능적으로 관련 있는 다른 구성요소(예: 카메라 모듈(180) 또는 통신 모듈(190))의 일부로서 구현될 수 있다. 일 실시예에 따르면, 보조 프로세서(123)(예: 신경망 처리 장치)는 인공지능 모델의 처리에 특화된 하드웨어 구조를 포함할 수 있다. 인공지능 모델은 기계 학습을 통해 생성될 수 있다. 이러한 학습은, 예를 들어, 인공지능이 수행되는 전자 장치(101) 자체에서 수행될 수 있고, 별도의 서버(예: 서버(108))를 통해 수행될 수도 있다. 학습 알고리즘은, 예를 들어, 지도형 학습(supervised learning), 비지도형 학습(unsupervised learning), 준지도형 학습(semi-supervised learning) 또는 강화 학습(reinforcement learning)을 포함할 수 있으나, 전술한 예에 한정되지 않는다. 인공지능 모델은, 복수의 인공 신경망 레이어들을 포함할 수 있다. 인공 신경망은 심층 신경망(DNN: deep neural network), CNN(convolutional neural network), RNN(recurrent neural network), RBM(restricted boltzmann machine), DBN(deep belief network), BRDNN(bidirectional recurrent deep neural network), 심층 Q-네트워크(deep Q-networks) 또는 상기 중 둘 이상의 조합 중 하나일 수 있으나, 전술한 예에 한정되지 않는다. 인공지능 모델은 하드웨어 구조 이외에, 추가적으로 또는 대체적으로, 소프트웨어 구조를 포함할 수 있다.
- [18] 메모리(130)는, 전자 장치(101)의 적어도 하나의 구성요소(예: 프로세서(120) 또는 센서 모듈(176))에 의해 사용되는 다양한 데이터를 저장할 수 있다. 데이터는, 예를 들어, 소프트웨어(예: 프로그램(140)) 및, 이와 관련된 명령에 대한 입력 데이터 또는 출력 데이터를 포함할 수 있다. 메모리(130)는, 휘발성 메모리(132) 또는 비휘발성 메모리(134)를 포함할 수 있다.
- [19] 프로그램(140)은 메모리(130)에 소프트웨어로서 저장될 수 있으며, 예를 들면, 운영 체제(142), 미들 웨어(144) 또는 어플리케이션(146)을 포함할 수 있다.
- [20] 입력 모듈(150)은, 전자 장치(101)의 구성요소(예: 프로세서(120))에 사용될 명령 또는 데이터를 전자 장치(101)의 외부(예: 사용자)로부터 수신할 수 있다. 입력 모듈(150)은, 예를 들면, 마이크, 마우스, 키보드, 키(예: 버튼), 또는 디지털 펜(예: 스타일러스 펜)을 포함할 수 있다.
- [21] 음향 출력 모듈(155)은 음향 신호를 전자 장치(101)의 외부로 출력할 수 있다. 음향 출력 모듈(155)은, 예를 들면, 스피커 또는 리시버를 포함할 수 있다. 스피커는 멀티미디어 재생 또는 녹음 재생과 같이 일반적인 용도로 사용될 수 있다. 리시버는 착신 전화를 수신하기 위해 사용될 수 있다. 일 실시예에 따르면, 리시버는 스피커와 별개로, 또는 그 일부로서 구현될 수 있다.

- [22] 디스플레이 모듈(160)은 전자 장치(101)의 외부(예: 사용자)로 정보를 시각적으로 제공할 수 있다. 디스플레이 모듈(160)은, 예를 들면, 디스플레이, 홀로그램 장치, 또는 프로젝터 및 해당 장치를 제어하기 위한 제어 회로를 포함할 수 있다. 일 실시예에 따르면, 디스플레이 모듈(160)은 터치를 감지하도록 설정된 터치 센서, 또는 상기 터치에 의해 발생하는 힘의 세기를 측정하도록 설정된 압력 센서를 포함할 수 있다.
- [23] 오디오 모듈(170)은 소리를 전기 신호로 변환시키거나, 반대로 전기 신호를 소리로 변환시킬 수 있다. 일 실시예에 따르면, 오디오 모듈(170)은, 입력 모듈(150)을 통해 소리를 획득하거나, 음향 출력 모듈(155), 또는 전자 장치(101)와 직접 또는 무선으로 연결된 외부 전자 장치(예: 전자 장치(102))(예: 스피커 또는 헤드폰)를 통해 소리를 출력할 수 있다.
- [24] 센서 모듈(176)은 전자 장치(101)의 작동 상태(예: 전력 또는 온도), 또는 외부의 환경 상태(예: 사용자 상태)를 감지하고, 감지된 상태에 대응하는 전기 신호 또는 데이터 값을 생성할 수 있다. 일 실시예에 따르면, 센서 모듈(176)은, 예를 들면, 제스처 센서, 자이로 센서, 기압 센서, 마그네틱 센서, 가속도 센서, 그립 센서, 근접 센서, 컬러 센서, IR(infrared) 센서, 생체 센서, 온도 센서, 습도 센서, 또는 조도 센서를 포함할 수 있다.
- [25] 인터페이스(177)는 전자 장치(101)가 외부 전자 장치(예: 전자 장치(102))와 직접 또는 무선으로 연결되기 위해 사용될 수 있는 하나 이상의 지정된 프로토콜들을 지원할 수 있다. 일 실시예에 따르면, 인터페이스(177)는, 예를 들면, HDMI(high definition multimedia interface), USB(universal serial bus) 인터페이스, SD카드 인터페이스, 또는 오디오 인터페이스를 포함할 수 있다.
- [26] 연결 단자(178)는, 그를 통해서 전자 장치(101)가 외부 전자 장치(예: 전자 장치(102))와 물리적으로 연결될 수 있는 커넥터를 포함할 수 있다. 일 실시예에 따르면, 연결 단자(178)는, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.
- [27] 햅틱 모듈(179)은 전기적 신호를 사용자가 촉각 또는 운동 감각을 통해서 인지할 수 있는 기계적인 자극(예: 진동 또는 움직임) 또는 전기적인 자극으로 변환할 수 있다. 일 실시예에 따르면, 햅틱 모듈(179)은, 예를 들면, 모터, 압전 소자, 또는 전기 자극 장치를 포함할 수 있다.
- [28] 카메라 모듈(180)은 정지 영상 및 동영상을 촬영할 수 있다. 일 실시예에 따르면, 카메라 모듈(180)은 하나 이상의 렌즈들, 이미지 센서들, 이미지 시그널 프로세서들, 또는 플래시들을 포함할 수 있다.
- [29] 전력 관리 모듈(188)은 전자 장치(101)에 공급되는 전력을 관리할 수 있다. 일 실시예에 따르면, 전력 관리 모듈(188)은, 예를 들면, PMIC(power management integrated circuit)의 적어도 일부로서 구현될 수 있다.
- [30] 배터리(189)는 전자 장치(101)의 적어도 하나의 구성요소에 전력을 공급할 수 있다. 일 실시예에 따르면, 배터리(189)는, 예를 들면, 재충전 불가능한 1차 전지,

재충전 가능한 2차 전지 또는 연료 전지를 포함할 수 있다.

- [31] 통신 모듈(190)은 전자 장치(101)와 외부 전자 장치(예: 전자 장치(102), 전자 장치(104), 또는 서버(108)) 간의 직접(예: 유선) 통신 채널 또는 무선 통신 채널의 수립, 및 수립된 통신 채널을 통한 통신 수행을 지원할 수 있다. 통신 모듈(190)은 프로세서(120)(예: 어플리케이션 프로세서)와 독립적으로 운영되고, 직접(예: 유선) 통신 또는 무선 통신을 지원하는 하나 이상의 커뮤니케이션 프로세서를 포함할 수 있다. 일 실시예에 따르면, 통신 모듈(190)은 무선 통신 모듈(192)(예: 셀룰러 통신 모듈, 근거리 무선 통신 모듈, 또는 GNSS(global navigation satellite system) 통신 모듈) 또는 유선 통신 모듈(194)(예: LAN(local area network) 통신 모듈, 또는 전력선 통신 모듈)을 포함할 수 있다. 이들 통신 모듈 중 해당하는 통신 모듈은 제1 네트워크(198)(예: 블루투스, WiFi(wireless fidelity) direct 또는 IrDA(infrared data association)와 같은 근거리 통신 네트워크) 또는 제2 네트워크(199)(예: 레거시 셀룰러 네트워크, 5G 네트워크, 차세대 통신 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN)와 같은 원거리 통신 네트워크)를 통하여 외부의 전자 장치(104)와 통신할 수 있다. 이런 여러 종류의 통신 모듈들은 하나의 구성요소(예: 단일 칩)로 통합되거나, 또는 서로 별도의 복수의 구성요소들(예: 복수 칩들)로 구현될 수 있다. 무선 통신 모듈(192)은 가입자 식별 모듈(196)에 저장된 가입자 정보(예: 국제 모바일 가입자 식별자(IMSI))를 이용하여 제1 네트워크(198) 또는 제2 네트워크(199)와 같은 통신 네트워크 내에서 전자 장치(101)를 확인 또는 인증할 수 있다.
- [32] 무선 통신 모듈(192)은 4G 네트워크 이후의 5G 네트워크 및 차세대 통신 기술, 예를 들어, NR 접속 기술(new radio access technology)을 지원할 수 있다. NR 접속 기술은 고용량 데이터의 고속 전송(eMBB(enhanced mobile broadband)), 단말 전력 최소화 및 다수 단말의 접속(mMTC(massive machine type communications)), 또는 고신뢰도와 저지연(URLLC(ultra-reliable and low-latency communications))을 지원할 수 있다. 무선 통신 모듈(192)은, 예를 들어, 높은 데이터 전송률 달성을 위해, 고주파 대역(예: mmWave 대역)을 지원할 수 있다. 무선 통신 모듈(192)은 고주파 대역에서의 성능 확보를 위한 다양한 기술들, 예를 들어, 빔포밍(beamforming), 거대 배열 다중 입출력(massive MIMO(multiple-input and multiple-output)), 전차원 다중입출력(FD-MIMO: full dimensional MIMO), 어레이 안테나(array antenna), 아날로그 빔형성(analog beam-forming), 또는 대규모 안테나(large scale antenna)와 같은 기술들을 지원할 수 있다. 무선 통신 모듈(192)은 전자 장치(101), 외부 전자 장치(예: 전자 장치(104)) 또는 네트워크 시스템(예: 제2 네트워크(199))에 규정되는 다양한 요구사항을 지원할 수 있다. 일 실시예에 따르면, 무선 통신 모듈(192)은 eMBB 실현을 위한 Peak data rate(예: 20Gbps 이상), mMTC 실현을 위한 손실 Coverage(예: 164dB 이하), 또는 URLLC 실현을 위한 U-plane latency(예: 다운링크(DL) 및 업링크(UL) 각각 0.5ms 이하, 또는 라운드 트립 1ms 이하)를 지원할 수 있다.

- [33] 안테나 모듈(197)은 신호 또는 전력을 외부(예: 외부의 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 일 실시예에 따르면, 안테나 모듈(197)은 서브스트레이트(예: PCB) 위에 형성된 도전체 또는 도전성 패턴으로 이루어진 방사체를 포함하는 안테나를 포함할 수 있다. 일 실시예에 따르면, 안테나 모듈(197)은 복수의 안테나들(예: 어레이 안테나)을 포함할 수 있다. 이런 경우, 제1 네트워크(198) 또는 제2 네트워크(199)와 같은 통신 네트워크에서 사용되는 통신 방식에 적합한 적어도 하나의 안테나가, 예를 들면, 통신 모듈(190)에 의하여 상기 복수의 안테나들로부터 선택될 수 있다. 신호 또는 전력은 상기 선택된 적어도 하나의 안테나를 통하여 통신 모듈(190)과 외부의 전자 장치 간에 송신되거나 수신될 수 있다. 어떤 실시예에 따르면, 방사체 이외에 다른 부품(예: RFIC(radio frequency integrated circuit))이 추가로 안테나 모듈(197)의 일부로 형성될 수 있다.
- [34] 다양한 실시예에 따르면, 안테나 모듈(197)은 mmWave 안테나 모듈을 형성할 수 있다. 일 실시예에 따르면, mmWave 안테나 모듈은 인쇄 회로 기판, 상기 인쇄 회로 기판의 제1 면(예: 아래 면)에 또는 그에 인접하여 배치되고 지정된 고주파 대역(예: mmWave 대역)을 지원할 수 있는 RFIC, 및 상기 인쇄 회로 기판의 제2 면(예: 윗 면 또는 측 면)에 또는 그에 인접하여 배치되고 상기 지정된 고주파 대역의 신호를 송신 또는 수신할 수 있는 복수의 안테나들(예: 어레이 안테나)을 포함할 수 있다.
- [35] 상기 구성요소들 중 적어도 일부는 주변 기기들간 통신 방식(예: 버스, GPIO(general purpose input and output), SPI(serial peripheral interface), 또는 MIPI(mobile industry processor interface))를 통해 서로 연결되고 신호(예: 명령 또는 데이터)를 상호간에 교환할 수 있다.
- [36] 일 실시예에 따르면, 명령 또는 데이터는 제2 네트워크(199)에 연결된 서버(108)를 통해서 전자 장치(101)와 외부의 전자 장치(104) 간에 송신 또는 수신될 수 있다. 외부의 전자 장치(102, 또는 104) 각각은 전자 장치(101)와 동일한 또는 다른 종류의 장치일 수 있다. 일 실시예에 따르면, 전자 장치(101)에서 실행되는 동작들의 전부 또는 일부는 외부의 전자 장치들(102, 104, 또는 108) 중 하나 이상의 외부의 전자 장치들에서 실행될 수 있다. 예를 들면, 전자 장치(101)가 어떤 기능이나 서비스를 자동으로, 또는 사용자 또는 다른 장치로부터의 요청에 반응하여 수행해야 할 경우에, 전자 장치(101)는 기능 또는 서비스를 자체적으로 실행시키는 대신에 또는 추가적으로, 하나 이상의 외부의 전자 장치들에게 그 기능 또는 그 서비스의 적어도 일부를 수행하라고 요청할 수 있다. 상기 요청을 수신한 하나 이상의 외부의 전자 장치들은 요청된 기능 또는 서비스의 적어도 일부, 또는 상기 요청과 관련된 추가 기능 또는 서비스를 실행하고, 그 실행의 결과를 전자 장치(101)로 전달할 수 있다. 전자 장치(101)는 상기 결과를, 그대로 또는 추가적으로 처리하여, 상기 요청에 대한 응답의 적어도 일부로서 제공할 수 있다. 이를 위하여, 예를 들면, 클라우드

컴퓨팅, 분산 컴퓨팅, 모바일 에지 컴퓨팅(MEC: mobile edge computing), 또는 클라이언트-서버 컴퓨팅 기술이 이용될 수 있다. 전자 장치(101)는, 예를 들어, 분산 컴퓨팅 또는 모바일 에지 컴퓨팅을 이용하여 초저지연 서비스를 제공할 수 있다. 다른 실시예에 있어서, 외부의 전자 장치(104)는 IoT(internet of things) 기기를 포함할 수 있다. 서버(108)는 기계 학습 및/또는 신경망을 이용한 지능형 서버일 수 있다. 일 실시예에 따르면, 외부의 전자 장치(104) 또는 서버(108)는 제2 네트워크(199) 내에 포함될 수 있다. 전자 장치(101)는 5G 통신 기술 및 IoT 관련 기술을 기반으로 지능형 서비스(예: 스마트 홈, 스마트 시티, 스마트 카, 또는 헬스케어)에 적용될 수 있다.

- [37] 도 2는, 다양한 실시예들에 따른, 전자 장치(201)에서 운용되는 REE(rich execution environment)(210) 및 TEE(trusted execution environment)(220)를 도시하는 블록도(200)이다.
- [38] 다양한 실시예들에 따르면, 전자 장치(201)(예: 전자 장치(101))는 보안 강화를 위해 복수의 보안 레벨들을 가지는 복수의 실행 환경을 운용할 수 있다. 복수의 실행 환경은, 예를 들면, REE(210) 및 TEE(220)를 포함할 수 있다. REE(210)는, 예를 들면, 제1 보안 레벨을 가지는 제1 실행 환경일 수 있다. TEE(220)는, 예를 들면, 제1 보안 레벨과 다른(예: 높은) 제2 보안 레벨을 가지는 제2 실행 환경일 수 있다. 한 실시예에 따르면, 전자 장치(201)는 제3 보안 레벨을 가지는 추가적인 다른 실행 환경(예: 제3 실행 환경)을 포함할 수 있으며, 이에 한정하는 것은 아니다.
- [39] TEE(220)는 상대적으로 높은 보안 레벨이 요구되는 데이터를 안전한 환경 내에서 저장하고 관련 동작을 수행할 수 있다. TEE(220)는 전자 장치(201)의 어플리케이션 프로세서(application processor, AP)(예: 도 1의 메인 프로세서(121)) 상에서 동작하고, 전자 장치(201)의 제조 과정에서 결정된 신뢰할 수 있는 하드웨어 구조에 기반하여 동작할 수 있다. TEE(220)는 어플리케이션 프로세서 또는 메모리(예: 도 1의 메모리(130))를 일반 영역(또는 일반 환경)과 보안 영역(또는 보안 환경)으로 구분하여 보안 영역에서 동작할 수 있다. TEE(220)는 보안이 필요한 소프트웨어나 하드웨어를 보안 영역에서만 동작하게 하도록 설정할 수 있다. 전자 장치(201)는 하드웨어의 물리적 변경 또는 소프트웨어의 논리적 변경을 통하여 TEE(220)를 운용할 수 있다.
- [40] TEE(220)는 REE(210)와 하드웨어적인 제약을 통하여 서로 분리될 수 있고, 동일한 하드웨어에서 소프트웨어적으로 분리되어 동작할 수 있다. REE(210)에서 동작하는 적어도 하나의 어플리케이션(client application, CA)(240)(예: 결제, 컨택트, 이메일, 또는 브라우저)은 TEE(220)에 접근이 허용된 API(예: TEE functional API(application programming interface)(221) 또는 TEE client API(223))를 이용할 수 있다. REE(210)에서 동작하는 적어도 하나의 어플리케이션(240)은 API(예: 221, 223)를 이용하여 REE 통신 에이전트(REE communication agent)(215)에서 TEE 통신 에이전트(TEE communication

agent)(225)로 메시지(messages)(251)를 전달할 수 있다. 메시지(251)는 하드웨어적으로 또는 소프트웨어적으로 TEE(220)에만 전달될 수 있도록 구현될 수 있다. REE(210)는 운영체제(예: rich OS components(211))를 포함할 수 있으며, 주변 장치(public peripherals)(212) 제어를 위한 드라이버(public device drivers)(213)를 운용할 수 있다.

- [41] TEE 통신 에이전트(225)는 메시지(251)를 수신하여 메시지(251)와 관련된 보안 어플리케이션(trusted application, TA)(231)(예: DRM(digital right management), 보안 결제 모듈, 또는 보안 생체 정보 모듈)에 전달할 수 있다. 보안 어플리케이션(231)은 메시지(251)에 관련된 동작을 수행할 수 있으며, 동작에 대한 결과를 TEE 통신 에이전트(225)를 통하여 REE 통신 에이전트(215)에 전달할 수 있다. REE 통신 에이전트(215)는 REE(210)에서 운용 중인 적어도 하나의 어플리케이션(240)에 상기 결과를 전달할 수 있다. TEE(220)는 내부 API(TEE internal API)(261)를 기반으로 보안 어플리케이션(231)을 운용하는 보안 운영 체제(trusted OS components)(263)를 포함할 수 있다. 보안 운영 체제(263)는 보안 주변 장치(trusted peripherals)(264) 제어를 위한 보안 커널(trusted kernel)(265) 및 보안 프레임 워크(trusted core framework)(267) 및/또는 보안 함수(trusted functions)(269)를 포함할 수 있다.
- [42] 이하, 다양한 실시예들에 따라 REE(210)를 일반 환경으로, TEE(220)를 보안 환경으로 정의하여 설명하기로 한다.
- [43] 도 3은, 다양한 실시예들에 따른, 전자 장치(301)를 도시한 블록도(300)이다.
- [44] 도 3을 참조하면, 전자 장치(301)(예: 도 1의 전자 장치(101) 및 도 2의 전자 장치(201))는 무선 통신 회로(310)(예: 도 1의 통신 모듈(190)), 메모리(320)(예: 도 1의 메모리(130)), 및/또는 프로세서(330)(예: 도 1의 프로세서(120))를 포함할 수 있다.
- [45] 본 개시의 다양한 실시예들에 따르면, 무선 통신 회로(310)(예: 도 1의 통신 모듈(190))는 외부 전자 장치(예: 도 1의 전자 장치(102, 104), 서버(108))와 통신 채널을 수립하고, 외부 전자 장치와 다양한 데이터를 송수신하도록 지원할 수 있다.
- [46] 일 실시예에서, 무선 통신 회로(310)는 프로세서(330)의 제어 하에 어플리케이션 제공 서버로부터 클라이언트 어플리케이션을 다운로드 할 수 있으며, 보안 인증 서버를 통해 공개 키를 수신함으로써 인증 동작을 수행할 수 있다.
- [47] 본 개시의 다양한 실시예들에 따르면, 메모리(320)(예: 도 1의 메모리(130))는 REE(321)(예: 도 2의 REE(rich execution environment)(210))(이하, 일반 환경) 및 TEE(323)(예: 도 2의 TEE(trusted execution environment)(220))(이하, 보안 환경)을 포함할 수 있다.
- [48] 일 실시예에서, 보안 환경(323)은 전자 장치(301)와 관련된 보안 시스템을 포함할 수 있다. 예컨대, 전자 장치(301)는 보안 환경(323)을 이용하여 외부의

- 요청, 수정, 또는 입력과 관련된 제어로부터 보안 환경(323)에 포함되거나, 또는 저장된 정보를 보호할 수 있다. 일 실시예에서, 보안 환경(323)은 보안 어플리케이션을 실행하거나 암호화된 정보를 관리할 수 있다.
- [49] 일 실시예에서, 일반 환경(321)은 어플리케이션 계층을 포함할 수 있으며, 보안 환경(323)과 달리 외부로부터의 접근 및/또는 제어를 허용할 수 있다.
- [50] 전술한 일반 환경(321) 및 보안 환경(323)과 관련하여, 후술하는 도 4 및 도 5에서 다양한 실시예들이 설명될 것이다.
- [51] 본 개시의 다양한 실시예들에 따르면, 프로세서(330)(예: 도 1의 프로세서(120))는 전자 장치(301)의 전반적인 동작 및 전자 장치(301)의 내부 구성들 간의 신호 흐름을 제어하고, 데이터 처리를 수행할 수 있다.
- [52] 일 실시예에서, 프로세서(330)는 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 메모리(320)에 제1 주소 공간 및 제2 주소 공간을 할당할 수 있다. 프로세서(330)는 메모리(320)의 제1 주소 공간 및 제2 주소 공간을 일반 환경(321)의 제1 페이지 테이블의 제1 사용자 가상 메모리 주소 공간 및 제2 사용자 가상 메모리 주소 공간에 매핑 할 수 있다. 프로세서(330)는 메모리(320)의 제1 주소 공간 및 제2 주소 공간을 일반 환경(321)의 제2 페이지 테이블의 제1 커널 가상 메모리 주소 공간 및 제2 커널 가상 메모리 주소 공간에 매핑 할 수 있다.
- [53] 일 실시예에서, 프로세서(330)는 메모리(320)의 제1 주소 공간 및 제2 주소 공간의 가상 메모리 주소와 커널에서 관리하고 있는 호출자 정보(예: 프로세서의 메모리 공간 정보)를 보안 환경(323)의 매니저에 전달할 수 있다.
- [54] 일 실시예에서, 프로세서(330)는 클라이언트 어플리케이션(예: 도 2의 클라이언트 어플리케이션(240))의 정적 영역에 대해 페이지 단위 별로 제1 해시 값을 생성할 수 있다. 프로세서(330)는 제1 해시 값과 기 저장된 클라이언트 어플리케이션(240)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값(예: 컴파일 시 생성된 제2 해시 값)을 비교하고, 비교 결과에 기반하여, 제1 해시 값과 제2 해시 값이 동일한지 여부를 확인하는 클라이언트 어플리케이션(441)의 정적 영역 중 로드(load)된 페이지에 대한 제1 호출자 인증을 수행할 수 있다.
- [55] 일 실시예에서, 제1 해시 값과 제2 해시 값이 동일한 것으로 결정되면, 프로세서(330)는 제1 호출자 인증을 성공한 것으로 결정하고, 메모리(320)의 제2 주소 공간에 매핑된 제2 사용자 가상 메모리 주소 공간에 대한 접근 권한을 읽기 접근 및 쓰기 접근이 비활성화되게 설정할 수 있다.
- [56] 일 실시예에서, 프로세서(330)는 메모리(320)의 제1 주소 공간에 데이터를 쓴(write) 후, 제2 주소 공간으로의 읽기(read)를 검출할 수 있다. 프로세서(330)는 제2 주소 공간의 접근 권한을 읽기 접근 및 쓰기 접근이 비활성화되게 설정하였으나, 읽기 접근이 검출됨에 따라 읽기 권한 오류(reading permission fault)를 발생시킬 수 있으며, 이에 기반하여 읽기 권한 오류가 메모리(320)의 제2 주소 공간에서 발생한 것인지 여부를 확인할 수 있다. 읽기 권한 오류가

메모리(320)의 제2 주소 공간에서 발생한 것으로 확인되는 것에 기반하여, 프로세서(330)는 제1 호출자 인증이 수행되지 않은 정적 영역(예: 클라이언트 어플리케이션(240)의 정적 영역)의 로드된 페이지에 대해 검증을 수행하는 제2 호출자 인증을 수행할 수 있다. 제2 호출자 인증이 성공한 것으로 결정되면, 프로세서(330)는 제1 사용자 가상 메모리 주소 공간 및 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대한 읽기 접근이 활성화되고, 쓰기 접근이 비활성화되게 설정 할 수 있다.

- [57] 도 4는, 다양한 실시예들에 따른, 전자 장치(301)에서 운용되는 REE(rich execution environment)(410) 및 TEE(trusted execution environment)(420) 간 신호 흐름을 도시하는 도면(400)이다.
- [58] 본 개시의 다양한 실시예들에 따른 REE(rich execution environment)(410)(예: 도 3의 REE(321))(이하, 일반 환경) 및 TEE(trusted execution environment)(420)(예: 도 3의 TEE(323))(이하, 보안 환경)는 복수의 익셉션 레벨(exception level)들로 구분될 수 있다. 복수의 익셉션 레벨들은 제1 익셉션 레벨(예: EL0(401)), 제2 익셉션 레벨(예: EL1(403)), 제3 익셉션 레벨(EL2)(미도시), 및 제4 익셉션 레벨(예: EL3(405))을 포함할 수 있다.
- [59] 일 실시예에서, 일반 환경(410) 및 보안 환경(420)의 제1 익셉션 레벨(EL0(401))은 사용자 공간(user space)을 포함할 수 있다. 사용자 공간은 어플리케이션(예: 클라이언트 어플리케이션(441))을 구동할 수 있다.
- [60] 일 실시예에서, 일반 환경(410) 및 보안 환경(420)의 제2 익셉션 레벨(EL1(403))은 커널 공간(kernel space)을 포함할 수 있다. 커널 공간은 다른 프로그램들에 구현된 동작 또는 기능을 실행하는 데 사용되는 시스템 리소스들을 제어 또는 관리할 수 있다. 커널 공간은 미들웨어, API, 또는 어플리케이션 프로그램에서 전자 장치(예: 도 3의 전자 장치(301))의 개별 구성요소에 접근함으로써, 시스템 리소스들을 제어 또는 관리할 수 있는 인터페이스를 제공할 수 있다.
- [61] 일 실시예에서, 보안 환경(420)의 제4 익셉션 레벨(EL3(405))은 보안 공간(secure space)을 포함할 수 있다. 예컨대, 보안 공간은 보안 모니터(secure monitor) 공간으로, 일반 환경(410)과 보안 환경(420)의 주소 공간을 전환할 수 있도록 지원하는 인터페이스 역할을 할 수 있다. 예컨대, 보안 공간은 ARM(Advance RISC Machine)사의 트러스트 존(TrustZone) 기술을 실행하는 공간일 수 있다.
- [62] 다양한 실시예들에 따른 일반 환경(410)에서 제1 익셉션 레벨(EL0(401))은 클라이언트 어플리케이션(client application, CA)(441), TEE 라이브러리(TEE library)(451)를 포함할 수 있다. 클라이언트 어플리케이션(441)은 내재화 어플리케이션(embedded application)과 서드파티 어플리케이션(3rd party application)을 포함할 수 있다. 예컨대, 내재화 어플리케이션은 웹 브라우저(web browser), 이메일(email) 프로그램, 인스턴트 메신저(instant messenger)를 포함할

수 있다. 클라이언트 어플리케이션(441)의 실행에 필요한 데이터 및 무선 통신 회로(예: 도 3의 무선 통신 회로(310))를 통해 외부 전자 장치(예: 도 1의 전자 장치(102, 104), 서버(108))로부터 수신한 데이터를 저장할 수 있다.

[63] 다양한 실시예들에 따른 일반 환경(410)에서 제2 익셉션 레벨(EL1(403))은 TEE 드라이버(TEE driver)(453)를 포함할 수 있다. TEE 드라이버(453)는 커널 공간에 저장된 데이터를 보안 환경(420)의 매니저(manager)(461)에 전달할 수 있다.

[64] 다양한 실시예들에 따른 보안 환경(420)에서 제1 익셉션 레벨(EL0(401))은 보안 어플리케이션(trusted application, TA)(465)을 포함할 수 있다. 보안 어플리케이션(465)은 보안 환경(420) 동작에 필요한 어플리케이션을 포함하거나, 커널 데이터의 무결성 검사(integrity verification), 증명(attestation)과 같이 보안이 필요한 프로세스에 있어서 보안 인증 및 인가를 위해 호출되는 보안 어플리케이션을 포함할 수 있다.

[65] 다양한 실시예들에 따른 보안 환경(420)에서 제2 익셉션 레벨(EL1(403))은 TEE OS(463)를 포함할 수 있다. TEE OS(463)는 보안 기술이 적용된 운영체제를 포함할 수 있다.

[66] 다양한 실시예들에 따른 보안 환경(420)에서 제4 익셉션 레벨(EL3(405))은 매니저(461)를 포함할 수 있다. 매니저(461)는 일반 환경(410)에서 전송 받은 일반 환경(410)의 데이터를 보안 환경(420)의 주소 공간(예: 매니저(461)에 의해 관리되는, 제4 익셉션 레벨(예: EL3(405))에 포함된 테이블)에 로드할 수 있다.

[67] 일 실시예에서, 메모리(430)에 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 일반 환경(410)의 클라이언트 어플리케이션(441)은 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)을 할당할 수 있다.

[68] 일 실시예에서, 메모리(430)의 제1 주소 공간(431)은 일반 환경(예: 도 4의 REE(rich execution environment)(410)) 및 보안 환경(예: 도 4의 TEE(trusted execution environment)(420)) 간 공유되는 주소 공간을 포함할 수 있다. 예컨대, 제1 주소 공간(431)은 일반 환경(410) 및 보안 환경(420) 간 데이터를 전송하는데 사용될 수 있다. 메모리(430)의 제2 주소 공간(433)은 일반 환경(410)의 커널(예: 일반 환경(410)의 제2 익셉션 레벨(EL1(403)))의 개입을 최소화하면서 보안 환경(420)의 보안 공간(예: 제4 익셉션 레벨(EL3(405))의 보안 공간)으로 전환하기 위해 할당된 주소 공간을 포함할 수 있다.

[69] 일 실시예에서, 일반 환경(410)의 제2 익셉션 레벨(EL1(403))인 커널은 사용자 공간(예: 일반 환경(410)의 제1 익셉션 레벨(EL0(401))) 및 커널 공간의 페이지 테이블(예: 제1 페이지 테이블(447), 제2 페이지 테이블(455))을 관리할 수 있다.

[70] 일 실시예에서, 전자 장치(301)(예: 커널 공간(예: 일반 환경(410)의 제2 익셉션 레벨(EL1(403)))는 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)을 일반 환경(410)에서 사용자 공간(예: 제1 익셉션 레벨(EL0(401)))의 제1 페이지 테이블(447)의 제1 사용자 가상 메모리 주소 공간(448) 및 제2 사용자 가상 메모리 주소 공간(449)에 매핑(471, 475) 할 수 있다. 제1 페이지 테이블(447)의

제1 사용자 가상 메모리 주소 공간(448)의 접근 권한 및 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한은 읽기 및 쓰기 접근이 활성화되게(read-writable) 설정(예: RW(read and write)로 설정)될 수 있다.

- [71] 일 실시예에서, 전자 장치(301)(예: 커널 공간(예: 일반 환경(410)의 제2 익셉션 레벨(EL1(403)))는 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)을 일반 환경(410)에서 커널 공간의 제2 페이지 테이블(455)의 제1 커널 가상 메모리 주소 공간(456) 및 제2 커널 가상 메모리 주소 공간(457)에 매핑(473, 477) 할 수 있다. 제2 페이지 테이블(455)의 제1 커널 가상 메모리 주소 공간(456)의 접근 권한 및 제2 커널 가상 메모리 주소 공간(457)의 접근 권한은 읽기 및 쓰기 접근이 활성화되게 설정(예: RW(read and write)로 설정)될 수 있다.
- [72] 일 실시예에서, 클라이언트 어플리케이션(441)은 API(예: 도 2의 TEE functional API(application programming interface)(221) 또는 TEE client API(223))를 호출(479)하여 TEE 라이브러리(451)에 데이터를 전달할 수 있다. TEE 라이브러리(451)는 추가된 API를 이용하여 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 TEE 드라이버(453)에 전달(481)할 수 있다. 커널 공간(예: 일반 환경(410)의 제2 익셉션 레벨(EL1(403)))의 TEE 드라이버(453)는 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소와 커널 공간에서 관리하고 있는 호출자 정보(예: 프로세스의 메모리 공간 정보)를 보안 환경(420)의 매니저(461)(예: 제4 익셉션 레벨(EL3(405)))에 전달(483)할 수 있다.
- [73] 일 실시예에서, 매니저(461)는 암호학적 해시(hash)를 이용하여 커널 공간에서 관리하고 있는 호출자 정보(예: 프로세스의 메모리 공간 정보)에 기반하여, 클라이언트 어플리케이션(441)의 정적 영역에 대해 페이지 단위 별로 제1 해시 값을 생성할 수 있다. 매니저(461)는 제1 해시 값과 기 저장된 클라이언트 어플리케이션(441)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값(예: 컴파일 시 생성된 제2 해시 값)을 비교할 수 있다. 매니저(461)는 비교를 통해 제1 해시 값과 제2 해시 값이 동일한지 여부에 기반하여 클라이언트 어플리케이션(441)의 정적 영역 중 로드된 페이지에 대해 인증을 수행하는, 제1 호출자 인증을 수행할 수 있다. 예컨대, 제1 호출자 인증을 수행하는 동작은 데이터 쓰기(write)를 요청한 클라이언트 어플리케이션(441)이 적합한지 여부를 판단하기 위한 동작일 수 있다.
- [74] 일 실시예에서, 생성된 클라이언트 어플리케이션(441)의 정적 영역에 대한1 해시 값 및 기 저장된 클라이언트 어플리케이션(441)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값이 동일한 것으로 결정되면, 매니저(461)는 제1 호출자 인증을 성공한 것으로 결정하고, 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 보안 환경(420)의 테이블(예: 매니저(461)에 의해 관리되는, 제4 익셉션 레벨(예: EL3(405)에 포함된 테이블)에 저장할 수 있다. 예컨대, 전자 장치(301)는 메모리(430)에 저장된 정보를 탐색하기 위한 주소 공간을 포함하는

레지스터(register)인 TTBR(translation table base register)을 제공할 수 있다. 제1 호출자 인증이 성공한 경우, 매니저(461)는 “TTBR0_EL1”을 식별자로 하여 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 보안 환경(420)(예: 제4 익셉션 레벨(예: EL3(405)))의 테이블에 저장할 수 있다.

- [75] 일 실시예에서, 제1 호출자 인증을 성공한 경우, 매니저(461)는 메모리(430)의 제2 주소 공간(433)에 매핑된 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한을 접근이 비활성화되게 설정(예: 읽기 접근 및 쓰기 접근을 비활성화되게 설정)할 수 있다. 예컨대, 제1 페이지 테이블(447)의 제2 사용자 가상 메모리 주소 공간(449)에 대한 접근 권한인 읽기 및 쓰기 접근이 활성화된 상태(예: RW(read and write)로 설정된 상태)에서 읽기 및 쓰기 접근이 비활성화된 상태(예: NA(no access))로 변경할 수 있다.
- [76] 일 실시예에서, 제1 호출자 인증을 성공한 경우, 전자 장치(301)는 제1 호출자 인증을 수행했음을 나타내는 값을 설정할 수 있다. 예컨대, 메모리(430)의 페이지 디스크립터(page descriptor)의 특정 비트를 이용하여, 제1 호출자 인증 수행 여부에 대한 값을 설정할 수 있다. 페이지 디스크립터의 특정 비트를 이용하여 제1 호출자 인증 수행 여부에 대한 값을 설정함에 따라, 제1 호출자 인증을 수행한 메모리의 주소 공간에 대해서는 후술하는 제2 호출자 인증을 수행하지 않을 수 있다.
- [77] 다양한 실시예들에 따라, 제1 호출자 인증을, 생성된 클라이언트 어플리케이션(441)의 정적 영역에 대한 제1 해시 값 및 기 저장된 클라이언트 어플리케이션(441)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값이 동일한지 여부에 기반하여 수행하는 것으로 설명하였으나, 이에 한정하는 것은 아니다. 예컨대, 매니저(461)는 제어 흐름 무결성(control flow integrity, CFI)을 이용하여 제1 호출자 인증을 수행할 수 있다. 다른 예를 들어, 매니저(461)는 생성된 클라이언트 어플리케이션(441)의 정적 영역에 대한 제1 해시 값 및 기 저장된 클라이언트 어플리케이션(441)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값이 동일한지 여부를 확인한 후, 추가적으로 제어 흐름 무결성(control flow integrity, CFI)을 검증하는, 제1 호출자 인증을 수행할 수 있다.
- [78] 다양한 실시예들에서, 제1 호출자 인증 수행으로, 일부 페이지(예: 로드된 페이지)에 대해 해시 계산을 수행할 수 있다. 제1 호출자 인증 수행으로 일부 페이지(예: 로드된 페이지)에 대해 해시 계산을 수행하고, 후술하는 제2 호출자 인증에서는 추가된 페이지(예: 제1 호출자 인증이 수행되지 않은 로드된 페이지)에 대해서만 검증을 수행하기 때문에, 시스템 오버헤드(overhead)가 낮아질 수 있다.
- [79] 일 실시예에서, 제1 페이지 테이블(447)의 제2 사용자 가상 메모리 주소 공간(449)에 접근이 비활성화 상태(예: 읽기 및 쓰기 접근이 비활성화 상태(no access, NA))로 변경된 상태에서, 클라이언트 어플리케이션(441)은 메모리(430)의 제1 주소 공간(431)에 데이터를 쓴(write) 후, 제2 주소 공간(433)을

읽을 수 있다.

- [80] 일 실시예에서, 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한에 대해 읽기 및 쓰기 접근이 비활성화 상태로 설정됨에 따라 이에 매핑된 제2 주소 공간(433)의 접근 권한 또한 읽기 및 쓰기 접근이 비활성화 상태이나, 제2 주소 공간(433)을 읽음에 따라 클라이언트 어플리케이션(441)은 읽기 권한 오류(reading permission fault)를 발생(489)시킬 수 있다. 읽기 권한 오류가 발생됨에 따라 전자 장치(301)는 익셉션 핸들러(exception handler)(미도시)를 실행할 수 있으며, 읽기 권한 오류에 대한 SMC(secure monitor call)를 통해 보안 환경(420)의 제4 익셉션 레벨(EL3(405))에 포함된 매니저(461)를 실행할 수 있다.
- [81] 일 실시예에서, 매니저(461)는 제2 주소 공간(433)에서 읽기 권한 오류가 발생한 것인지 여부를 확인할 수 있다. 예컨대, 매니저(461)는 시스템 레지스터들(예: TTBR0_EL1, FAR(fault address register)_EL1, ELR(exception link register)_EL1)을 확인할 수 있다. 예컨대, TTBR은 가상 메모리 주소를 물리적 주소로 변환할 시 참조하는 변환 테이블 주소를 의미할 수 있다. FAR(fault address register)_EL1은 제2 주소 공간(433)에서 읽기 권한 오류가 발생한 시점의 메모리(430)의 제2 주소 공간(433)의 주소를 포함할 수 있다. ELR(exception link register)은 익셉션(exception)을 종료한 후 리턴(return)할 주소를 포함할 수 있다. 예컨대, ELR_EL1은 읽기 권한 오류를 발생시킨 명령어 위치(예: 주소 공간)를 확인할 수 있는 레지스터를 의미할 수 있다.
- [82] 일 실시예에서, 매니저(461)는 확인한 시스템 레지스터들(예: TTBR0_EL1, FAR_EL1, ELR_EL1)에 기반하여 읽기 권한 오류가 메모리(430)의 제2 주소 공간(433)에 의해 발생한 것인지 여부를 확인할 수 있다. 예컨대, 매니저(461)는 시스템 레지스터들(예: TTBR0_EL1, FAR_EL1, ELR_EL1)을 읽어, 읽기 권한 오류를 발생시킨 클라이언트 어플리케이션(441), 읽기 권한 오류가 발생한 주소 공간을 확인할 수 있다. 읽기 권한 오류가 메모리(430)의 제2 주소 공간(433)에서 발생한 것으로 결정되는 것에 기반하여, 매니저(461)는 제2 호출자 인증을 수행(485)할 수 있다.
- [83] 일 실시예에서, 매니저(461)는 메모리(430)의 페이지 디스크립터의 특정 비트에 설정된 제1 호출자 인증 수행 여부에 대한 값을 확인할 수 있다. 매니저(461)는 페이지 디스크립터의 특정 비트에 설정된 제1 호출자 인증 수행 여부에 대한 값을 확인하고, 제1 호출자 인증이 수행되지 않은 정적 영역(예: 클라이언트 어플리케이션(441)의 정적 영역)의 로드된 페이지에 대해 제2 호출자 인증을 수행할 수 있다. 예컨대, 매니저(461)는 제1 호출자 인증이 수행되지 않은 정적 영역(예: 클라이언트 어플리케이션(441)의 정적 영역)의 로드된 페이지에 대한 제3 해시 값을 생성(계산)할 수 있다. 매니저(461)는 제3 해시 값과 기 저장된 클라이언트 어플리케이션(441)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값과 비교하고, 비교 결과에 기반하여, 제3 해시 값과 제2 해시 값이 동일한지 여부를 확인하는 정적 영역에 대한 제2 호출자 인증을

수행할 수 있다.

- [84] 다양한 실시예들에 따라, 제2 호출자 인증을, 제1 호출자 인증이 수행되지 않은 정적 영역(예: 클라이언트 어플리케이션(441)의 정적 영역)의 로드된 페이지에 대한 생성된 제3 해시 값 및 기 저장된 클라이언트 어플리케이션(441)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값이 동일한지 여부에 기반하여 수행하는 것으로 설명하였으나, 이에 한정하는 것은 아니다. 예컨대, 매니저(461)는 제어 흐름 무결성(control flow integrity, CFI)을 이용하여 제2 호출자 인증을 수행할 수 있다. 다른 예를 들어, 매니저(461)는 생성된 제3 해시 값 및 제2 해시 값이 동일한지 여부를 확인한 후, 추가적으로 제어 흐름 무결성(control flow integrity, CFI)을 검증하는 제2 호출자 인증을 수행할 수 있다.
- [85] 일 실시예에서, 생성된 제3 해시 값과 기 저장된 제2 해시 값이 동일한 것으로 결정되면, 매니저(461)는 제2 호출자 인증을 성공한 것으로 결정하고, 제1 사용자 가상 메모리 주소 공간(448), 제2 사용자 가상 메모리 주소 공간(449), 및 제1 커널 가상 메모리 주소 공간(456)의 접근 권한을 읽기 접근이 활성화되고, 쓰기 접근이 비활성화되게 설정(491)할 수 있다.
- [86] 일 실시예에서, 클라이언트 어플리케이션(441)은 제2 주소 공간(433)의 접근 권한에 대해 읽기 및 쓰기 접근이 비활성화 상태로 설정되어 읽기 권한 오류가 발생됨에 따라 제2 주소 공간(433)으로의 읽기가 홀드 되었으나, 제2 주소 공간(433)에 대해 읽기 접근이 활성화되도록 설정됨에 따라 제2 주소 공간(433)에 저장된 값을 읽을 수 있다(487). 이에 따라, 보안 어플리케이션(465)이 호출될 수 있다.
- [87] 일 실시예에서, 매니저(461)는 보안 어플리케이션(465)을 호출 시, 보안 환경(420)(예: 제4 익셉션 레벨(EL3(405)))의 테이블, 제1 주소 공간(431)의 접근 권한을 확인할 수 있다. 보안 환경(420)의 테이블에 TTBR0_EL1이 등록되어 있고, 제1 주소 공간(431)의 접근 권한에 대해 읽기 접근이 활성화 및 쓰기 접근이 비활성화로 설정된 경우, 매니저(461)는 TEE OS(463)로 메모리(430)의 제1 주소 공간(431)의 가상 메모리 주소를 전달(493)하고, 보안 어플리케이션(465)을 호출(495)할 수 있다. 보안 어플리케이션(465)은 제1 주소 공간(431)의 가상 메모리 주소를 참조하여, 메모리(430)의 제1 주소 공간(431)의 데이터를 읽을 수 있다(497).
- [88] 일 실시예에서, 보안 환경(420)의 테이블에 TTBR0_EL1이 등록되어 있지 않거나, 및/또는 제1 주소 공간(431)의 접근 권한에 대해 쓰기 접근이 활성화로 설정된 경우, 매니저(461)는 보안 어플리케이션(465)의 호출을 차단할 수 있다. 전술한 동작에 의해 허용된 일반 어플리케이션(441)만이 보안 어플리케이션(465)을 호출할 수 있으며, 이에 따라, 메모리(430)의 보안을 강화할 수 있다.
- [89] 일 실시예에서, 클라이언트 어플리케이션(441)은 TEE 라이브러리(479)의 API를 통해 매니저(461)에 접근 권한을 복구하는 요청을 전달할 수 있다.

매니저(461)는 TTBR0_EL1이 보안 환경(420)의 테이블에 등록된 경우, 제1 주소 공간(431) 및 제2 주소 공간(433)의 접근 권한을 읽기 및 쓰기 접근이 활성화되도록 변경할 수 있다. 매니저(461)는 보안 환경(420)의 테이블에서 TTBR0_EL1로 등록된 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 삭제할 수 있다. 제1 주소 공간(431) 및 제2 주소 공간(433)의 접근 권한이 읽기 및 쓰기 접근이 활성화되도록 변경되면, 클라이언트 어플리케이션(441)은 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)의 할당을 해제할 수 있다.

[90] 도 5는, 다양한 실시예들에 따른, 페이지 디스크립터(page descriptor)(550)를 도시한 도면(500)이다.

[91] 도 5를 참조하면, 메모리(예: 도 4의 메모리(430))에 대한 페이지 디스크립터(550)를 도시한 것이다. 페이지 디스크립터(550)는 64 비트(bit) 크기일 수 있다. 하지만 이에 한정하는 것은 아니다.

[92] 일 실시예에서, 페이지 디스크립터(550)는 64 비트를 기반으로 다수 개의 영역으로 분할될 수 있다. 예컨대, 페이지 디스크립터(550)는 하위 속성(lower attributes) 영역(510)(예: 2번 비트부터 11번 비트까지), 주소(address) 영역(520)(예: 12번 비트부터 50비트까지, 메모리(430)에 접근하기 위한 주소 정보가 저장된 영역), 및 상위 속성(upper attribute) 영역(530)(예: 51번 비트부터 63번 비트까지)으로 분할될 수 있다.

[93] 다양한 실시예들에 따른 전술한 페이지 디스크립터(550)를 구성하는 하위 속성 영역(510)(예: 2번 비트부터 11번 비트까지), 주소 영역(520)(예: 12번 비트부터 50비트까지), 및 상위 속성 영역(530)(예: 51번 비트부터 63번 비트까지) 각각에 대한 사이즈는, 하나의 실시예로, 이에 한정하는 것은 아니다.

[94] 일 실시예에서, 전자 장치(301)(예: 도 3의 전자 장치(301))는 하위 속성(lower attributes) 영역(510)의 접근 권한(access permission, AP)을 설정할 수 있는 영역(511)에 비트 정보를 저장할 수 있다. 예컨대, 하위 속성(lower attributes) 영역(510)의 접근 권한(access permission) 영역(511)은 6번 비트 및 7번 비트로 표현될 수 있다. 예컨대, 비특권 레벨(unprivileged level)은 EL0(예: 도 4의 제1 익셉션 레벨(예: EL0(401)))을 포함할 수 있으며, 특권 레벨(privileged level)은 EL1(예: 도 4의 제2 익셉션 레벨(예: EL1(403))), EL2(예: 제3 익셉션 레벨(미도시)), 및 EL3(예: 도 4의 제4 익셉션 레벨(예: EL3(405)))을 포함할 수 있다. 7번 비트는 특권 레벨(privileged level)(예: EL1(403), EL2, EL3(405))의 접근 권한을 나타낼 수 있으며, 6번 비트는 비특권 레벨(unprivileged level)(예: EL0(401))의 접근 권한을 나타낼 수 있다. 전자 장치(301)는 접근 권한 영역(511)을 이용하여, 하기 <표 1>과 같이 메모리(430)의 접근 권한을 설정할 수 있다.

[95] [표1]

접근 권한	비특권 레벨(EL0)	특권 레벨(EL1/2/3)
00	읽기 및 쓰기 접근이 비활성화 (no access, NA)	읽기 및 쓰기 접근을 활성화 (read and write, RW)
01	읽기 및 쓰기 접근을 활성화 (read and write, RW)	읽기 및 쓰기 접근을 활성화 (read and write, RW)
10	읽기 및 쓰기 접근이 비활성화 (no access, NA)	읽기 접근만을 활성화 (read-only, RO)
11	읽기 접근만을 활성화 (read-only, RO)	읽기 접근만을 활성화 (read-only, RO)

[96] 다양한 실시예들에서, 하기 <표 2>는 메모리(예: 도 4의 메모리(430))의 제1 주소 공간(예: 도 4의 제1 주소 공간(431)) 및 제2 주소 공간(예: 도 4의 제2 주소 공간(433))에 매핑된 제1 페이지 테이블(예: 도 4의 제1 페이지 테이블(447)) 및 제2 페이지 테이블(예: 도 4의 제2 페이지 테이블(455))의 가상 주소 공간(예: 제1 사용자 가상 메모리 주소 공간(448), 제2 사용자 가상 메모리 주소 공간(449), 제1 커널 가상 메모리 주소 공간(456), 제2 커널 가상 메모리 주소 공간(457))에 대한 접근 권한을 나타낸 것이다. 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)은 제1 페이지 테이블(447)의 제1 사용자 가상 메모리 주소 공간(448) 및 제2 사용자 가상 메모리 주소 공간(449)과 제2 페이지 테이블(455)의 제1 커널 가상 메모리 주소 공간(456) 및 제2 커널 가상 메모리 주소 공간(457)에 더블 매핑(double mapping)되기 때문에, 사용자 가상 주소 공간 및 커널 가상 주소 공간에 대한 접근 권한을 변경할 수 있다.

[97] 예컨대, 전자 장치(301)는 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)을 제1 페이지 테이블(447)(예: EL0(401)의 제1 페이지 테이블(447))의 제1 사용자 가상 메모리 주소 공간(448) 및 제2 사용자 가상 메모리 주소 공간(449)에 매핑 시, 제1 사용자 가상 메모리 주소 공간(448)의 접근 권한 및 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한의 비트를 “01(RW)”로 설정할 수 있다. 전자 장치(301)는 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)을 제2 페이지 테이블(455)(예: EL1(403)의 제2 페이지 테이블(455))의 제1 커널 가상 메모리 주소 공간(456) 및 제2 커널 가상 메모리 주소 공간(457)에 매핑 시, 제1 커널 가상 메모리 주소 공간(456)의 접근 권한 및 제2 커널 가상 메모리 주소 공간(457)의 접근 권한의 비트를 “00(RW)”로 설정할 수 있다.

[98] 전술한 제1 페이지 테이블(447)(예: EL0(401)의 제1 페이지 테이블(447))의 제1 사용자 가상 메모리 주소 공간(448) 및 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한의 비트를 01(RW)”로 설정하고, 제2 페이지 테이블(455)(예:

EL1(403)의 제2 페이지 테이블(455)의 제1 커널 가상 메모리 주소 공간(456) 및 제2 커널 가상 메모리 주소 공간(457)의 접근 권한의 비트를 “00(RW)”로 설정하는 것은, 예컨대, 할당 단계로 정의할 수 있다.

- [99] 다른 예를 들어, 제1 호출자 인증을 수행한 후, 전자 장치(301)는 제1 사용자 가상 메모리 주소 공간(448)의 접근 권한의 비트를 “01(RW)” 및 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한의 비트를 “10(NA)”, 제1 커널 가상 메모리 주소 공간(456)의 접근 권한의 비트를 “00(RW)”으로 설정할 수 있다. 다시 말해, 제1 호출자 인증을 수행한 후, 전자 장치(301)는 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한만을 “01(RW)”에서 “10(NA)”으로 변경할 수 있다.
- [100] 전술한 전자 장치(301)는 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한의 비트를 “01(RW)”에서 “10(NA)”로 변경하는 것은, 예컨대, 초기화 단계로 정의할 수 있다.
- [101] 또 다른 예를 들어, 전자 장치(301)는 제2 주소 공간(433)에서 읽기 권한 오류가 발생하는 것에 기반하여, 제2 호출자 인증을 수행함에 따라, 제1 사용자 가상 메모리 주소 공간(448)의 접근 권한의 비트를 “11(RO)” 및 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한의 비트를 “11(RO)”, 제1 커널 가상 메모리 주소 공간(456)의 접근 권한의 비트를 “11(RO)”로 설정할 수 있다. “11”로 설정함에 따라 모든 익셉션 레벨(exception level)(예: 제1 익셉션 레벨(EL0), 제2 익셉션 레벨(EL1), 제3 익셉션 레벨(EL2), 및 제4 익셉션 레벨(EL3))은 읽기 접근만이 활성화될 수 있다. 모든 익셉션 레벨(exception level)(예: 제1 익셉션 레벨(EL0), 제2 익셉션 레벨(EL1), 및 제4 익셉션 레벨(EL3))에 대한 접근 권한이 읽기 접근만이 활성화됨에 따라, 공격자가 커널 권한을 가지고 있더라도 데이터를 수정하거나, 삭제할 수 없다.
- [102] 전술한 제1 사용자 가상 메모리 주소 공간(448), 제2 사용자 가상 메모리 주소 공간(449), 제1 커널 가상 메모리 주소 공간(456)의 접근 권한의 비트를 “11(RO)”로 설정하는 것은, 동작 단계로 정의할 수 있다.

[103] [표2]

메모리		할당 단계	초기화 단계	동작 단계
제1 주소 공간	제1 사용자 가상 주소 공간	01(RW)	01(RW)	11(RO)
	제1 커널 가상 주소 공간	00(RW)	00(RW)	11(RO)
제2 주소 공간	제2 사용자 가상 주소 공간	01(RW)	10(NA)	11(RO)
	제2 커널 가상 주소 공간	00(RW), 01(RW), 10(RO), 또는, 11(RO)	00(RW), 01(RW), 10(RO), 또는, 11(RO)	00(RW), 01(RW), 10(RO), 또는, 11(RO)

[104] 다양한 실시예들에서, 전술한 <표 1> 및 <표 2>에 따른 6번 비트 및 7번 비트를 이용하여 접근 권한을 설정하는 구성 및 가상 주소 공간에 따른 할당 단계, 초기화 단계, 및 동작 단계에서의 접근 권한의 비트 값은 하나의 실시예로, <표 1> 및 <표 2>에 한정하는 것은 아니다. 예컨대, 접근 권한을 설정할 수 있는 비트 및 가상 주소 공간에 따른 할당 단계, 초기화 단계, 및 동작 단계에서의 접근 권한의 비트 값은 ARM 아키텍처(ARM architecture)의 타입에 따라 달라질 수 있다.

[105] 일 실시예에서, 전자 장치(301)는 상위 속성(upper attribute) 영역(530)의 일부 영역에 비트 정보를 저장할 수 있다. 예컨대, 상위 속성(upper attribute) 영역(530)에서 57번 비트로 표현되는 영역(531)을 이용하여, 제1 호출자 인증의 수행 여부를 나타내는 값을 설정할 수 있다. 제2 호출자 인증을 수행하는 경우, 상위 속성(upper attribute) 영역(530)의 57번 비트에 설정된 제1 호출자 인증의 수행 여부를 나타내는 값에 기반하여, 제1 호출자 인증을 수행한 메모리의 주소 공간에 대해서는 제2 호출자 인증을 수행하지 않을 수 있다. 예컨대, 상위 속성(upper attribute) 영역(530)의 57번 비트는 페이지 디스크립터(550)에서 사용하지 않는 비트(예: 미사용 비트)일 수 있다.

[106] 다양한 실시예들에서, 사용하지 않는 비트를 상위 속성(upper attribute) 영역(530)의 57번 비트로 정의한 것은, 하나의 실시예로, 이에 한정하는 것은 아니다. 예컨대, 페이지 디스크립터(550)에서 사용하지 않는 비트는 ARM 아키텍처(ARM architecture)의 타입에 따라 달라질 수 있다.

[107] 도 6은, 다양한 실시예들에 따른, 메모리 보호 방법을 설명하기 위한 흐름도(600)이다.

[108] 도 6을 참조하면, 전자 장치(예: 도 3의 전자 장치(301))(예: 도 4의 클라이언트 어플리케이션(441))는 605동작에서, 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 메모리(예: 도 4의 메모리(430))에 제1 주소 공간(예: 도 4의 제1 주소

- 공간(431)) 및 제2 주소 공간(예: 도 4의 제2 주소 공간(433))을 할당할 수 있다.
- [109] 일 실시예에서, 메모리(430)의 제1 주소 공간(431)은 일반 환경(예: 도 4의 REE(rich execution environment)(410)) 및 보안 환경(예: 도 4의 TEE(trusted execution environment)(420)) 간 공유되는 주소 공간으로, 일반 환경(410) 및 보안 환경(420) 간 데이터를 전송하는데 사용될 수 있다. 메모리(430)의 제2 주소 공간(433)의 일반 환경(410)의 개입을 최소화하면서 보안 환경(420)의 보안 공간(예: 제4 익셉션 레벨(EL3(405))의 보안 공간)으로 전환하기 위해 할당된 주소 공간을 포함할 수 있다.
- [110] 일 실시예에서, 전자 장치(301)(예: 커널 공간(예: 일반 환경(410)의 제2 익셉션 레벨(EL1(403)))는 610동작에서, 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)을 일반 환경(410)의 제1 페이지 테이블(예: 도 4의 제1 페이지 테이블(447))의 제1 사용자 가상 메모리 주소 공간(448) 및 제2 사용자 가상 메모리 주소 공간(449)에 매핑 할 수 있다. 일 실시예에서, 전자 장치(301)는 제1 페이지 테이블(447)의 제1 사용자 가상 메모리 주소 공간(448)의 접근 권한 및 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한을 읽기 및 쓰기 접근이 활성화되게 설정(예: RW(read and write)로 설정)할 수 있다.
- [111] 일 실시예에서, 전자 장치(301)(예: 커널 공간(예: 일반 환경(410)의 제2 익셉션 레벨(EL1(403)))는 615동작에서, 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)을 일반 환경(410)의 제2 페이지 테이블(예: 도 4의 제2 페이지 테이블(455))의 제1 커널 가상 메모리 주소 공간(456) 및 제2 커널 가상 메모리 주소 공간(457)에 매핑 할 수 있다. 일 실시예에서, 전자 장치(301)는 제2 페이지 테이블(455)의 제1 커널 가상 메모리 주소 공간(456)의 접근 권한 및 제2 커널 가상 메모리 주소 공간(457)의 접근 권한을 읽기 및 쓰기 접근이 활성화되게 설정(예: RW(read and write)로 설정)할 수 있다.
- [112] 다양한 실시예들에 따른, 610동작 및 615동작은 실질적으로 동시에 수행될 수 있다.
- [113] 일 실시예에서, 전자 장치(301)(예: 클라이언트 어플리케이션(441))는 TEE 라이브러리(예: 도 4의 TEE 라이브러리(451))에 추가된 API를 이용하여 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 TEE 드라이버(예: 도 4의 TEE 드라이버(453))에 전달할 수 있다. TEE 드라이버(453)는 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소와 커널(예: 도 4의 EL1(403))에서 관리하고 있는 호출자 정보(예: 프로세스의 메모리 공간 정보)를 보안 환경(420)의 매니저(예: 도 4의 매니저(461))에 전달할 수 있다.
- [114] 일 실시예에서, 전자 장치(301)(예: 매니저(461))는 620동작에서, 제1 호출자 인증을 수행할 수 있다. 예컨대, 전자 장치(301)(예: 매니저(461))는 암호학적 해시(hash)를 이용하여 호출자 프로세스 예컨대, 클라이언트 어플리케이션(441)의 정적 영역(예: 도 4의 정적 영역(445))에 대해 페이지 단위

별로 제1 해시 값을 생성할 수 있다. 전자 장치(301)(예: 매니저(461))는 컴파일 시 생성된 제2 해시 값을 기 저장하고 있을 수 있으며, 제1 해시 값과 기 저장된 제2 해시 값을 비교하고, 비교 결과에 기반하여, 제1 해시 값과 제2 해시 값이 동일한지 여부를 확인하는 클라이언트 어플리케이션(441)의 정적 영역 중 로드(load)된 페이지에 대한 제1 호출자 인증을 수행할 수 있다. 컴파일 시 생성된 제2 해시 값은 보안 환경(420)의 매니저(461)에 정적으로 전달(예: 컴파일 시 전달)되거나, 또는 동적으로 전달(예: 부팅 시 전달)될 수 있다.

- [115] 일 실시예에서, 제1 해시 값과 제2 해시 값이 동일한 것으로 결정되면, 전자 장치(301)(예: 매니저(461))는 제1 호출자 인증을 성공한 것으로 결정하고, 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 보안 환경(420)의 테이블에 저장할 수 있다. 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 보안 환경(420)의 테이블에 저장한 후, 매니저(461)는 후술하는 625동작을 수행할 수 있다.
- [116] 일 실시예에서, 전자 장치(301)(예: 매니저(461))는 625동작에서, 메모리(430)의 제2 주소 공간(433)에 매핑된 제2 사용자 가상 메모리 주소 공간(449)에 대한 읽기 및 쓰기 접근이 비활성화되게 설정할 수 있다. 예컨대, 전자 장치(301)(예: 매니저(461))는 610동작에서 설정된 제1 페이지 테이블(447)의 제2 사용자 가상 메모리 주소 공간(449)에 대한 접근 권한인 읽기 및 쓰기 접근이 활성화된 상태(예: RW(read and write)로 설정된 상태)에서 읽기 및 쓰기 접근이 비활성화된 상태(예: NA(no access))로 변경할 수 있다.
- [117] 일 실시예에서, 전자 장치(301)는 TLB(translation lookaside buffer)를 포함할 수 있다. TLB는 최근 변환된 페이지 테이블의 주소 정보를 가질 수 있다. 제1 페이지 테이블(447)의 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한에 대해 읽기 및 쓰기 접근이 비활성화(예: NA(no access))로 변경한 후, 전자 장치(301)는 TLB를 무효화(invalidate)할 수 있다.
- [118] 일 실시예에서, 전자 장치(301)(예: 클라이언트 어플리케이션(441))는 630동작에서, 메모리(430)의 제1 주소 공간(431)에 데이터를 쓴(write) 후, 제2 주소 공간(433)으로의 읽기(read)를 검출할 수 있다. 예컨대, 전자 장치(301)는 보안 어플리케이션(예: 도 4의 보안 어플리케이션(465))을 호출하기 전에 제2 주소 공간(433)으로의 읽기를 검출할 수 있다.
- [119] 일 실시예에서, 전자 장치(301)(예: 매니저(461))는 635동작에서, 제2 주소 공간(433)에서 에러가 발생하는 것에 기반하여, 제2 호출자 인증을 수행할 수 있다. 예컨대, 전자 장치(301)는 제2 주소 공간(433)의 접근 권한에 대해 읽기 및 쓰기 접근을 비활성화 상태로 설정(예: 625동작)하였으나, 읽기 접근이 검출됨에 따라 읽기 권한 오류(reading permission fault)를 발생시킬 수 있다. 읽기 권한 오류가 발생됨에 따라 전자 장치(301)는 익셉션 핸들러(exception handler)(미도시)를 실행할 수 있으며, 읽기 권한 오류에 대한 SMC(secure monitor call)를 통해 보안 환경(420)의 제4 익셉션 레벨(EL3(405))에 포함된

매니저(461)를 실행할 수 있다.

- [120] 실행된 매니저(461)는 시스템 레지스터들(예: TTBR0_EL1, FAR_EL1, ELR_EL1)을 읽어, 읽기 권한 오류를 발생시킨 클라이언트 어플리케이션(441), 읽기 권한 오류가 발생한 주소 공간을 확인할 수 있다. 읽기 권한 오류가 메모리(430)의 제2 주소 공간(433)에서 발생한 것으로 결정되는 것에 기반하여, 전자 장치(301)(예: 매니저(461))는 제2 호출자 인증을 수행할 수 있다. 예컨대, 전자 장치(301)(예: 매니저(461))는 메모리(430)의 페이지 디스크립터(page descriptor)의 특정 비트에 설정된 제1 호출자 인증 수행 여부에 대한 값을 확인하고, 제1 호출자 인증이 수행되지 않은 정적 영역(예: 클라이언트 어플리케이션(240)의 정적 영역)의 로드된 페이지에 대해 검증을 수행하는 제2 호출자 인증을 수행할 수 있다. 전자 장치(301)(예: 매니저(461))는 메모리(430)의 페이지 디스크립터의 특정 비트에 설정된 제1 호출자 인증 수행 여부에 대한 값을 확인하고, 제1 호출자 인증이 수행되지 않은 메모리(430)의 주소 공간에 대해 제2 호출자 인증을 수행할 수 있다. 예컨대, 전자 장치(301)(예: 매니저(461))는 제1 호출자 인증 수행이 수행되지 않은 메모리(430)의 주소 공간의 가상 메모리 주소에 대한 정적 영역에 대한 제3 해시 값을 생성(계산)할 수 있다. 전자 장치(301)(예: 매니저(461))는 제3 해시 값과 기 저장된 클라이언트 어플리케이션(441)의 정적 영역의 가상 메모리 주소에 대한 제2 해시 값과 비교하고, 비교 결과에 기반하여, 제3 해시 값과 제2 해시 값이 동일한지 여부를 확인하는, 정적 영역에 대한 제2 호출자 인증을 수행할 수 있다. 예컨대, 생성된 제3 해시 값과 기 저장된 제2 해시 값이 동일한 경우, 전자 장치(301)(예: 매니저(461))는 제2 호출자 인증을 성공한 것으로 결정할 수 있다.

- [121] 일 실시예에서, 제2 호출자 인증을 성공한 경우, 전자 장치(301)(예: 매니저(461))는 640동작에서, 제1 사용자 가상 메모리 주소 공간(448) 및 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한에 대한 읽기 접근이 활성화되고, 쓰기 접근이 비활성화되게 설정(예: RO(read-only))할 수 있다. 예컨대, 전자 장치(301)는 보안 환경(420)의 매니저(461)를 이용하여, 메모리(430)의 제1 주소 공간(431)에 매핑된 일반 환경(410)의 제1 페이지 테이블(447)의 제1 사용자 가상 메모리 주소 공간(448)의 읽기 및 쓰기가 활성화(예: RW)된 접근 권한에서 쓰기 접근이 비활성화(예: RO)되게 변경할 수 있다. 전자 장치(301)는 보안 환경(420)의 매니저(461)를 이용하여, 메모리(430)의 제2 주소 공간(433)에 매핑된 일반 환경(410)의 제1 페이지 테이블(447)의 제2 사용자 가상 메모리 주소 공간(449)의 접근 권한에 대해 읽기 및 쓰기 접근이 비활성화 상태(예: NA)에서 쓰기 접근이 비활성화되게, 읽기 접근이 활성화(RO)되게 변경할 수 있다.

- [122] 일 실시예에서, 전자 장치(301)(예: 매니저(461))는 645동작에서, 제1 커널 가상 메모리 주소 공간(456)의 접근 권한에 대한 읽기 접근이 활성화되고, 쓰기 접근이 비활성화되게 설정할 수 있다. 예컨대, 전자 장치(301)는 보안 환경(420)의 매니저(461)를 이용하여, 메모리(430)의 제1 주소 공간(431)에 매핑된 일반

환경(410)의 제2 페이지 테이블(455)의 제1 커널 가상 메모리 주소 공간(456)의 읽기 및 쓰기가 활성화(예: RW)된 접근 권한에서 쓰기 접근이 비활성화(RO)되게 변경할 수 있다. 메모리(430)의 제2 주소 공간(433)에 매핑된 일반 환경(410)의 제2 페이지 테이블(455)의 제2 커널 가상 메모리 주소 공간(457)의 접근 권한은 쓰기 및 읽기가 활성화된 상태(예: RW)가 유지될 수 있다.

[123] 다양한 실시예들에 따른 640동작 및 645동작은 실질적으로 동시에 수행될 수 있다. 640동작 및 645동작을 수행한 후, 전자 장치(301)는 일반 환경(410)의 제1 익셉션 레벨(EL0(401))로 리턴하여, 제2 주소 공간(433)에 접근하여 제2 주소 공간(433)에 저장된 값을 리드할 수 있다.

[124] 일 실시예에서, 전자 장치(301)는 650동작에서, 보안 환경(420)의 테이블과 메모리(430)의 제1 주소 공간(431)의 접근 권한을 확인하고, 보안 환경(420)의 테이블에 데이터, 제1 주소 공간 및 제2 주소 공간의 가상 메모리 주소가 저장(예: 데이터, 제1 주소 공간 및 제2 주소 공간의 가상 메모리 주소가 TTBR0_EL1을 식별자로 하여 보안 환경(420)의 테이블에 등록)되어 있고, 제1 주소 공간(431)의 접근 권한에 대한 읽기 접근이 활성화되고, 쓰기 접근이 비활성화로 설정된 경우, 보안 어플리케이션(465)을 호출(495)할 수 있다.

[125] 일 실시예에서, 전자 장치(301)는 보안 환경(420)의 테이블에 데이터, 제1 주소 공간 및 제2 주소 공간의 가상 메모리 주소가 저장되어 있지 않거나(예: 데이터, 제1 주소 공간 및 제2 주소 공간의 가상 메모리 주소가 TTBR0_EL1을 식별자로 하여 보안 환경(420)의 테이블에 등록되어 있지 않거나) 및/또는 제1 주소 공간(431)의 접근 권한에 대해 쓰기 접근이 활성화로 설정된 경우, 보안 어플리케이션의 호출(465)을 차단할 수 있다.

[126] 다양한 실시예들에 따라, 미도시 되었으나, 전자 장치(301)는 접근 권한을 복구하는 요청을 검출하면, 매니저(461)를 통해 제1 주소 공간(431) 및 제2 주소 공간(433)의 접근 권한을 읽기 및 쓰기 접근이 활성화되도록 변경하고, 보안 환경(420)의 테이블로부터 제1 주소 공간(431) 및 제2 주소 공간(433)의 가상 메모리 주소를 삭제할 수 있다. 제1 주소 공간(431) 및 제2 주소 공간(433)의 접근 권한이 읽기 및 쓰기 접근이 활성화되도록 변경되면, 전자 장치(301)는 메모리(430)의 제1 주소 공간(431) 및 제2 주소 공간(433)의 할당을 해제할 수 있다.

[127] 본 문서에 개시된 다양한 실시예들에 따른 전자 장치는 다양한 형태의 장치가 될 수 있다. 전자 장치는, 예를 들면, 휴대용 통신 장치(예: 스마트폰), 컴퓨터 장치, 휴대용 멀티미디어 장치, 휴대용 의료 기기, 카메라, 웨어러블 장치, 또는 가전 장치를 포함할 수 있다. 본 문서의 실시예에 따른 전자 장치는 전술한 기기들에 한정되지 않는다.

[128] 본 문서의 다양한 실시예들 및 이에 사용된 용어들은 본 문서에 기재된 기술적 특징들을 특정한 실시예들로 한정하려는 것이 아니며, 해당 실시예의 다양한 변경, 균등물, 또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과

관련하여, 유사한 또는 관련된 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 아이টে에 대응하는 명사의 단수 형은 관련된 문맥상 명백하게 다르게 지시하지 않는 한, 상기 아이টে 한 개 또는 복수 개를 포함할 수 있다. 본 문서에서, "A 또는 B", "A 및 B 중 적어도 하나", "A 또는 B 중 적어도 하나", "A, B 또는 C", "A, B 및 C 중 적어도 하나", 및 "A, B, 또는 C 중 적어도 하나"와 같은 문구들 각각은 그 문구들 중 해당하는 문구에 함께 나열된 항목들 중 어느 하나, 또는 그들의 모든 가능한 조합을 포함할 수 있다. "제1", "제2", 또는 "첫째" 또는 "둘째"와 같은 용어들은 단순히 해당 구성요소를 다른 해당 구성요소와 구분하기 위해 사용될 수 있으며, 해당 구성요소들을 다른 측면(예: 중요성 또는 순서)에서 한정하지 않는다. 어떤(예: 제1) 구성요소가 다른(예: 제2) 구성요소에, "기능적으로" 또는 "통신적으로"라는 용어와 함께 또는 이런 용어 없이, "커플드" 또는 "커넥티드"라고 언급된 경우, 그것은 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로(예: 유선으로), 무선으로, 또는 제3 구성요소를 통하여 연결될 수 있다는 것을 의미한다.

[129] 본 문서의 다양한 실시예들에서 사용된 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구현된 유닛을 포함할 수 있으며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로와 같은 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는, 상기 부품의 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 일 실시예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.

[130] 본 문서의 다양한 실시예들은 기기(machine)(예: 전자 장치(101)) 의해 읽을 수 있는 저장 매체(storage medium)(예: 내장 메모리(136) 또는 외장 메모리(138))에 저장된 하나 이상의 명령어들을 포함하는 소프트웨어(예: 프로그램(140))로서 구현될 수 있다. 예를 들면, 기기(예: 전자 장치(101))의 프로세서(예: 프로세서(120))는, 저장 매체로부터 저장된 하나 이상의 명령어들 중 적어도 하나의 명령어를 호출하고, 그것을 실행할 수 있다. 이것은 기기가 상기 호출된 적어도 하나의 명령어에 따라 적어도 하나의 기능을 수행하도록 운영되는 것을 가능하게 한다. 상기 하나 이상의 명령어들은 컴파일러에 의해 생성된 코드 또는 인터프리터에 의해 실행될 수 있는 코드를 포함할 수 있다. 기기로 읽을 수 있는 저장 매체는, 비일시적(non-transitory) 저장 매체의 형태로 제공될 수 있다. 여기서, '비일시적'은 저장 매체가 실재(tangible)하는 장치이고, 신호(signal)(예: 전자기파)를 포함하지 않는다는 것을 의미할 뿐이며, 이 용어는 데이터가 저장 매체에 반영구적으로 저장되는 경우와 임시적으로 저장되는 경우를 구분하지 않는다.

[131] 일 실시예에 따르면, 본 문서에 개시된 다양한 실시예들에 따른 방법은 컴퓨터 프로그램 제품(computer program product)에 포함되어 제공될 수 있다. 컴퓨터 프로그램 제품은 상품으로서 판매자 및 구매자 간에 거래될 수 있다. 컴퓨터 프로그램 제품은 기기로 읽을 수 있는 저장 매체(예: compact disc read only

memory(CD-ROM))의 형태로 배포되거나, 또는 어플리케이션 스토어(예: 플레이 스토어™)를 통해 또는 두 개의 사용자 장치들(예: 스마트폰들) 간에 직접, 온라인으로 배포(예: 다운로드 또는 업로드)될 수 있다. 온라인 배포의 경우에, 컴퓨터 프로그램 제품의 적어도 일부는 제조사의 서버, 어플리케이션 스토어의 서버, 또는 중계 서버의 메모리와 같은 기기로 읽을 수 있는 저장 매체에 적어도 일시 저장되거나, 임시적으로 생성될 수 있다.

- [132] 다양한 실시예들에 따르면, 상기 기술한 구성요소들의 각각의 구성요소(예: 모듈 또는 프로그램)는 단수 또는 복수의 개체를 포함할 수 있으며, 복수의 개체 중 일부는 다른 구성요소에 분리 배치될 수도 있다. 다양한 실시예들에 따르면, 전술한 해당 구성요소들 중 하나 이상의 구성요소들 또는 동작들이 생략되거나, 또는 하나 이상의 다른 구성요소들 또는 동작들이 추가될 수 있다. 대체적으로 또는 추가적으로, 복수의 구성요소들(예: 모듈 또는 프로그램)은 하나의 구성요소로 통합될 수 있다. 이런 경우, 통합된 구성요소는 상기 복수의 구성요소들 각각의 구성요소의 하나 이상의 기능들을 상기 통합 이전에 상기 복수의 구성요소들 중 해당 구성요소에 의해 수행되는 것과 동일 또는 유사하게 수행할 수 있다. 다양한 실시예들에 따르면, 모듈, 프로그램 또는 다른 구성요소에 의해 수행되는 동작들은 순차적으로, 병렬적으로, 반복적으로, 또는 휴리스틱하게 실행되거나, 상기 동작들 중 하나 이상이 다른 순서로 실행되거나, 생략되거나, 또는 하나 이상의 다른 동작들이 추가될 수 있다.

청구범위

- [청구항 1] 전자 장치에 있어서,
메모리; 및
상기 메모리와 작동적으로 연결된 프로세서를 포함하며,
상기 메모리는, 실행될 때, 상기 프로세서가,
상기 메모리에 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 일반
환경에서, 상기 메모리에 제1 주소 공간 및 제2 주소 공간을 할당하고,
상기 일반 환경에서, 상기 메모리의 상기 제1 주소 공간에 데이터를 쓴 후,
상기 제2 주소 공간으로의 접근을 검출하고,
상기 제2 주소 공간으로의 접근을 검출하는 것에 기반하여, 보안 환경의
매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반
환경의 제1 사용자 가상 메모리 주소 공간의 접근 권한에 대한 쓰기
접근이 비활성화되게 설정하고, 상기 제2 주소 공간에 매핑된 상기 일반
환경의 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대한 읽기
접근이 활성화되고, 쓰기 접근이 비활성화되게 설정하고, 및
상기 보안 환경의 상기 매니저에 의해, 상기 메모리의 상기 제1 주소
공간에 매핑된 상기 일반 환경의 제1 커널 가상 메모리 주소 공간의 접근
권한에 대한 쓰기 접근이 비활성화되게 설정하도록 하는
인스트럭션들(instructions)을 저장하는 전자 장치.
- [청구항 2] 제 1 항에 있어서,
상기 메모리는, 실행될 때, 상기 프로세서가,
상기 제1 주소 공간 및 상기 제2 주소 공간을 할당한 후, 상기 일반 환경의
커널에 의해, 상기 메모리의 상기 제1 주소 공간 및 상기 제2 주소 공간을
상기 일반 환경의 제1 페이지 테이블의 상기 제1 사용자 가상 메모리 주소
공간 및 상기 제2 사용자 가상 메모리 주소 공간에 매핑하고,
상기 일반 환경의 상기 커널에 의해, 상기 메모리의 상기 제1 주소 공간 및
상기 제2 주소 공간을 상기 일반 환경의 제2 페이지 테이블의 상기 제1
커널 가상 메모리 주소 공간 및 제2 커널 가상 메모리 주소 공간에
매핑하고, 및
상기 제1 사용자 가상 메모리 주소 공간의 접근 권한, 상기 제2 사용자
가상 메모리 주소 공간의 접근 권한, 및 상기 제1 커널 가상 메모리 주소
공간의 접근 권한, 및 상기 제2 커널 가상 메모리 주소 공간의 접근 권한에
대한 읽기 및 쓰기 접근이 활성화(read-writable)되게 설정하도록 하는
인스트럭션들을 저장하는 전자 장치.
- [청구항 3] 제 2 항에 있어서,
상기 메모리는, 실행될 때, 상기 프로세서가,
상기 제1 주소 공간 및 상기 제2 주소 공간을 상기 제1 커널 가상 메모리

주소 공간 및 상기 제2 커널 가상 메모리 주소 공간에 매핑한 후, 상기 일반 환경의 드라이버를 통해, 상기 데이터, 상기 제1 주소 공간 및 상기 제2 주소 공간의 가상 메모리 주소, 및 상기 커널에서 관리하고 있는 프로세스의 메모리 공간 정보를 상기 보안 환경의 상기 매니저로 전송하고,

상기 매니저에 의해, 상기 프로세스의 메모리 공간 정보에 기반하여, 상기 일반 환경의 클라이언트 어플리케이션의 정적 영역에 대한 제1 해시 값을 생성하고,

상기 매니저에 의해, 상기 제1 해시 값과 기 저장된 상기 정적 영역의 가상 메모리 주소에 대한 제2 해시 값을 비교하고, 및

상기 매니저에 의해, 상기 제1 해시 값과 상기 제2 해시 값이 동일한지 여부에 기반하여, 상기 정적 영역 중 로드된 페이지에 대해 검증을 수행하는, 제1 호출자 인증을 수행하도록 하는 인스트럭션들을 저장하는 전자 장치.

[청구항 4]

제 3 항에 있어서,

상기 메모리는, 실행될 때, 상기 프로세서가,

상기 제1 해시 값과 상기 제2 해시 값이 동일한 경우, 상기 매니저에 의해, 상기 제1 호출자 인증을 성공한 것으로 결정하고, 상기 데이터, 상기 제1 주소 공간 및 상기 제2 주소 공간의 가상 메모리 주소를 상기 보안 환경의 테이블에 저장하도록 하는 인스트럭션들을 저장하는 전자 장치.

[청구항 5]

제 4 항에 있어서,

상기 메모리는, 실행될 때, 상기 프로세서가,

상기 제1 호출자 인증을 수행한 후, 상기 매니저에 의해, 상기 메모리의 상기 제2 주소 공간에 매핑된 상기 일반 환경의 상기 제2 사용자 가상 메모리 주소 공간에 대한 상기 읽기 및 상기 쓰기 접근이 활성화된 상태를, 상기 읽기 및 상기 쓰기 접근이 비활성화 상태로 변경하도록 설정하고, 및

상기 제1 호출자 인증을 수행한 후, 상기 메모리의 페이지

디스크립터(page descriptor)의 특정 비트를 이용하여, 상기 제1 호출자 인증을 수행했음을 나타내는 값을 설정하도록 하는 인스트럭션들을 저장하는 전자 장치.

[청구항 6]

제 5 항에 있어서,

상기 메모리는, 실행될 때, 상기 프로세서가,

상기 일반 환경에서, 상기 메모리의 상기 제2 주소 공간에 매핑된 상기 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대해 읽기 및 쓰기 접근이 비활성화 상태에서 상기 클라이언트 어플리케이션에 의해, 상기 제2 주소 공간으로의 접근을 검출하는 것에 기반하여, 상기 제2 주소 공간에서 접근 권한 오류가 발생하고,

상기 접근 권한 오류가 발생하는 것에 기반하여 상기 매니저를 호출하고,
 상기 매니저에 의해, 상기 접근 권한 오류가 상기 메모리의 상기 제2 주소
 공간에서 발생한 것인지 여부를 확인하고,
 상기 매니저에 의해, 상기 접근 권한 오류가 상기 메모리의 상기 제2 주소
 공간에서 발생한 것으로 확인되는 것에 기반하여, 상기 페이지
 디스크립터의 특정 비트를 확인하고,
 상기 매니저에 의해, 상기 특정 비트에 기반하여, 상기 제1 호출자 인증이
 수행되지 않은 상기 정적 영역의 로드된 페이지에 대해 검증을 수행하는,
 제2 호출자 인증을 수행하고,
 상기 매니저에 의해, 상기 제1 호출자 인증이 수행되지 않은 상기 정적
 영역의 로드된 페이지에 대한 제3 해시 값을 생성하고,
 상기 매니저에 의해, 상기 기 저장된 상기 정적 영역의 가상 메모리
 주소에 대한 제2 해시 값과 상기 생성된 제3 해시 값을 비교하고, 및
 상기 매니저에 의해, 상기 제2 해시 값과 상기 제3 해시 값이 동일한지
 여부에 기반하여, 상기 제1 호출자 인증이 수행되지 않은 상기 정적
 영역의 로드된 페이지에 대한 검증을 수행하는 상기 제2 호출자 인증을
 수행하도록 하는 인스트럭션들을 저장하는 전자 장치.

[청구항 7]

제 6 항에 있어서,
 상기 메모리는, 실행될 때, 상기 프로세서가,
 상기 제2 해시 값과 상기 제3 해시 값이 동일한 경우, 상기 매니저에 의해,
 상기 제2 호출자 인증을 성공한 것으로 결정하고, 상기 일반 환경의 상기
 제2 사용자 가상 메모리 주소 공간의 접근 권한을 상기 읽기 및 쓰기
 접근이 비활성화 상태에서, 상기 읽기 접근이 활성화되고 상기 쓰기
 접근이 비활성되도록 변경하는 인스트럭션들을 저장하는 전자 장치.

[청구항 8]

제 7 항에 있어서,
 상기 메모리는, 실행될 때, 상기 프로세서가,
 상기 매니저에 의해, 상기 보안 환경의 테이블 및 상기 제1 주소 공간의
 접근 권한을 확인하고,
 상기 보안 환경의 테이블에 상기 데이터, 상기 제1 주소 공간 및 상기 제2
 주소 공간의 가상 메모리 주소가 저장되어 있고, 상기 제1 주소 공간의
 접근 권한에 대해 읽기 접근이 활성화, 쓰기 접근이 비활성화로 설정된
 경우, 상기 보안 환경의 보안 어플리케이션을 호출하고, 및
 상기 보안 환경의 테이블에 상기 데이터, 상기 제1 주소 공간 및 상기 제2
 주소 공간의 가상 메모리 주소가 저장되어 있지 않거나, 및/또는 상기 제1
 주소 공간의 접근 권한에 대해 상기 쓰기 접근이 활성화로 설정된 경우,
 상기 매니저에 의해 상기 보안 어플리케이션의 호출을 차단하도록 하는
 인스트럭션들을 저장하는 전자 장치.

[청구항 9]

제 1 항에 있어서,

상기 제1 주소 공간은, 상기 일반 환경 및 상기 보안 환경 간 데이터를 전송하는데 사용하기 위해 할당된 주소 공간을 포함하고, 및
상기 제2 주소 공간은, 상기 일반 환경의 사용자 공간에서 상기 보안 환경의 보안 공간으로 전환하기 위해 할당된 주소 공간을 포함하는 전자 장치.

- [청구항 10] 전자 장치의 메모리 보호 방법에 있어서,
메모리에 데이터 쓰기(write) 요청을 검출하는 것에 기반하여, 일반 환경에서, 상기 메모리에 제1 주소 공간 및 제2 주소 공간을 할당하는 동작;
상기 일반 환경에서, 상기 메모리의 상기 제1 주소 공간에 데이터를 쓴 후, 상기 제2 주소 공간으로의 접근을 검출하는 동작;
상기 제2 주소 공간으로의 접근을 검출하는 것에 기반하여, 보안 환경의 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 사용자 가상 메모리 주소 공간의 접근 권한에 대한 쓰기 접근이 비활성화되게 설정하고, 상기 제2 주소 공간에 매핑된 상기 일반 환경의 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대한 읽기 접근(read access)이 활성화되고, 쓰기 접근(write access)이 비활성화되게 설정하는 동작; 및
상기 보안 환경의 상기 매니저에 의해, 상기 메모리의 상기 제1 주소 공간에 매핑된 상기 일반 환경의 제1 커널 가상 메모리 주소 공간의 접근 권한에 대한 쓰기 접근이 비활성화되게 설정하는 동작을 포함하는 방법.
- [청구항 11] 제 10 항에 있어서,
상기 제1 주소 공간 및 상기 제2 주소 공간을 할당한 후, 상기 일반 환경의 커널에 의해, 상기 메모리의 상기 제1 주소 공간 및 상기 제2 주소 공간을 상기 일반 환경의 제1 페이지 테이블의 상기 제1 사용자 가상 메모리 주소 공간 및 상기 제2 사용자 가상 메모리 주소 공간에 매핑하는 동작;
상기 일반 환경의 상기 커널에 의해, 상기 메모리의 상기 제1 주소 공간 및 상기 제2 주소 공간을 상기 일반 환경의 제2 페이지 테이블의 상기 제1 커널 가상 메모리 주소 공간 및 제2 커널 가상 메모리 주소 공간에 매핑하는 동작; 및
상기 제1 사용자 가상 메모리 주소 공간의 접근 권한, 상기 제2 사용자 가상 메모리 주소 공간의 접근 권한, 및 상기 제1 커널 가상 메모리 주소 공간의 접근 권한, 및 상기 제2 커널 가상 메모리 주소 공간의 접근 권한에 대한 읽기 및 쓰기 접근이 활성화(read-writable)되게 설정하는 동작을 더 포함하는 방법.
- [청구항 12] 제 11 항에 있어서,
상기 일반 환경의 드라이버를 통해, 상기 데이터, 상기 제1 주소 공간 및 상기 제2 주소 공간의 가상 메모리 주소, 및 상기 커널에서 관리하고 있는

프로세스의 메모리 공간 정보를 상기 보안 환경의 상기 매니저로 전송하는 동작;
 상기 매니저에 의해, 상기 프로세스의 메모리 공간 정보에 기반하여, 상기 일반 환경의 클라이언트 어플리케이션의 정적 영역에 대한 제1 해시 값을 생성하는 동작;
 상기 매니저에 의해, 상기 제1 해시 값과 기 저장된 상기 정적 영역의 가상 메모리 주소에 대한 제2 해시 값을 비교하는 동작; 및
 상기 매니저에 의해, 상기 제1 해시 값과 상기 제2 해시 값이 동일한지 여부에 기반하여, 상기 정적 영역 중 로드된 페이지에 대해 검증을 수행하는, 제1 호출자 인증을 수행하는 동작을 더 포함하는 방법.

[청구항 13]

제 12 항에 있어서,
 상기 매니저에 의해, 상기 메모리의 상기 제2 주소 공간에 매핑된 상기 일반 환경의 상기 제2 사용자 가상 메모리 주소 공간에 대한 상기 읽기 및 상기 쓰기 접근이 활성화된 상태를 상기 읽기 및 상기 쓰기 접근이 비활성화 상태로 변경하도록 설정하는 동작;
 상기 일반 환경에서, 상기 메모리의 상기 제2 주소 공간에 매핑된 상기 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대해 읽기 및 쓰기 접근이 비활성화 상태에서 상기 제2 주소 공간으로의 접근을 검출하는 것에 기반하여, 상기 제2 주소 공간에서 접근 권한 오류가 발생하는 동작;
 상기 접근 권한 오류가 발생하는 것에 기반하여 상기 매니저를 호출하는 동작;
 상기 매니저에 의해, 상기 접근 권한 오류가 상기 메모리의 상기 제2 주소 공간에서 발생한 것인지 여부를 확인하는 동작;
 상기 매니저에 의해, 상기 접근 권한 오류가 상기 메모리의 상기 제2 주소 공간에서 발생한 것으로 확인되는 것에 기반하여, 상기 페이지 디스크립터의 특정 비트를 확인하는 동작; 및
 상기 매니저에 의해, 상기 특정 비트에 기반하여, 상기 제1 호출자 인증이 수행되지 않은 상기 정적 영역의 로드된 페이지에 대해 검증을 수행하는, 제2 호출자 인증을 수행하는 동작을 더 포함하는 방법.

[청구항 14]

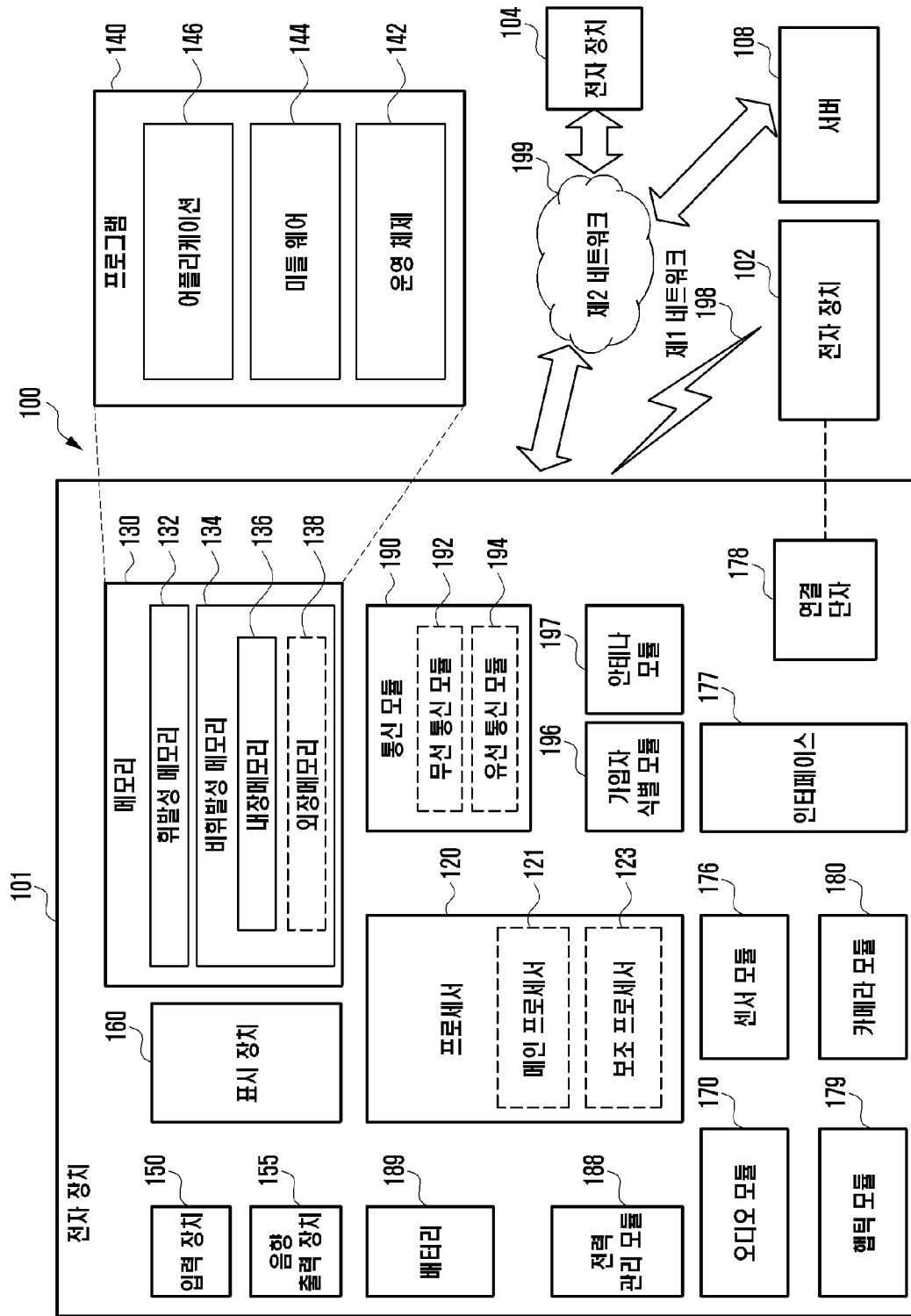
제 13 항에 있어서,
 상기 제2 호출자 인증을 수행하는 동작은,
 상기 매니저에 의해, 상기 제1 호출자 인증이 수행되지 않은 상기 정적 영역의 로드된 페이지에 대한 제3 해시 값을 생성하는 동작;
 상기 매니저에 의해, 상기 기 저장된 상기 정적 영역의 가상 메모리 주소에 대한 제2 해시 값과 상기 생성된 제3 해시 값을 비교하는 동작; 및
 상기 매니저에 의해, 상기 제2 해시 값과 상기 제3 해시 값이 동일한지 여부에 기반하여, 상기 제1 호출자 인증이 수행되지 않은 상기 정적 영역의 로드된 페이지에 대한 검증을 수행하는 상기 제2 호출자 인증을

수행하는 동작을 포함하고,
상기 제2 사용자 가상 메모리 주소 공간의 접근 권한에 대한 상기 읽기 접근이 활성화되고, 상기 쓰기 접근이 비활성화되게 설정하는 동작은,
상기 제2 해시 값과 상기 제3 해시 값이 동일한 경우, 상기 매니저에 의해,
상기 제2 호출자 인증을 성공한 것으로 결정하고, 상기 일반 환경의 상기 제2 사용자 가상 메모리 주소 공간의 접근 권한을 상기 읽기 및 쓰기 접근이 비활성화 상태에서, 상기 읽기 접근이 활성화되고 상기 쓰기 접근이 비활성되도록 변경하는 동작을 포함하는 방법.

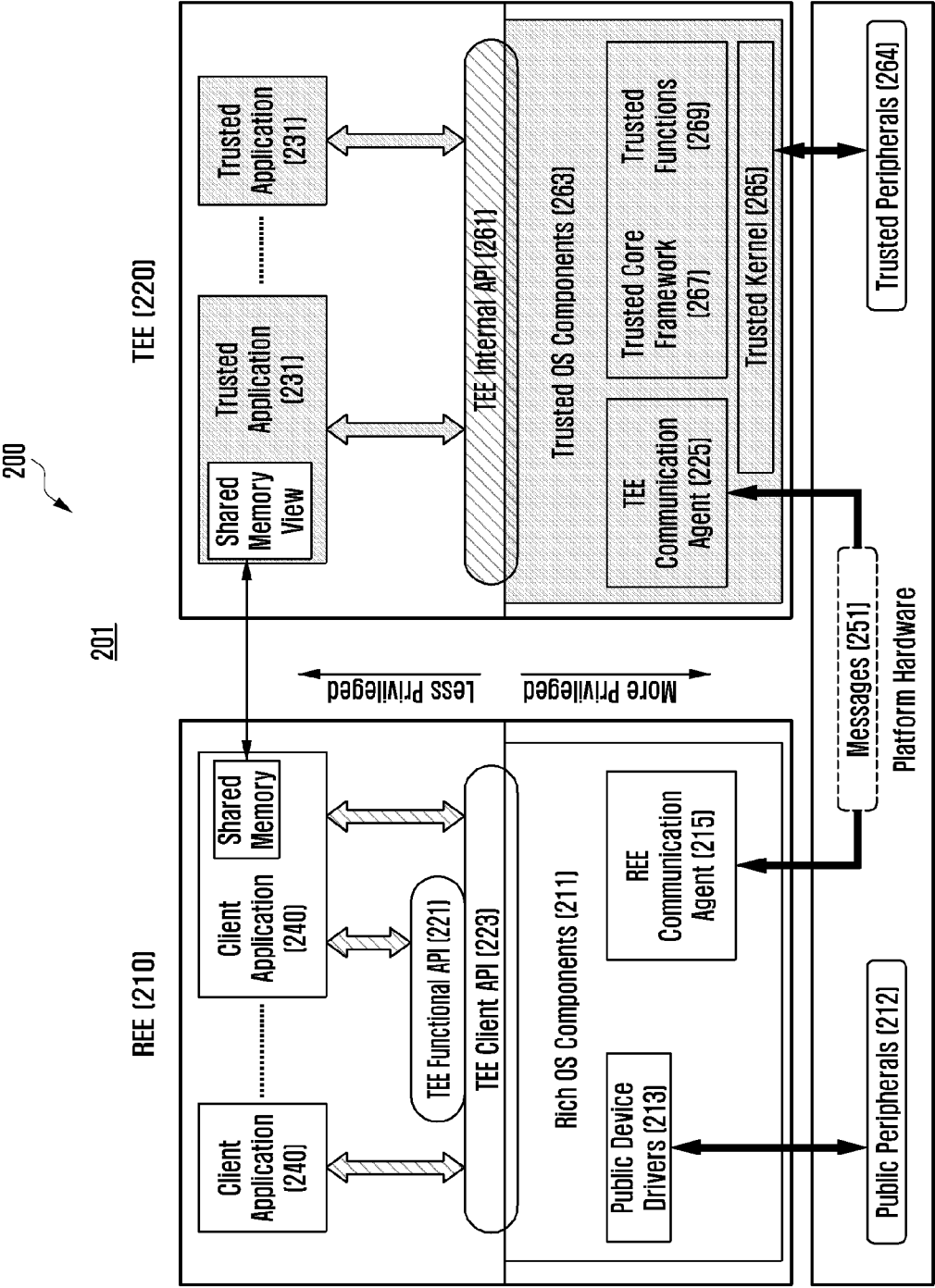
[청구항 15]

제 14 항에 있어서,
상기 매니저에 의해, 상기 보안 환경의 테이블 및 상기 제1 주소 공간의 접근 권한을 확인하는 동작;
상기 보안 환경의 테이블에 상기 데이터, 상기 제1 주소 공간 및 상기 제2 주소 공간의 가상 메모리 주소가 저장되어 있고, 상기 제1 주소 공간의 접근 권한에 대한 읽기 접근이 활성화되고, 쓰기 접근이 비활성화로 설정된 경우, 상기 보안 환경의 보안 어플리케이션을 호출하는 동작; 및
상기 보안 환경의 테이블에 상기 데이터, 상기 제1 주소 공간 및 상기 제2 주소 공간의 가상 메모리 주소가 저장되어 있지 않거나, 및/또는 상기 제1 주소 공간의 접근 권한에 대해 상기 쓰기 접근이 활성화로 설정된 경우, 상기 매니저에 의해 상기 보안 어플리케이션의 호출을 차단하는 동작을 더 포함하는 방법.

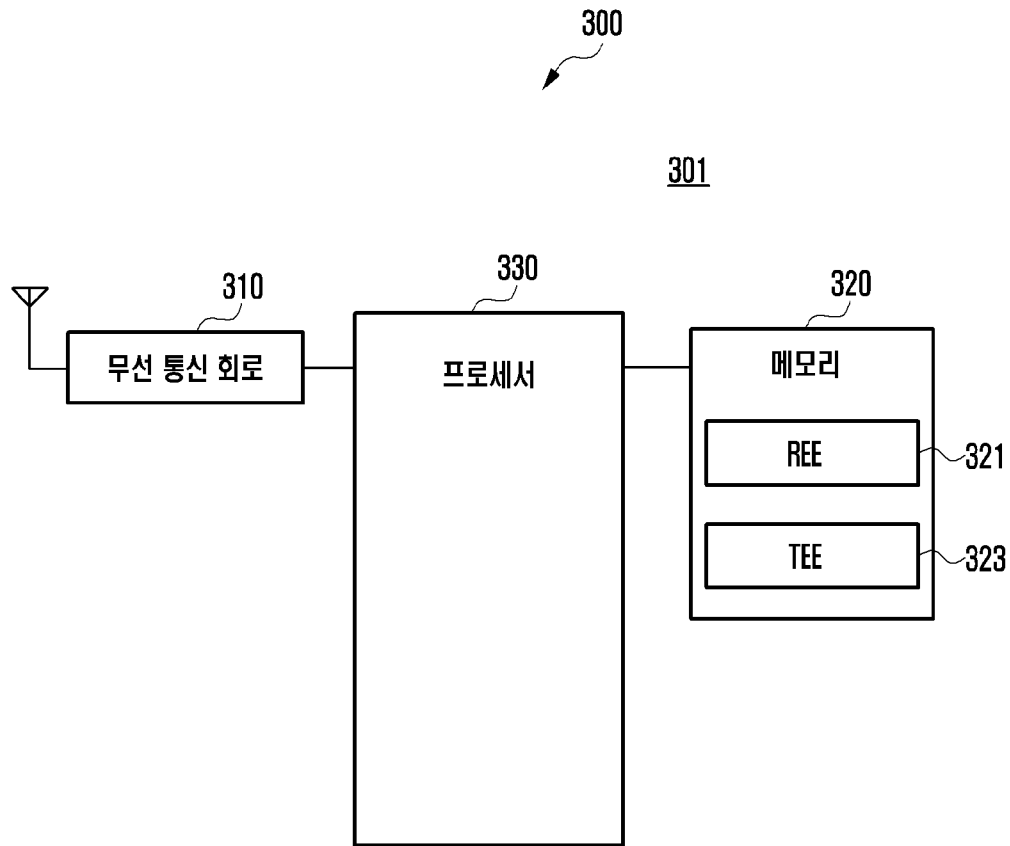
[도 1]



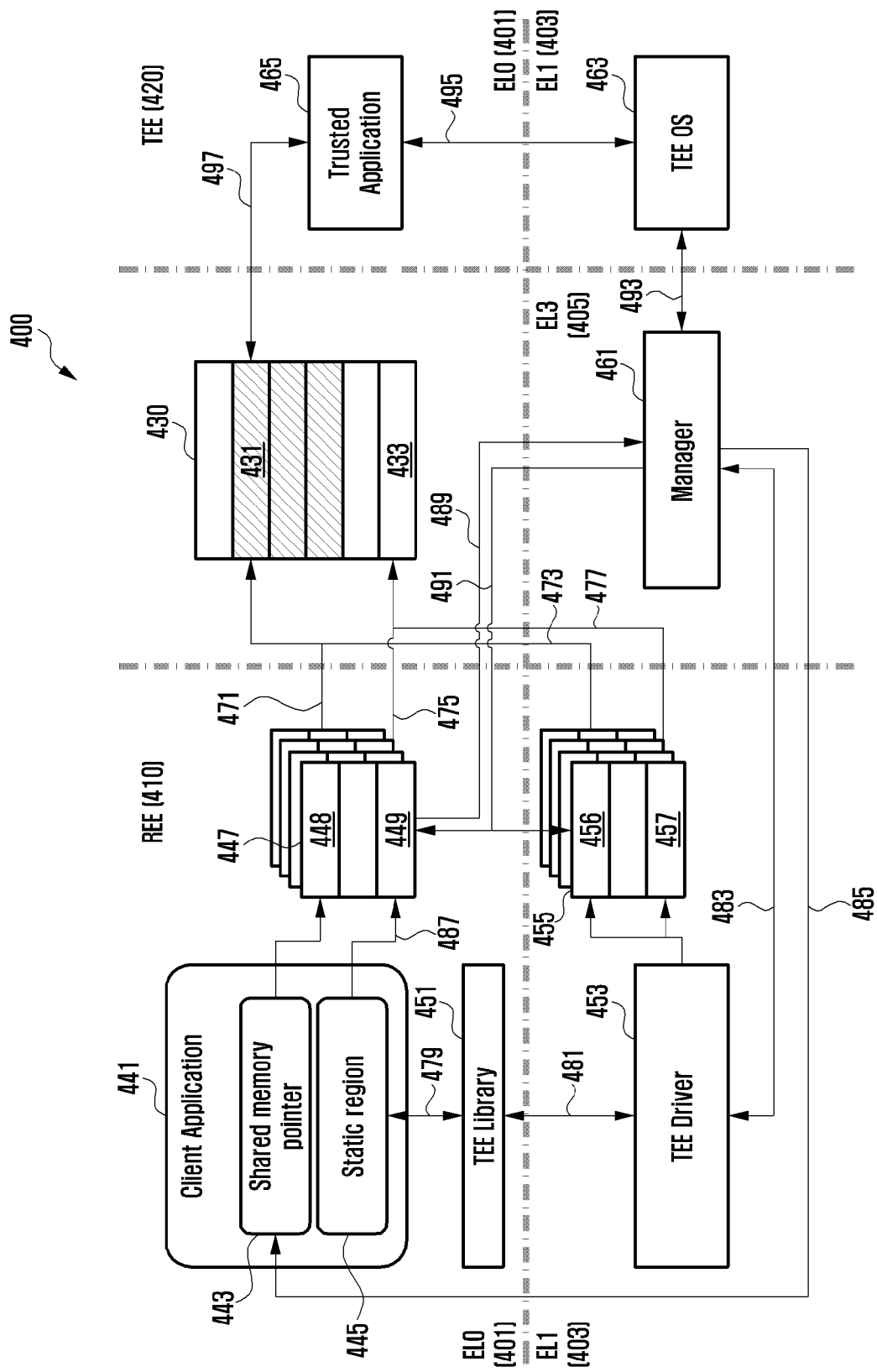
[도2]



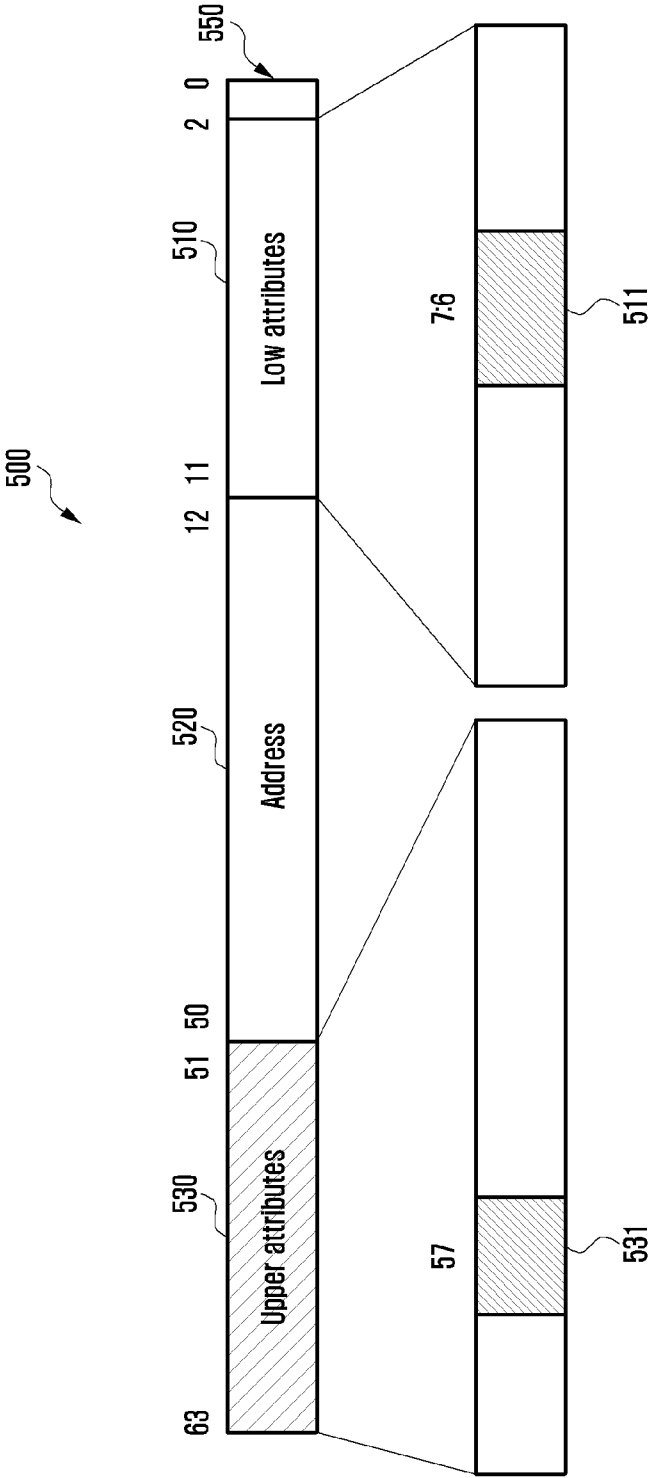
[도3]



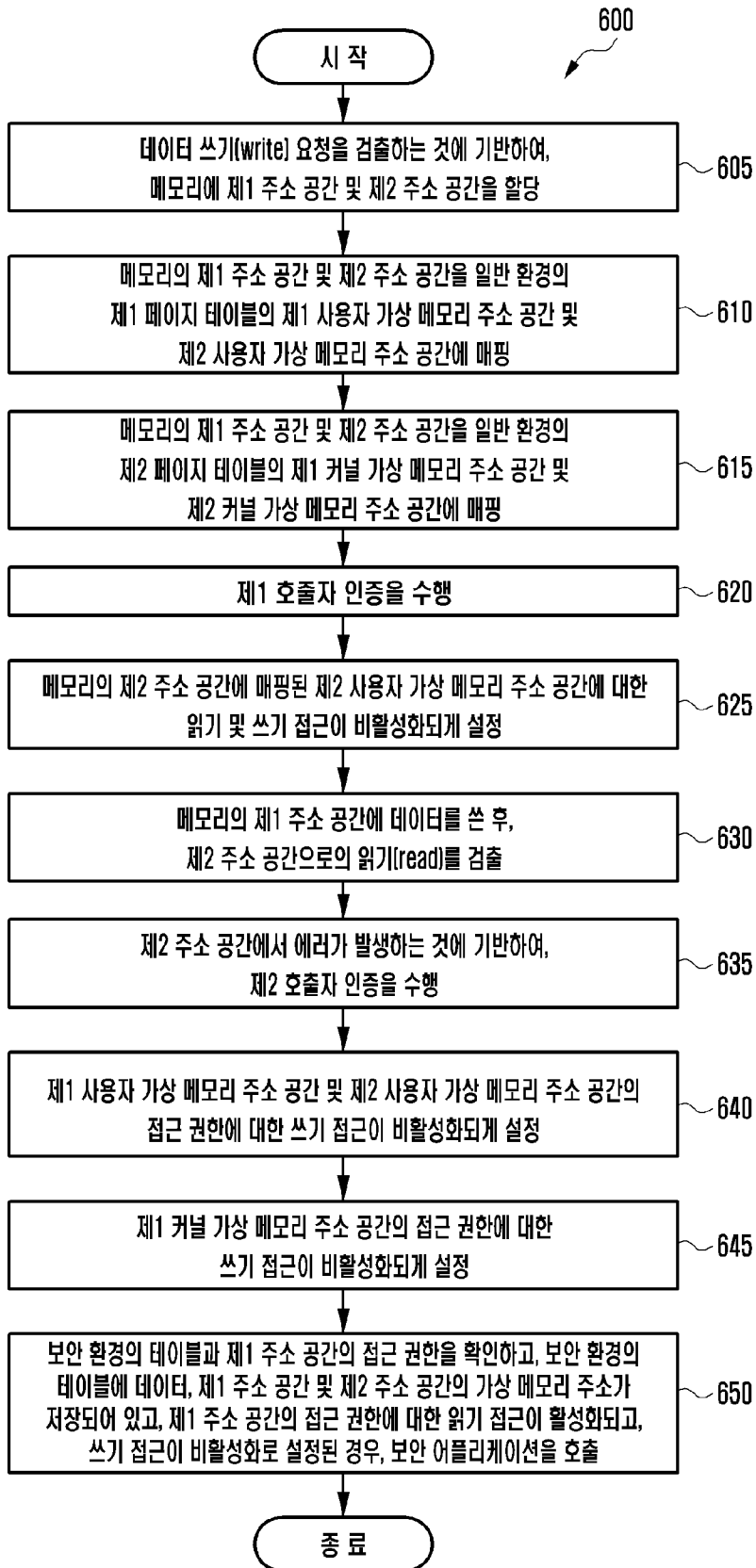
[도4]



[도5]



[도6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2021/015343

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/53(2013.01)i; G06F 21/60(2013.01)i; G06F 21/30(2013.01)i; G06F 12/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/53(2013.01); G06F 12/10(2006.01); G06F 12/14(2006.01); G06F 21/44(2013.01); G06F 21/60(2013.01);
G06F 21/62(2013.01); G06F 21/64(2013.01); G06F 9/455(2006.01); G06F 9/48(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 메모리(memory), 쓰기(write), 읽기(read), 비활성화(deactivate), 일반 환경(rich execution environment, REE)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2017-0067740 A (MICROSOFT TECHNOLOGY LICENSING, LLC) 16 June 2017 (2017-06-16) See paragraphs [0012]-[0014], [0032], [0039], [0041]-[0043] and [0057]-[0059]; claims 1-3 and 9; and figures 1-2.	1-15
A	KR 10-2017-0136406 A (SAMSUNG ELECTRONICS CO., LTD.) 11 December 2017 (2017-12-11) See paragraphs [0014]-[0035]; and figure 1.	1-15
A	KR 10-2075701 B1 (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) 10 February 2020 (2020-02-10) See paragraphs [0011]-[0039]; and figures 1-5.	1-15
A	US 2016-0364341 A1 (INTEL CORPORATION) 15 December 2016 (2016-12-15) See paragraphs [0037]-[0045]; and figure 1.	1-15
A	US 2017-0249260 A1 (SAHITA, Ravi L. et al.) 31 August 2017 (2017-08-31) See paragraphs [0045]-[0048].	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

07 February 2022

Date of mailing of the international search report

09 February 2022

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon Building 4, 189 Cheongsaro, Seo-gu, Daejeon 35208

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2021/015343

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
KR	10-2017-0067740	A	16 June 2017	CN	107077428	A	18 August 2017
				CN	107077428	B	14 August 2020
				EP	3201820	A1	09 August 2017
				US	2016-0092678	A1	31 March 2016
				US	9628279	B2	18 April 2017
				WO	2016-053923	A1	07 April 2016
KR	10-2017-0136406	A	11 December 2017	US	10705894	B2	07 July 2020
				US	2017-0344407	A1	30 November 2017
KR	10-2075701	B1	10 February 2020	None			
US	2016-0364341	A1	15 December 2016	CN	107667350	A	06 February 2018
				EP	3308317	A1	18 April 2018
				EP	3308317	B1	13 January 2021
				EP	3825851	A1	26 May 2021
				US	10754794	B2	25 August 2020
				US	2018-0113817	A1	26 April 2018
				US	2020-0364158	A1	19 November 2020
				US	9842065	B2	12 December 2017
				WO	2016-204892	A1	22 December 2016
US	2017-0249260	A1	31 August 2017	US	10503664	B2	10 December 2019
				US	10515023	B2	24 December 2019
				US	11144479	B2	12 October 2021
				US	2017-0249261	A1	31 August 2017
				US	2020-0159673	A1	21 May 2020

A. 발명이 속하는 기술분류(국제특허분류(IPC)) G06F 21/53(2013.01)i; G06F 21/60(2013.01)i; G06F 21/30(2013.01)i; G06F 12/08(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) G06F 21/53(2013.01); G06F 12/10(2006.01); G06F 12/14(2006.01); G06F 21/44(2013.01); G06F 21/60(2013.01); G06F 21/62(2013.01); G06F 21/64(2013.01); G06F 9/455(2006.01); G06F 9/48(2006.01) 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 메모리(memory), 쓰기(write), 읽기(read), 비활성화(deactivate), 일반 환경(rich execution environment, REE)		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2017-0067740 A (마이크로소프트 테크놀로지 라이선싱, 엔엘씨) 2017.06.16 단락 [0012]-[0014], [0032], [0039], [0041]-[0043], [0057]-[0059]; 청구항 1-3, 9; 및 도면 1-2	1-15
A	KR 10-2017-0136406 A (삼성전자주식회사) 2017.12.11 단락 [0014]-[0035]; 및 도면 1	1-15
A	KR 10-2075701 B1 (서울대학교산학협력단) 2020.02.10 단락 [0011]-[0039]; 및 도면 1-5	1-15
A	US 2016-0364341 A1 (INTEL CORPORATION) 2016.12.15 단락 [0037]-[0045]; 및 도면 1	1-15
A	US 2017-0249260 A1 (RAVIL L. SAHITA 등) 2017.08.31 단락 [0045]-[0048]	1-15
☐ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: “A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 “D” 본 국제출원에서 출원인이 인용한 문헌 “E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2022년02월07일(07.02.2022)		국제조사보고서 발송일 2022년02월09일(09.02.2022)
ISA/KR의 명칭 및 우편주소 대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578		심사관 양정록 전화번호 +82-42-481-5709

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2017-0067740 A	2017/06/16	CN 107077428 A	2017/08/18
		CN 107077428 B	2020/08/14
		EP 3201820 A1	2017/08/09
		US 2016-0092678 A1	2016/03/31
		US 9628279 B2	2017/04/18
		WO 2016-053923 A1	2016/04/07
KR 10-2017-0136406 A	2017/12/11	US 10705894 B2	2020/07/07
		US 2017-0344407 A1	2017/11/30
KR 10-2075701 B1	2020/02/10	없음	
US 2016-0364341 A1	2016/12/15	CN 107667350 A	2018/02/06
		EP 3308317 A1	2018/04/18
		EP 3308317 B1	2021/01/13
		EP 3825851 A1	2021/05/26
		US 10754794 B2	2020/08/25
		US 2018-0113817 A1	2018/04/26
		US 2020-0364158 A1	2020/11/19
		US 9842065 B2	2017/12/12
		WO 2016-204892 A1	2016/12/22
US 2017-0249260 A1	2017/08/31	US 10503664 B2	2019/12/10
		US 10515023 B2	2019/12/24
		US 11144479 B2	2021/10/12
		US 2017-0249261 A1	2017/08/31
		US 2020-0159673 A1	2020/05/21