(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2024 년 5 월 30 일 (30.05.2024)

WIPO | PCT

(10) 국제공개번호
WO 2024/112057 A1

(51) 국제특허분류:
G06F 21/79 (2013.01) *G06F 21/60* (2013.01)
G06F 21/53 (2013.01) *H04W 12/03* (2021.01)

(21) 국제출원번호: PCT/KR2023/018740

(22) 국제출원일: 2023 년 11 월 21 일 (21.11.2023)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2022-0160173 2022 년 11 월 25 일 (25.11.2022) KR

(71) 출원인: 삼성전자 주식회사 (**SAMSUNG ELECTRONICS CO., LTD.**) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(72) 발명자: **황진하 (HWANG, Jinha)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **김인호 (KIM, Inho)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **이동선 (LEE, Dongsun)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **류재민 (RYU, Jaemin)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **정경임 (JUNG, Kyungim)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

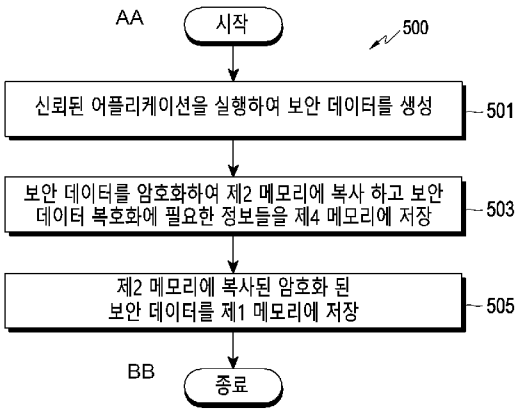
(74) 대리인: **이건주 등 (LEE, Keon-Joo** et al.); 03079 서울특별시 종로구 대학로9길 16 미화빌딩, Seoul (KR).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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 역내 권리의 보호를 위하여): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ,

(54) **Title:** ELECTRONIC DEVICE FOR STORING SECURE DATA AND OPERATION METHOD THEREFOR

(54) **발명의 명칭:** 보안 데이터를 저장하는 전자 장치 및 그 동작 방법



501 ... Generate secure data by running trusted application
503 ... Encrypt secure data, copy same to second memory, and store information necessary for secure data decryption in fourth memory
505 ... Store, in first memory, encrypted secure data copied to second memory
AA ... Start
BB ... End

(57) Abstract: According to one embodiment, an electronic device may comprise: a first processor operating in a general non-secure environment; a second processor operating in a secure environment; a first memory allocated to the general non-secure environment; a second memory allocated to the secure environment; and a third memory shared between the general non-secure environment and the secure environment. The second processor may be configured to: encrypt at least a part of secure data in order to generate an encrypted portion, wherein the secure data is generated by a trusted application running in the secure environment; store the encrypted portion in the third memory; and store, in the second memory, first information used to encrypt at least a part of the secure data and second information generated while encrypting at least a part of the secure data. The first processor may be configured to store, in the first memory, the encrypted portion that is stored in the third memory.

(57) 요약서: 일 실시 예에 따라서, 전자 장치는, 일반 비보안 환경에서 동작하는 제1 프로세서; 보안 환경에서 동작하는 제2 프로세서; 상기 일반 비보안 환경에 할당된 제1 메모리; 상기 보안 환경에 할당된 제2 메모리; 및 상기 일반 비보안 환경과 상기 보안 환경에서 공유되는 제3 메모리를 포함할 수 있다. 상기 제2 프로세서는, 암호화 된 부분을 생성하기 위해 보안 데이터 중 적어도 일부를 암호고, 상기 보안 데이터는 상기 보안 환경에서 실행되는 신뢰된 어플리케이션에 의해 생성되고, 상기 암호화 된 부분을 상기 제3 메모리에 저장하고, 상기 보안 데이터 중 적어도 일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를 상기 제2 메모리에 저장하도록 설정될 수 있다. 상기 제1 프로세서는, 상기 제3 메모리에 저장된, 상기 암호화 된 부분을 상기 제1 메모리에 저장하도록 설정될 수 있다.

WO 2024/112057 A1

[다음 쪽 계속]

TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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))

명세서

발명의 명칭: 보안 데이터를 저장하는 전자 장치 및 그 동작 방법

기술분야

[1] 본 개시는 보안 데이터를 저장하는 전자 장치 및 그 동작 방법에 관한 것이다.

배경기술

[2] 무선 통신 시스템에서 전자 장치(예: 사용자 장치(user equipment: UE))는 무선 통신 네트워크에 접속하여 정해진 위치나 이동 중에 음성 통신 서비스 또는 데이터 통신 서비스를 이용할 수 있다. 음성 통신 서비스 또는 데이터 통신 서비스 이외에도 전자 장치를 통해 제공되는 서비스 및 부가 기능들은 점차 증가하고 있다. 전자 장치에 다양한 서비스와 부가 기능들을 제공하기 위해서는 적절한 인증 과정이 필요하며 보안이 요구되는 데이터들을 안전하게 처리할 필요가 있다.

[3] 일반적으로는 UICC(universal integrated circuit card; 범용 집적 회로 카드)가 전자 장치에 삽입되고, UICC 내부에 설치되어 있는 USIM(universal subscriber identity module)을 통해 전자 장치와 통신 사업자(mobile network operator; MNO)의 서버 간에 인증이 수행된다. 전자 장치의 사용자가 MNO가 제공하는 무선 통신 서비스에 가입하면, MNO는 사용자에게 UICC(예: SIM 카드 또는 USIM 카드)를 제공하고, 사용자가 자신의 전자 장치에 제공받은 UICC를 삽입할 수 있다. 최근에는 사용자가 MNO를 변경하더라도 UICC를 교체하지 않고도, 통신 서비스 제공을 위한 프로파일(profile)을 네트워크를 통해 원격으로 설치할 수 있는 이른바 eUICC(embedded UICC)이 제안되고 있다. 상기 eUICC는 단말의 제조 과정에서 단말 내에 고정된 UICC 칩으로 제작될 수 있다. eUICC 보다 진보된 SIM 기능을 전자 기기의 하드웨어에 통합하여 SOC(system on chip) 형태로 구성하는 통합형 SIM(integrated SIM, 이하 iSIM)이 제안되었다.

[4] iSIM은 휴대폰과 같은 일반 무선 단말은 물론 M2M(machine to machine) 또는 D2D(device to device) 단말, 및 사물 인터넷(internet of things: IoT) 기기와 같이 물리적으로 UICC의 착탈이 용이하지 않는 구조를 가질 수 있는 각종 전자 장치에 이용될 수 있다.

발명의 상세한 설명

과제 해결 수단

[5] 일 실시 예에 따른 전자 장치는, 일반 비보안 환경에서 동작하는 제1 프로세서; 보안 환경에서 동작하는 제2 프로세서; 상기 일반 비보안 환경에 할당된 제1 메모리; 상기 보안 환경에 할당된 제2 메모리; 및 상기 일반 비보안 환경과 상기 보안 환경에서 공유되는 제3 메모리를 포함할 수 있다. 상기 제2 프로세서는, 암호화 된 부분을 생성하기 위해 보안 데이터 중 적어도 일부를 암호고, 상기 보안 데이터는 상기 보안 환경에서 실행되는 신뢰된 어플리케이션에 의해 생성되고, 상기 암호화 된 부분을 상기 제3 메모리에 저장하고, 상기 보안 데이터 중 적어도

일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를 상기 제2 메모리에 저장하도록 설정될 수 있다. 상기 제1 프로세서는, 상기 제3 메모리에 저장된, 상기 암호화 된 부분을 상기 제1 메모리에 저장하도록 설정될 수 있다.

[6] 일 실시 예에 따른 전자 장치의 동작 방법은, 보안 환경에서 동작하는 제1 프로세서에 의해, 상기 보안 환경에서 신뢰된 어플리케이션을 실행하고 보안 데이터를 생성하는 동작을 포함할 수 있다. 상기 방법은, 상기 제1 프로세서에 의해, 암호화 된 부분을 생성하기 위해 상기 생성된 보안 데이터 중 적어도 일부를 암호화 하고, 상기 암호화된 부분을 상기 보안 환경과 일반 비보안 환경에서 공유되는 제1 메모리에 저장하는 동작을 포함할 수 있다. 상기 방법은, 상기 제1 프로세서에 의해, 상기 보안 데이터 중 적어도 일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를, 상기 보안 환경에 할당된 제2 메모리에 저장하는 동작을 포함할 수 있다. 상기 방법은, 상기 일반 비보안 환경에서 동작하는 제2 프로세서에 의해, 상기 제1 메모리에 저장된, 상기 암호화 된 부분을 상기 일반 비보안 환경에 할당된 제3 메모리에 저장하는 동작을 포함할 수 있다.

[7] 일 실시 예에 따른 하나 이상의 프로그램을 저장하는 비일시적 컴퓨터 판독 가능 저장 매체에 있어서, 상기 하나 이상의 프로그램은 전자 장치의 적어도 하나의 프로세서에 의해 실행될 때 상기 전자 장치가; 보안 환경에서 동작하는 제1 프로세서에 의해, 상기 보안 환경에서 신뢰된 어플리케이션을 실행하고 보안 데이터를 생성하고, 상기 제1 프로세서에 의해, 암호화 된 부분을 생성하기 위해 상기 생성된 보안 데이터 중 적어도 일부를 암호화 하고, 상기 암호화된 부분을 상기 보안 환경과 일반 비보안 환경에서 공유되는 제1 메모리에 저장하고, 상기 제1 프로세서에 의해, 상기 보안 데이터 중 적어도 일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를, 상기 보안 환경에 할당된 제2 메모리에 저장하고, 상기 일반 비보안 환경에서 동작하는 제2 프로세서에 의해, 상기 제1 메모리에 저장된, 상기 암호화 된 부분을 상기 일반 비보안 환경에 할당된 제3 메모리에 저장하도록 구성하는 명령어들을 포함할 수 있다.

도면의 간단한 설명

[8] 도 1은, 하나 또는 그 이상의 실시 예에 따른, 네트워크 환경 내의 전자 장치(101)의 블록도이다.

[9] 도 2는 하나 또는 그 이상의 실시 예에 따른 프로그램의 블록도이다.

[10] 도 3은 하나 또는 그 이상의 실시 예에 따른 프로그램 모듈을 설명하기 위한 블록도를 도시한다.

[11] 도 4는 하나 또는 그 이상의 실시 예에 따른 전자 장치의 프로그램 모듈에 따른 실행 환경의 일 예를 설명하기 위한 도면이다.

[12] 도 5는 하나 또는 그 이상의 실시 예에 따른 전자 장치의 동작의 일 예를 설명하기 위한 흐름도이다.

[13] 도 6은 하나 또는 그 이상의 실시 예에 따라 도 5의 전자 장치의 동작의 일 예를 설명하기 위한 도면이다.

[14] 도 7은 하나 또는 그 이상의 실시 예에 따른 전자 장치의 동작의 일 예를 설명하기 위한 흐름도이다.

[15] 도 8은 하나 또는 그 이상의 실시 예에 따라 도 7의 전자 장치의 동작의 일 예를 설명하기 위한 도면이다.

[16] 도 9는 하나 또는 그 이상의 실시 예에 따른 전자 장치의 메모리에 저장되는 보안 데이터의 포맷의 일 예를 설명하기 위한 도면이다.

발명의 실시를 위한 형태

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

[18] 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. 하나 또는 그 이상의 실시 예에 따르면, 전자 장치(101)는 서버(108)를 통하여 전자 장치(104)와 통신할 수 있다. 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에서는, 전자 장치(101)에는, 이 구성요소들 중 적어도 하나(예: 연결 단자(178))가 생략되거나, 하나 이상의 다른 구성요소가 추가될 수 있다. 어떤 실시 예에서는, 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.

[19] 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. 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에 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.

[20] 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. 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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. 하나 또는 그 이상의 실시 예에 따르면, 리시버는 스피커와 별개로, 또는 그 일부로서 구현될 수 있다.

[25] 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. 하나 또는 그 이상의 실시 예에 따르면, 디스플레이 모듈(160)은 터치를 감지하도록 설정된 터치 센서, 또는 상기 터치에 의해 발생되는 힘의 세기를 측정하도록 설정된 압력 센서를 포함할 수 있다.

[26] 오디오 모듈(170)은 소리를 전기 신호로 변환시키거나, 반대로 전기 신호를 소리로 변환시킬 수 있다. 하나 또는 그 이상의 실시 예에 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.

[27] 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. 하나 또는 그 이상의 실시 예에 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.

[28] 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. 하나 또는 그 이상의 실시 예에 따르면, 인터페이스(177)는, 예를 들면, HDMI(high definition multimedia interface), USB(universal serial bus) 인터페이스, SD카드 인터페이스, 또는 오디오 인터페이스를 포함할 수 있다.

[29] 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. 하나 또는 그 이상의 실시 예에 따르면, 연결 단자(178)는, 예를 들면, HDMI 커넥터, USB 커넥터, SD 카드 커넥터, 또는 오디오 커넥터(예: 헤드폰 커넥터)를 포함할 수 있다.

[30] 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. 하나 또는 그 이상의 실시 예에 따르면, 햅틱 모듈(179)은, 예를 들면, 모터, 압전 소자, 또는 전기 자극 장치를 포함할 수 있다.

[31] 카메라 모듈(180)은 정지 영상 및 동영상을 촬영할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 카메라 모듈(180)은 하나 이상의 렌즈들, 이미지 센서들, 이미지 시그널 프로세서들, 또는 플래시들을 포함할 수 있다.

[32] 전력 관리 모듈(188)은 전자 장치(101)에 공급되는 전력을 관리할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 전력 관리 모듈(188)은, 예를 들면, PMIC(power management integrated circuit)의 적어도 일부로서 구현될 수 있다.

[33] 배터리(189)는 전자 장치(101)의 적어도 하나의 구성요소에 전력을 공급할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 배터리(189)는, 예를 들면, 재충전 불가능한 1차 전지, 재충전 가능한 2차 전지 또는 연료 전지를 포함할 수 있다.

[34] 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. 하나 또는 그 이상의 실시 예에 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.

[35] 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 최소화와 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. 하나 또는 그 이상의 실시 예에 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.

[36] 안테나 모듈(197)은 신호 또는 전력을 외부(예: 외부의 전자 장치)로 송신하거나 외부로부터 수신할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 안테나 모듈(197)은 서브스트레이트(예: PCB) 위에 형성된 도전체 또는 도전성 패턴으로 이루어진 방사체를 포함하는 안테나를 포함할 수 있다. 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에 따르면, 방사체 이외에 다른 부품(예: RFIC(radio frequency integrated circuit))이 추가로 안테나 모듈(197)의 일부로 형성될 수 있다.

[37] 하나 또는 그 이상의 실시 예에 따르면, 안테나 모듈(197)은 mmWave 안테나 모듈을 형성할 수 있다. 하나 또는 그 이상의 실시 예에 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.

[38] 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))을 통해 서로 연결되고 신호(예: 명령 또는 데이터)를 상호간에 교환할 수 있다.

[39] 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에 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 헬스 케어)에 적용될 수 있다.

[40] 도 2는 하나 또는 그 이상의 실시 예에 따른 프로그램(140)의 블록도(200)이다. 하나 또는 그 이상의 실시 예에 따르면, 프로그램(140)은 전자 장치(101)의 하나 이상의 리소스들을 제어하기 위한 운영 체제(142), 미들 웨어(144), 또는 상기 운영 체제(142) 상에서 실행 가능한 어플리케이션(146)을 포함할 수 있다. 운영 체제(142)는, 예를 들면, Android™, iOS™, Windows™, Symbian™, Tizen™, 또는 Bada™를 포함할 수 있다. 프로그램(140) 중 적어도 일부 프로그램은, 예를 들면, 제조 시에 전자 장치(101)에 프리로드 되거나, 또는 사용자가 전자 장치를 사용하는 환경에서 외부 전자 장치(예: 전자 장치(102 또는 104), 또는 서버(108))로부터 다운로드 되거나 갱신 될 수 있다.

[41] 운영 체제(142)는 전자 장치(101)의 시스템 리소스 (예: 프로세스, 메모리, 또는 전원)를 제어(예: 할당 또는 회수)할 수 있다. 운영 체제(142)는, 추가적으로 또는 대체적으로, 전자 장치(101)의 다른 하드웨어 디바이스, 예를 들면, 입력 장치(150), 음향 출력 장치(155), 표시 장치(160), 오디오 모듈(170), 센서 모듈(176), 인터페이스(177), 햅틱 모듈(179), 카메라 모듈(180), 전력 관리 모듈(188), 배터리(189), 통신 모듈(190), 가입자 식별 모듈(196), 또는 안테나 모듈(197)을 구동하기 위한 하나 이상의 드라이버 프로그램들을 포함할 수 있다.

[42] 미들 웨어(144)는 어플리케이션(146)이 전자 장치(101)의 하나 이상의 리소스들이 제공하는 기능 또는 정보를 사용할 수 있도록 다양한 기능들을 어플리케이션(146)으로 제공할 수 있다. 미들 웨어(144)는, 예를 들면, 어플리케이션 매니저(201), 윈도우 매니저(203), 멀티미디어 매니저(205), 리소스 매니저(207), 파워 매

니저(209), 데이터베이스 매니저(211), 패키지 매니저(213), 커넥티비티 매니저(215), 노티피케이션 매니저(217), 로케이션 매니저(219), 그래픽 매니저(221), 시큐리티 매니저(223), 통화 매니저(225), 또는 음성 인식 매니저(227)를 포함할 수 있다. 어플리케이션 매니저(201)는, 예를 들면, 어플리케이션(146)의 생명 주기를 관리할 수 있다. 윈도우 매니저(203)는, 예를 들면, 화면에서 사용되는 GUI 자원을 관리할 수 있다. 멀티미디어 매니저(205)는, 예를 들면, 미디어 파일들의 재생에 필요한 포맷을 파악하고, 해당 포맷에 맞는 코덱을 이용하여 미디어 파일의 인코딩 또는 디코딩을 수행할 수 있다. 리소스 매니저(207)는, 예를 들면, 어플리케이션(146)의 소스 코드 또는 메모리의 공간을 관리할 수 있다. 파워 매니저(209)는, 예를 들면, 배터리의 용량, 온도 또는 전원을 관리하고, 이 중 해당 정보를 이용하여 전자 장치(101)의 동작에 필요한 전력 정보를 결정 또는 제공할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 파워 매니저(209)는 바이오스(BIOS: basic input/output system)와 연동할 수 있다.

[43] 데이터베이스 매니저(211)는, 예를 들면, 어플리케이션(146)에서 사용될 데이터베이스를 생성, 검색, 또는 변경할 수 있다. 패키지 매니저(213)는, 예를 들면, 패키지 파일의 형태로 배포되는 어플리케이션의 설치 또는 갱신을 관리할 수 있다. 커넥티비티 매니저(215)는, 예를 들면, 전자 장치(101)와 외부 전자 장치 간의 무선 또는 유선 연결을 관리할 수 있다. 노티피케이션 매니저(217)는, 예를 들면, 발생된 이벤트(예: 통화, 메시지, 또는 알람)를 사용자에게 알리기 위한 기능을 제공할 수 있다. 로케이션 매니저(219)는, 예를 들면, 전자 장치(101)의 위치 정보를 관리할 수 있다. 그래픽 매니저(221)는, 예를 들면, 사용자에게 제공될 그래픽 효과 또는 이와 관련된 사용자 인터페이스를 관리할 수 있다. 시큐리티 매니저(223)는, 예를 들면, 시스템 보안 또는 사용자 인증을 제공할 수 있다. 통화(telephony) 매니저(225)는, 예를 들면, 전자 장치(101)의 음성 통화 또는 영상 통화 기능을 관리할 수 있다. 음성 인식 매니저(227)는, 예를 들면, 사용자의 음성 데이터를 서버(108)로 전송하고, 해당 음성 데이터에 기반하여 전자 장치(101)에서 수행될 기능에 대응하는 명령어(command) 또는 해당 음성 데이터에 기반하여 변환된 문자 데이터를 수신할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 미들 웨어(244)는 동적으로 기존의 구성요소를 일부 삭제하거나 새로운 구성요소들을 추가할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 미들 웨어(144)의 적어도 일부는 운영 체제(142)의 일부로 포함되거나, 또는 운영 체제(142)와는 별도의 소프트웨어로 구현될 수 있다.

[44] 어플리케이션(146)은, 예를 들면, 홈(251), 다이얼러(253), SMS/MMS(255), IM(instant message)(257), 브라우저(259), 카메라(261), 알람(263), 컨택트(265), 음성 인식(267), 이메일(269), 달력(271), 미디어 플레이어(273), 앨범(275), 와치(277), 헬스(279)(예: 운동량 또는 혈당 등을 측정), 또는 환경 정보(281)(예: 기압, 습도, 또는 온도 정보) 어플리케이션을 포함할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 어플리케이션(146)은 전자 장치(101)와 외부 전자 장치 사이의 정

보 교환을 지원하도록 구성된 정보 교환 어플리케이션을 더 포함할 수 있다. 정보 교환 어플리케이션은, 예를 들면, 외부 전자 장치로 지정된 정보 (예: 통화, 메시지, 또는 알람)를 전달하기 위한 노티피케이션 릴레이 어플리케이션, 또는 외부 전자 장치를 관리하기 위한 장치 관리 어플리케이션을 포함할 수 있다. 노티피케이션 릴레이 어플리케이션은, 예를 들면, 전자 장치(101)의 다른 어플리케이션(예: 이메일 어플리케이션(269))에서 발생된 이벤트(예: 메일 수신)에 대응하는 알림 정보를 외부 전자 장치로 전달하거나, 또는 외부 전자 장치로부터 알림 정보를 수신하여 전자 장치(101)의 사용자에게 제공할 수 있다. 장치 관리 어플리케이션은, 예를 들면, 전자 장치(101)와 통신하는 외부 전자 장치 또는 그 일부 구성 요소(예: 표시 장치(160) 또는 카메라 모듈(180))의 전원(예: 턴-온 또는 턴-오프) 또는 기능(예: 표시 장치(160) 또는 카메라 모듈(180)의 밝기, 해상도, 또는 포커스)을 제어할 수 있다. 장치 관리 어플리케이션은, 추가적으로 또는 대체적으로, 외부 전자 장치에서 동작하는 어플리케이션의 설치, 삭제, 또는 갱신을 지원할 수 있다.

[45] 이하에서는 다양한 실시 예들에 따른 전자 장치(예: 도 1의 전자 장치(101))의 구성의 일 예에 대해서 설명한다. 이하에서 기술되는 전자 장치는 도 1에서 전술한 전자 장치(101)와 같이 구현될 수 있으므로 중복되는 설명은 생략한다.

[46] 도 3은 하나 또는 그 이상의 실시 예에 따른 전자 장치(101)의 구성의 일 예를 설명하기 위한 도면이다. 다만 당업자가 이해하는 바와 같이, 전자 장치(101)는 도 3에 도시되는 구성들 보다 더 많은 구성들 또는 더 적은 구성들을 포함하도록 구현될 수 있다. 이하에서는 도 4를 참조하여 도 3에 대해서 설명한다.

[47] 도 4는 하나 또는 그 이상의 실시 예에 따른 전자 장치(예: 도 1의 전자 장치(101))의 프로그램 모듈에 따른 실행 환경의 일 예를 설명하기 위한 도면이다.

[48] 도 4를 참조하면, 프로그램 모듈(400)은, REE(rich execution environment)(410) 및 TEE(trusted execution environment)(420)를 포함할 수 있다. REE(410) 및 TEE(420)는, 예를 들어 하드웨어적으로 구분될 수 있거나, 또는 소프트웨어적으로 구분될 수도 있다. 하나 또는 그 이상의 예에서, REE(410) 및 TEE(420)는 물리적으로 분리되고/또는 소프트웨어적으로도 분리될 수도 있다. REE(410)는, 일반적인 운영체제(예: 도 2의 운영 체제(242))가 작동하는 환경일 수 있다. 예를 들어 안드로이드 운영 체제, 윈도우즈(windows) 운영 체제, 리눅스(linux) 운영 체제 등이 REE(410)에서 작동할 수 있다. TEE(420)는, 보안적으로 안전하게 보호되는 운영 체제, 예를 들어 보안 운영 체제(secured operating system)가 작동하는 환경 또는 당업자에게 잘 알려진 어떤 다른 작업 시스템일 수 있다. 예를 들어, 퀄컴(qualcomm)의 QSee, 트러스토닉(trustonic)의 Kinibi 등의 보안 운영 체제가 TEE(420)에서 작동할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, iSIM 기능을 지원하는 애플리케이션이 TEE(420)에서 작동할 수 있다. 보안 운영 체제를 기반으로 하는 데이터 처리가 보안적으로 또한 안전하게 TEE(420) 내에서 수행될 수 있다. TEE(420)는, 트러스트 존(trust zone), 보안 실행 환경(secure execution

environment), 플랫폼 보안 프로세서(platform security processor), 신뢰된 실행 기술(trusted execution technology), 소프트웨어 방어 확장(software guard extensions), 또는 당업자에게 알려진 어떤 다른 구현 구성과 같은 다양한 방식으로 구현될 수 있으며, 구현되는 구성에는 제한이 없음을 당업자가 용이하게 이해할 수 있을 것이다.

[49] 하나 또는 그 이상의 실시 예에 따라서, REE(410)에는, 어플리케이션 계층(411), 프레임워크(framework) 계층(412) 및 커널(kernel) 계층(413)이 포함될 수 있다. 어플리케이션 계층(411)에서는, 다양한 어플리케이션(예: 도 2의 어플리케이션(246))이 작동할 수 있다. 프레임워크 계층(412)은, 어플리케이션의 작동을 지원하는 기능 및 운영 체제가 제공하는 서비스가 작동할 수 있다. 커널 계층(413)은, 운영 체제의 핵심 기능이 작동하는 계층일 수 있다. 커널 계층(413), 예를 들면, 다른 프로그램들에 구현된 작동 또는 기능을 실행하는 데 사용되는 시스템 리소스들을 제어 또는 관리하도록 구성될 있다. 또한, 커널 계층(413)은 전자 장치(101)의 개별 구성요소에 접근함으로써, 시스템 리소스들을 제어 또는 관리할 수 있는 인터페이스를 제공할 수 있다.

[50] 하나 또는 그 이상의 실시 예에 따라서, TEE(420)에는, 신뢰된 어플리케이션(trusted application) 계층(421), 신뢰된 프레임워크(trusted framework) 계층(422) 및 보안 OS 커널(secured operating system kernel) 계층(423)이 포함될 수 있다. 신뢰된 어플리케이션 계층(421)에서는, 신뢰된 어플리케이션(trusted application)이 작동할 수 있다. 하나 또는 그 이상의 실시 예에 따라서, 전자 장치(101)는, iSIM 기능을 수행하는 어플리케이션을 신뢰된 어플리케이션 계층(421)에서 실행시킬 수 있다. 신뢰된 어플리케이션은, 어플리케이션의 실행 과정에서 보안이 필요한 데이터들을 생성, 송수신, 및 저장할 수 있으며, 이에 대하여서는 더욱 상세하게 후술하도록 한다. 신뢰된 프레임워크 계층(422)은, TEE(420)에서 작동하는 운영 체제, 예를 들어 보안 운영 체제가 작동할 수 있다. 보안 OS 커널 계층(423)은, 보안 운영 체제의 핵심 기능이 작동하는 계층일 수 있다. 보안 OS 커널 계층(423), 예를 들면, 신뢰된 어플리케이션 또는 보안 운영 체제에 구현된 작동 또는 기능을 실행하는 데 사용되는 시스템 리소스들을 제어 또는 관리할 수 있다.

[51] 하드웨어 계층(430)에서는, 전자 장치(101)의 다양한 하드웨어(예: 메모리(330) 및 프로세서(320))가 작동할 수 있다.

[52] 프로세서(320)는 제1 프로세서(321) 및 제2 프로세서(322)를 포함할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 제1 프로세서(321)와 제2 프로세서(322)는 서로 격리된 복수의 실행 환경들(예: REE(410) 및 TEE(420))에서 실행되는 동작을 수행할 수 있다. 예를 들어, 복수의 실행 환경들은, 소프트웨어적으로 격리된 실행 환경들로 구현되거나, 하드웨어적으로 격리된 실행 환경들로 구현되거나 이들의 조합으로 구현될 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 제1 프로세서(321) 및 제2 프로세서(322) 각각은 복수의 실행 환경들 중 적어도 하나에서 동작하여, 지정된 동작을 수행하거나, 및/또는 전자 장치(101)에 포함된

적어도 하나의 하드웨어 구성 요소를 제어할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 제1 프로세서(321)는 AP(application processor)를 포함할 수 있고, REE(410)에서 실행되는 동작들을 수행할 수 있다. 일 실시 예에 따르면, 제2 프로세서(322)는 SP(secure processor)를 포함할 수 있고, TEE(420)에서 실행되는 동작들을 수행할 수 있다. 이하에서 설명되는 프로세서(320)(예: 제1 프로세서(321), 및 제2 프로세서(322))의 동작은 메모리(330)에 저장되는 모듈들의 실행에 따라서 수행될 수 있다. 예를 들어, 모듈들의 적어도 일부는 소프트웨어, 펌웨어, 또는 이들 중 적어도 둘 이상의 조합으로 구현(예를 들어, 실행)될 수 있다. 예를 들어, 상기 모듈들은 프로세서(320)에 의해 실행 가능한 어플리케이션(application), 프로그램(program), 컴퓨터 코드(computer code), 인스트럭션들(instructions), 루틴(routine), 내지는 프로세스(process)의 형태로 구현될 수 있다. 이에 따라, 상기 모듈들이 프로세서(320)에 의해 실행되는 경우, 상기 모듈들은 상기 프로세서(320)가 상기 모듈과 연관된 동작(또는, 모듈이 제공 가능한 기능)을 수행하도록 야기할 수 있다. 따라서 이하에서 특정 모듈이 동작을 수행한다는 기재는, 특정 모듈이 실행됨에 따라서 프로세서(320)가 해당 동작을 수행하는 것으로 해석될 수 있다. 하나 또는 그 이상의 예에서, 상기 모듈들은 특정 어플리케이션의 일부로 구현될 수도 있다. 하나 또는 그 이상의 예에서, 기재 및/또는 도시된 바에 제한되지 않고, 각 모듈들은 프로세서(320)와는 별도의 하드웨어(예: 프로세서, 제어 회로)로 구현될 수도 있다.

[53] 메모리(330)는 제1 메모리(331), 제2 메모리(332), 제3 메모리(333), 및 제4 메모리(334)를 포함할 수 있다.

[54] 제1 메모리(331)(예: 도 1의 비휘발성 메모리(138)의 적어도 일부)는 비보안성 메모리로 비휘발성 메모리일 수 있다. 제1 메모리(332)는 REE(410)의 어플리케이션 계층(311)에서 작동하는 어플리케이션으로부터 출력되는 데이터를 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 제1 프로세서(321)에 의해 어플리케이션 계층(411)에서 어플리케이션이 실행되고, 제1 프로세서(321)는 어플리케이션 실행 중에 생성되는 데이터를 커널 계층(413)을 통해 제1 메모리(332)에 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 제1 프로세서(321)는 어플리케이션 실행 중에 요구되는 데이터를 커널 계층(413)을 통해 제1 메모리(331)로부터 독출할 수 있다.

[55] 제2 메모리(332)는 휘발성 메모리로서 REE(410)와 TEE(420)에 공유되는 공유 메모리일 수 있다. 제2 메모리(332)는 DRAM(dynamic random access memory)일 수 있다. 제2 메모리(332)는 제1 프로세서(321) 및 제2 프로세서(322)의 제어에 따라, 신뢰된 어플리케이션 계층(421)에서 작동하는 신뢰된 어플리케이션으로부터 출력되는 보안 데이터 중 적어도 일부를 임시 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 제2 프로세서(322)에 의해 신뢰된 어플리케이션 계층(421)에서 신뢰된 어플리케이션이 실행되고, 제2 프로세서(322)는 신뢰된 어플리케이션이 실행됨에 따라 데이터를 보안 OS 커널 계층(423)의 메일 박스를 통해 제1 프

로세서(321)로 요청하고, 제1 프로세서(321)는 현재 실행중인 데몬(demon)이 커널 계층(413)의 메일 박스를 통해 제2 프로세서(322)의 요청을 수신함에 따라, 데몬을 통해 제1 메모리(331)에 저장된 데이터를 읽어 들여서 제2 메모리(332)에 임시 저장할 수 있다. 제2 프로세서(322)는 보안 OS 커널 계층(423)을 통해 제2 메모리(332)에 임시 저장된 데이터를 읽어 들여서 신뢰된 어플리케이션 계층(421)에 전달할 수 있다. 하나 또는 그 이상의 실시 예에서, 제2 프로세서(322)에 의해 신뢰된 어플리케이션 계층(421)에서 신뢰된 어플리케이션이 실행되고, 제2 프로세서(322)는 신뢰된 어플리케이션이 실행됨에 따라 생성되는 보안 데이터를 제2 메모리(332)에 저장하고, 보안 OS 커널 계층(423)의 메일 박스를 통해 제1 프로세서(321)로 제2 메모리(332)에 임시 저장된 보안 데이터의 저장을 요청할 수 있다. 제1 프로세서(321)는 현재 실행중인 데몬(demon)이 커널 계층(413)의 메일 박스를 통해 제2 프로세서(322)의 요청을 수신함에 따라, 데몬을 통해 제2 메모리(332)에 임시 저장된 보안 데이터를 읽어들여서 제1 메모리(331)에 저장할 수 있다. 제2 프로세서(322)의 요청에는 보안 데이터가 저장된 제2 메모리(332)의 주소가 포함될 수 있다.

[56] 제3 메모리(333)는 휘발성 메모리(예: 도 1의 휘발성 메모리(132))일 수 있으며, 제1 메모리(331) 대비 저용량을 가질 수 있다. 제3 메모리(333)는 SRAM(static random access memory)일 수 있다. 제3 메모리(333)는 신뢰된 어플리케이션 계층(421)에서 작동하는 신뢰된 어플리케이션으로부터 출력되는 보안 데이터 중 적어도 일부를 임시 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 제2 프로세서(322)에 의해 신뢰된 어플리케이션 계층(421)에서 신뢰된 어플리케이션이 실행되고, 제2 프로세서(322)는 신뢰된 어플리케이션이 실행됨에 따라 생성되는 보안 데이터 중 적어도 일부를 보안 OS 커널 계층(423)을 통해 제3 메모리(333)에 임시 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 제2 프로세서(322)의 제어에 의해, 제3 메모리(333)에 저장된 데이터가 암호화 되어 제2 메모리(332)로 복사(예: swap out)될 수 있고, 제2 메모리(332)에 저장된 데이터가 복호화 되어 제3 메모리(333)로 복사(예: swap in)될 수 있다.

[57] 하나 또는 그 이상의 실시 예에서, 제4 메모리(334)(예: 도 1의 비휘발성 메모리(138)의 적어도 일부)는 비휘발성 메모리로 보안 메모리일 수 있다. 제4 메모리(334)는 신뢰된 어플리케이션 계층(421)에서 작동하는 신뢰된 어플리케이션으로부터 출력되는 보안 데이터 중 적어도 일부를 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 제2 프로세서(322)에 의해 신뢰된 어플리케이션 계층(421)에서 신뢰된 어플리케이션이 실행되고, 제2 프로세서(322)는 신뢰된 어플리케이션이 실행됨에 따라 생성되는 보안 데이터 중 적어도 일부를 보안 OS 커널 계층(423)을 통해 제4 메모리(334)에 저장할 수 있다. 제4 메모리(334)는 데이터의 독출, 수정 또는 삭제 기능이 드물게 수행되는 저장 공간일 수 있다. 전자 장치(101)는, 특정한 명령어 세트에 대하여서만 제4 메모리(334)에 접근을 허용하도록 설정될 수 있다. 예를 들어, 신뢰된 어플리케이션으로부터의 명령어에 따라, 제4 메

모리(334)의 데이터가 독출, 수정 또는 삭제될 수 있다. 아울러, 신뢰된 어플리케이션이 아닌 일반적인 어플리케이션으로부터의 명령어에 따라, 제4 메모리(334)의 데이터가 독출, 수정 또는 삭제되지 않을 수 있다. 하나 또는 그 이상의 실시예에 따르면, 보안 데이터를 암호화 하는 과정에서 사용되는 정보들이 제4 메모리(334)에 저장될 수 있다. 제4 메모리(334)에 저장된 정보들은 추후 암호화 된 보안 데이터를 복호화 하기 위해 사용될 수 있다. 이에 대하여서는 더욱 상세하게 후술하도록 한다.

[58] 하나 또는 그 이상의 실시 예에 따르면, 전자 장치(101)는, 서로 독립적으로 구현된 하드웨어들(예: 메모리들(331 내지 334) 및/또는 프로세서들(321, 322))에 기반하여 복수의 실행 환경들에서 동작(또는, 기능)을 수행하도록 구현될 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 서로 다른 권한과 관련된 서로 다른 하드웨어 조각이 복수의 실행 환경들(예: REE(410) 및 TEE(420)) 별로 할당될 수 있다. 예를 들어, 도 4를 참조하면, 점선을 기준으로 좌측에 위치되는 하드웨어 장치들은 REE(410)에 할당(또는, REE(410)에서 구동)되고, 우측에 위치되는 하드웨어 장치들은 TEE(420)에 할당(또는, TEE(420)에서 구동)될 수 있다. 예를 들어, 도 4를 참조하면, 복수의 실행 환경들(예: REE(410) 및 TEE(420)) 별로 서로 다른 메모리(331 내지 334)가 할당될 수 있다. 제1 프로세서(321)는, REE(410)에서 제1 운영 체제를 실행하여 적어도 하나의 동작을 수행하고, REE(410)에 할당된 제1 메모리(331)에 데이터를 읽고 쓸(write) 수 있다. 제2 프로세서(322)는, TEE(420)에서 REE(410)의 제1 운영 체제와는 별도의 독립된 제2 운영 체제를 실행하여 적어도 하나의 동작을 수행하고, TEE(420)에 할당된 제3 메모리(323) 및 제4 메모리(334)에 데이터를 읽고 쓸 수 있다. 하나 또는 그 이상의 실시 예에 따르면, TEE(420)에 대한 권한 및/또는 보안성은, REE(410)에 대한 권한 및/또는 보안성보다 더 높을 수 있다. 하나 또는 그 이상의 예에서, 제2 프로세서(322)는, TEE(420)에서 REE(410)에 할당된 제1 메모리(331)에 접근하여 데이터를 읽고 쓸 수 있으나, 제1 프로세서(321)는 REE(410)에서 TEE(420)에 할당된 제4 메모리(334)로의 접근이 제한될 수 있다. 예를 들어, 제1 프로세서(321)는 제4 메모리(334)에 데이터를 쓰거나 제4 메모리(334)에 저장된 데이터를 읽을 수 없을 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 제2 메모리(332)에 대하여, REE(410)와 TEE(420)의 접근이 허용될 수 있다. 예를 들어, 제1 프로세서(321)는, REE(410)에서 제2 메모리(332)에 데이터를 쓰거나 제2 메모리(332)에 저장된 데이터를 읽을 수 있다. 예를 들어, 제2 프로세서(322)는, TEE(420)에서 제2 메모리(332)에 데이터를 쓰거나 제2 메모리(332)에 저장된 데이터를 읽을 수 있다.

[59] 이하에서는 하나 또는 그 이상의 실시 예에 따른 전자 장치(101)의 동작의 예에 대해서 설명한다.

[60] 하나 또는 그 이상의 실시 예에 따르면 전자 장치(101)는 TEE(420)에서 신뢰된 어플리케이션의 실행에 의해 생성된 보안 데이터를 암호화 하여 제2 메모리(332)를 통해 REE(410)에 할당된 제1 메모리(331)에 파일 형태로 저장하고, 보안 데이

터를 암호화 및/또는 복호화 하는데 사용되는 정보들을 제4 메모리(334)에 저장할 수 있다. 하나 또는 그 이상의 실시 예에 따르면 전자 장치(101)는 TEE(420)에서 신뢰된 어플리케이션이 실행됨에 따라, REE(410)에서 현재 실행중인 데몬을 통해 REE(410)에 할당된 제1 메모리(331)에 파일 형태로 저장된 암호화 된 보안 데이터를 읽어 들여서 제2 메모리(332)에 복사하고, 제4 메모리(334)로부터 보안 데이터를 암호화 및/또는 복호화 하는데 사용되는 보안 정보들을 읽어 들이고, 보안 정보들을 이용하여 제2 메모리(332)에 복사된 암호화 된 보안 데이터를 복호화 하여 제3 메모리(333)에 임시 저장하고, 신뢰된 어플리케이션이 실행되는 동안 복호화된 보안 데이터를 사용할 수 있다.

[61] 도 5는 하나 또는 그 이상의 실시 예에 따른 전자 장치(101)의 동작의 일 예를 설명하기 위한 흐름도(500)이다. 당업자에 의해 이해되는 바와 같이, 도 5에 도시되는 동작들은 도시되는 순서에 국한되지 않고 다양한 순서로 수행될 수 있다. 또한, 하나 또는 그 이상의 실시 예에 따르면 도 5에 도시되는 동작들 보다 더 많은 동작들이 수행되거나, 더 적은 적어도 하나의 동작이 수행될 수도 있다. 이하에서는, 도 6을 참조하여 도 5에 대해서 설명한다.

[62] 하나 또는 그 이상의 실시 예에 따르면, 전자 장치(101)(예: 제2 프로세서(322))는 501 동작에서 TEE(420)의 신뢰된 어플리케이션 계층(421)에서 신뢰된 어플리케이션을 실행하여 보안 데이터를 생성할 수 있다. 예를 들어, 신뢰된 어플리케이션 중 iSIM이 실행되는 경우, 생성되는 데이터는 가입자 식별정보, 인증 키, 가입자 전화번호, 로컬 영역 ID, 개인 식별 번호(PIN), 및 서비스 공급자 정보 등 보안이 필요한 정보들 중 적어도 하나를 포함할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 보안 데이터는 실행되는 어플리케이션에 따라 다를 수 있으며, 해당 어플리케이션 개발자가 지정한 정보들이 포함될 수 있다. 전자 장치(101)(예: 제2 프로세서(322))는 신뢰된 어플리케이션의 실행으로 생성된 보안 데이터(예: 도 6의 631)를, 보안 OS 커널 계층(423)을 통해 제3 메모리(333)에 임시 저장될 수 있다.

[63] 전자 장치(101)(예: 제2 프로세서(322))는 503 동작에서 신뢰된 어플리케이션에서 사용중인 보안 데이터 또는 그것의 일부분을 암호화 하여(예: 도 6의 601) 보안 OS 커널 계층(423)을 통해 제2 메모리(332)에 복사(예: swap out)할 수 있다(예: 도 6의 621). 하나 또는 그 이상의 실시 예에서 데이터를 암호화 하는 방식으로 AES(advanced encryption standard)-GCM(galois/counter mode)가 사용될 수 있다. 암호화 방식은 이에 한정되지 않으며, 기밀성과 무결성이 보장되는 당업자에게 알려진 다른 암호화 방식이 사용될 수도 있다. 하나 또는 그 이상의 실시 예에서 데이터 암호화는 데이터를 소정 크기로 분할한 블록 단위로 수행될 수 있다. 데이터를 블록 단위로 암호화 할 때 롤백(rollback)을 방지하기 위한 기법이 사용될 수 있다. 당업자에 의해 이해되는 바와 같이, 암호화된 데이터의 롤백은 암호화된 데이터를 암호화되지 않은 데이터와 같은 이전 형태로 변경하는 것을 포함할 수 있다. 하나 또는 그 이상의 실시 예에 따르면 롤백 방지를 위해 ARC(anti-

replay counter)가 사용될 수 있다. 롤백 방지를 위해 데이터 블록 별로 서로 다른 ARC 값이 사용될 수 있다. 데이터 블록 별로 사용되는 서로 다른 ARC 값들은 테이블 형태로 제3 메모리(333)에 임시 저장될 수 있다. 하나 또는 그 이상의 실시 예에서 데이터 블록 별로 사용되는 서로 다른 ARC 값들은 테이블 형태로 제3 메모리(333)에 임시 저장될 수 있다(예: 도 6의 632). ARC 테이블은 ARC 값들로 구성된 선형 배열(linear array)일 수 있다. ARC 값들의 개수는 제2 메모리(332)로 복사(예: swap out)되는 보안 데이터의 크기에 따라 결정될 수 있다. 예를 들어 2MB의 보안 데이터를 암호화 하여 제2 메모리(332)로 복사(예: swap out)하기 위해서는 256개의 ARC 값이 사용될 수 있다. 각각의 ARC 값은 미리 정해진 초기값으로부터 1씩 증가될 수 있다. 하나 또는 그 이상의 실시 예에서 보안 데이터가 제2 메모리(332)로 복사(예: swap out)되거나 제2 메모리(332)로부터 복사(예: swap in)될 때, 해당 ARC 값은 보안 데이터의 암호화 또는 복호화 동작의 IV(initial vector)로서 사용될 수 있다. 하나 또는 그 이상의 실시 예에서 IV는 다음 식에 의해 계산될 수 있다.

[64] [수학식 1]

[65] IV = device specific value + ARC + zero padding

[66] 상기 식에서 device specific value는 전자 장치 고유의 값으로 4byte로 구성될 수 있다. ARC는 8byte로 구성될 수 있고, IV는 4byte의 제로 패딩(zero padding)을 포함하여 16byte로 구성될 수 있다.

[67] 전자 장치(101)(예: 제2 프로세서(322))는 데이터를 블록 단위로 암호화 하는 과정에서 생성되는 파라미터 값들을 암호화 하여 보안 OS 커널 계층(423)을 통해 제2 메모리(332)에 저장(예: swap out)할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, AES-GCM을 사용하여 데이터를 암호화 하는 과정에서 데이터 블록 별로 태그(TAG) (예: 도 6의 651)가 생성되며, 전자 장치(101)(예: 제2 프로세서(322))는 암호화 과정에서 생성된 태그들을 테이블 형태로 암호화 하여(예: 도 6의 603) 보안 OS 커널 계층(423)을 통해 제2 메모리(332)에 저장(예: swap out)할 수 있다(예: 도 6의 623). 하나 또는 그 이상의 실시 예에서 태그를 암호화 하는 방식으로 AES-ECB(electronic code block) 모드가 사용될 수 있다. 암호화 방식은 이에 한정되지 않으며, 기밀성이 보장되는 당업자에게 알려진 다른 암호화 방식이 사용될 수도 있다.

[68] 하나 또는 그 이상의 실시 예에서, 전자 장치(101)(예: 제2 프로세서(322))는 데이터 암호화 과정에서 생성되고 제3 메모리(333)에 저장된 정보들을 암호화 하여 보안 OS 커널 계층(423)을 통해 제2 메모리(332)에 복사(예: swap out)할 수 있다. 하나 또는 그 이상의 실시 예에서, 전자 장치(101)(예: 제2 프로세서(322))는 제3 메모리(333)에 저장된 ARC 테이블을 암호화 하여(예: 도 6의 605) 보안 OS 커널 계층(423)을 통해 제2 메모리(332)에 복사(예: swap out)할 수 있다(예: 도 6의 622). 하나 또는 그 이상의 실시 예에서 ARC 테이블을 암호화 하는 방식으로 AES-GCM가 사용될 수 있다. 암호화 방식은 이에 한정되지 않으며, 기밀성과 무

결성이 보장되는 당업자에게 알려진 다른 암호화 방식이 사용될 수도 있다. 하나 또는 그 이상의 실시 예에서, 전자 장치(101)(예: 제2 프로세서(322))는 암호화 과정에서 생성되는 정보들을 암호화 할 때 사용되고 생성되는 파라미터들을 보안 OS 커널(423)을 통해 제4 메모리(334)에 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 전자 장치(101)(예: 제2 프로세서(322))는 ARC 테이블을 암호화 할 때, IV(initial vector)로서 마스터 ARC를 사용할 수 있다. 마스터 ARC는 신뢰된 어플리케이션으로부터 생성된 보안 데이터를 저장할 때마다 랜덤 값으로 생성될 수 있다. 하나 또는 그 이상의 실시 예에서, 마스터 ARC는 암호화 된 ARC 테이블을 복호화 할 때 사용될 수 있다. 예를 들어, 전자 장치(101)(예: 제2 프로세서(322))는 보안 OS 커널 계층(423)을 통해 마스터 ARC를 제4 메모리(334)에 저장할 수 있다(예: 도 6의 641). 하나 또는 그 이상의 실시 예에서 ARC 테이블을 암호화 하는 과정에서 마스터 태그가 생성될 수 있다. 마스터 태그는 암호화 된 ARC 테이블을 복호화 할 때 사용될 수 있다. 예를 들어, 전자 장치(101)(예: 제2 프로세서(322))는 보안 OS 커널 계층(423)을 통해 마스터 태그를 제4 메모리(334)에 저장할 수 있다(예: 도 6의 642).

[69] 동작 505 에서, 전자 장치(101)(예: 제1 프로세서(321))는 제2 메모리(332)에 저장된 암호화 된 데이터들을 REE(410)에 할당된 제1 메모리(331)에 저장할 수 있다. 하나 또는 그 이상의 실시 예에서, 전자 장치(101)의 제2 프로세서(322)는 보안 OS 커널 계층(423)의 메일 박스를 통해 제1 프로세서(321)로 보안 데이터를 REE(410)에 할당된 제1 메모리(331)에 저장하도록 요청할 수 있다. 전자 장치(101)의 제1 프로세서(321)는 REE(410)에서 데몬을 실행 중인 상태에서 커널 계층(413)의 메일 박스를 통해 제2 프로세서(322)로부터 보안 데이터의 요청을 수신할 수 있다. 하나 또는 그 이상의 실시 예에서 제2 프로세서(322)에서 제1 프로세서(321)로 전달되는 요청에는 보안 데이터가 저장된 제2 메모리(332)의 주소가 포함될 수 있다. 전자 장치(101)의 제1 프로세서(321)는 REE(410)에서 실행 중인 데몬을 통해서 제2 메모리(332)에 저장된 암호화 된 데이터들을 읽어 들이고, 커널 계층(413)을 통해 읽어 들인 암호화 된 데이터들을 제1 메모리(331)에 저장할 수 있다(예: 도 6의 607). 하나 또는 그 이상의 실시 예에서, 제2 메모리(332)에 저장된 암호화 된 데이터들은 암호화 된 보안 데이터(예: 도 6의 611), 암호화 된 ARC 테이블(예: 도 6의 612), 및 암호화 된 태그 테이블(예: 도 6의 613)을 포함할 수 있고, 암호화 된 데이터들은 하나의 파일 형태로 제1 메모리(331)에 저장될 수 있다(예: 도 6의 610).

[70] 도 7은 하나 또는 그 이상의 실시 예에 따른 전자 장치(101)의 동작의 일 예를 설명하기 위한 흐름도(700)이다. 당업자가 이해하는 바와 같이, 도 7에 도시되는 동작들은 도시되는 순서에 국한되지 않고 다양한 순서로 수행될 수 있다. 또한, 하나 또는 그 이상의 실시 예에 따르면 도 7에 도시되는 동작들 보다 더 많은 동작들이 수행되거나, 더 적은 적어도 하나의 동작이 수행될 수도 있다. 이하에서는, 도 8을 참조하여 도 7에 대해서 설명한다.

[71] 하나 또는 그 이상의 실시 예에 따르면, 전자 장치(101)(예: 제2 프로세서(322))는 701 동작에서 TEE(420)의 신뢰된 어플리케이션 계층(421)에서 신뢰된 어플리케이션을 실행할 수 있다. 하나 또는 그 이상의 실시 예에서, 신뢰된 어플리케이션이 실행됨에 따라, 제2 프로세서(322)는 보안 OS 커널(423)의 메일 박스를 통해 제1 프로세서(321)로 제1 메모리(331)에 저장된 보안 데이터를 요청할 수 있다.

[72] 전자 장치(101)(예: 제1 프로세서(321))는 703 동작에서 제1 메모리(331)에 저장된 암호화 된 데이터 파일(예: 도 8의 610)을 독출할 수 있다(예: 도 8의 801). 하나 또는 그 이상의 실시 예에서, 제1 프로세서(321)는 커널 계층(413)의 메일 박스를 통해 제2 프로세서(322)로부터의 보안 데이터 요청을 수신하면, REE(410)에서 실행중인 데몬(daemon)을 통해서 제2 메모리(332)에 저장된 암호화 된 데이터 파일(예: 도 8의 610)을 독출할 수 있다(예: 도 8의 801). 하나 또는 그 이상의 실시 예에 따르면, 보안 데이터의 암호화 방식으로 AES-GCM이 사용되고 롤백 방지를 위해 ARC가 사용된 경우, 제1 메모리(331)에는 암호화 된 데이터(예: 도 8의 611), 암호화 된 ARC 테이블(예: 도 8의 612), 및 암호화 된 태그 테이블(예: 도 8의 613)이 저장되어 있을 수 있다. 이 경우, 전자 장치(101)(예: 제1 프로세서(321))는 제1 메모리(331)로부터 독출한 파일에 포함된 암호화 된 데이터(예: 도 8의 611), 암호화 된 ARC 테이블(예: 도 8의 612), 및 암호화 된 태그 테이블(예: 도 8의 613)을 제2 메모리(332)에 복사할 수 있다. 하나 또는 그 이상의 실시 예에서, 제1 프로세서(321)는 REE(410)에서 실행중인 데몬을 통해서 제1 메모리(331)로부터 독출한 파일에 포함된 암호화 된 데이터(예: 도 8의 611), 암호화 된 ARC 테이블(예: 도 8의 612), 및 암호화 된 태그 테이블(예: 도 8의 613)을 제2 메모리(332)에 복사할 수 있다.

[73] 전자 장치(101)(예: 제2 프로세서(322))는 705 동작에서 제2 메모리(332)에 복사된 암호화 된 데이터(예: 도 8의 611)를 신뢰된 어플리케이션에서 사용하기 위하여 복호화 할 수 있다. 하나 또는 그 이상의 실시 예에서, 전자 장치(101)(예: 제2 프로세서(322))는 암호화 된 데이터(예: 도 6의 411)암호화 된 ARC 테이블(예: 도 8의 612), 및 암호화 된 태그 테이블(예: 도 8의 613)을 각각 복호화 할 수 있다. 하나 또는 그 이상의 실시 예에서 전자 장치(101)(예: 제2 프로세서(322))는 암호화 과정에서 생성된 암호화 데이터들을 제4 메모리(334)에 저장된 암호화 정보들을 이용하여 검증하고 복호화 할 수 있다. 하나 또는 그 이상의 실시 예에서 전자 장치(101)(예: 제2 프로세서(322))는 암호화 된 ARC 테이블(예: 도 8의 622)을 복호화(예: 도 8의 803)할 수 있다. 하나 또는 그 이상의 실시 예에서, 보안 데이터를 암호화 하는 과정에서 ARC 테이블이 AES-GCM으로 암호화 된 경우, 제4 메모리(334)에는 암호화 과정에서 생성되고 사용된 마스터 ARC(예: 도 8의 641)와 마스터 태그(예: 도 8의 642)가 저장되어 있다. 하나 또는 그 이상의 실시 예에서 제2 프로세서(322)는 보안 OS 커널 계층(423)을 통해 제4 메모리(334)에 저장된 마스터 ARC(예: 도 8의 641)와 마스터 태그(예: 도 8의 642)를 읽어들이고, 마스터 ARC(예: 도 8의 641)와 마스터 태그(예: 도 8의 642)를 이용하여 제2 메모리(332)

에 저장된, 암호화 된 ARC 테이블(예: 도 8의 622)을 복호화(예: 도 8의 803)할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 마스터 태그는 암호화 된 ARC 테이블의 검증을 위해 사용될 수 있다. 전자 장치(101)(예: 제2 프로세서(322))는 복호화 된 ARC 테이블은 보안 OS 커널 계층(423)을 통해 제3 메모리(333)에 저장(swap in)할 수 있다(예: 도 8의 632).

[74] 전자 장치(101)(예: 제2 프로세서(322))는 복호화 된 정보들을 이용하여 암호화 된 보안 데이터를 복호화 할 수 있다. 하나 또는 그 이상의 실시 예에서 전자 장치(101)(예: 제2 프로세서(322))는 복호화 된 ARC 테이블(예: 도 8의 632)의 ARC 값들과 제2 메모리(332)에 복사된 복호화 된 태그 테이블(예: 도 8의 623)의 태그 값들을 이용하여, 제2 메모리(332)에 복사된 암호화 된 보안 데이터(예: 도 8의 621)를 블록 단위로 복호화 할 수 있다(예: 도 8의 805). 예를 들어, 데이터는 하나 이상의 블록으로 분할될 수 있으며, 여기서 데이터는 블록 단위로 암호화되고, 이후 블록 단위로 복호화된다.

[75] 하나 또는 그 이상의 실시 예에서, 전자 장치(101)(예: 제2 프로세서(322))는 복호화 된 보안 데이터를 보안 OS 커널 계층(423)을 통해 제3 메모리(333)에 저장(예: swap in)할 수 있다(예: 도 8의 631). 이후 전자 장치(101)(예: 제2 프로세서(322))는 TEE(420)의 신뢰된 어플리케이션 계층(421)에서 실행 중인 신뢰된 어플리케이션을 통해 제3 메모리(333)에 저장된 복호화 된 보안 데이터를 사용할 수 있다.

[76] 도 9는 하나 또는 그 이상의 실시 예에 따른 전자 장치(101)의 제4 메모리(334)에 저장되는 보안 데이터의 포맷의 일 예를 설명하기 위한 도면이다.

[77] 하나 또는 그 이상의 실시 예에서 제4 메모리(334)에는 신뢰된 어플리케이션 계층(421)에서 작동하는 신뢰된 어플리케이션으로부터 출력되는 보안 데이터 중 적어도 일부가 저장될 수 있다. 하나 또는 그 이상의 실시 예에서, 제2 프로세서(322)에 의해 신뢰된 어플리케이션 계층(421)에서 신뢰된 어플리케이션이 실행되고, 제2 프로세서(322)는 신뢰된 어플리케이션이 실행됨에 따라 생성되는 보안 데이터 중 적어도 일부를 보안 OS 커널 계층(423)을 통해 제4 메모리(334)에 저장할 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 제4 메모리(334)에는 보안 데이터를 암호화 하는 과정에서 사용되는 정보들이 제4 메모리(334)에 저장될 수 있다.

[78] 도 9를 참조하면, 신뢰된 어플리케이션 1번(SA#1)의 실행에 의해 생성된 데이터(910)가 제4 메모리(334)의 슬롯 A(slot A)(920)에 저장될 수 있다. 하나 또는 그 이상의 실시 예에 따르면, 제2 프로세서(322)가 ARC 테이블을 암호화 할 때 IV(initial vector)로서 사용되는 마스터 ARC 필드(915)와, ARC 테이블을 암호화 하는 과정에서 생성된 마스터 태그 필드(916)를 포함하는 데이터가 제4 메모리(334)에 저장될 수 있다. 제4 메모리(334)에 저장되는 데이터는, 마스터 ARC 필드(915)와 마스터 태그 필드(916) 외에도 매직(magic) 필드(911), 버전(version) 필드

(912), 액티브 셋(active set) 필드(913), 데이터 사이즈 필드(914), 및 Reserved 필드(917)를 더 포함할 수 있다.

[79] 매직(magic) 필드(911)는 4byte로 이루어질 수 있으며, 명령을 확인하기 위해 사용되는 정수일 수 있다. 버전(version) 필드(912)는 4byte로 이루어질 수 있으며, 해당 데이터의 버전 정보를 나타내는 값일 수 있다. 액티브 셋(active set) 필드(913)는 4byte로 이루어질 수 있으며, 올바른 정보가 저장된 셋을 나타내는 플래그 값일 수 있다. 데이터 사이즈 필드(914)는 4byte로 이루어질 수 있으며, 해당되는 신뢰된 어플리케이션에 의해 생성된 보안 데이터의 사이즈를 나타내는 값일 수 있다. 마스터 ARC 필드(915)는 8byte로 이루어질 수 있으며, 마스터 ARC는 신뢰된 어플리케이션으로부터 생성된 보안 데이터를 저장할 때마다 생성된 랜덤 값일 수 있다. 마스터 ARC는 ARC 테이블을 암호화 하거나 암호화 된 ARC 테이블을 복호화 할 때 IV(initial vector)로 사용될 수 있다. 마스터 태그 필드(916)는 16byte로 이루어질 수 있으며, 마스터 태그는 ARC 테이블이 암호화 되어 제2 메모리(332)로 복사(예: swap out)될 때 암호화 동작의 결과로 생성되는 인증태그일 수 있다. 마스터 태그는 암호화 된 ARC 테이블을 복호화 할 때 인증태그로 사용될 수 있다.

[80] 하나 또는 그 이상의 실시 예에 따른 전자 장치는, 일반 환경(410)에서 동작하는 제1 프로세서(321); 보안 환경(420)에서 동작하는 제2 프로세서(322); 상기 일반 환경에 할당된 제1 메모리(331); 상기 보안 환경에 할당된 제2 메모리(334); 및 상기 일반 환경과 상기 보안 환경에서 공유되는 제3 메모리(332)를 포함할 수 있다. 상기 제2 프로세서는, 상기 보안 환경에서 실행되는 신뢰된 어플리케이션에 의해 생성된 보안 데이터 중 적어도 일부를 암호화 하여 상기 제3 메모리에 저장하고, 상기 보안 데이터 중 적어도 일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를 상기 제2 메모리에 저장하도록 설정될 수 있다. 상기 제1 프로세서는, 상기 제3 메모리에 저장된, 상기 암호화 된 적어도 일부의 보안 데이터를 상기 제1 메모리에 저장하도록 설정될 수 있다.

[81] 하나 또는 그 이상의 실시 예에서, 상기 제2 프로세서는, 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하되, 상기 블록 별로 서로 다른 ARC(anti-replay counter) 값들을 사용하여 암호화 하고, 상기 ARC 값들이 저장된 ARC 테이블(432)을 암호화 하며, 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하는 과정에서 생성되는 태그값들(651)이 저장된 태그 테이블을 암호화 하도록 설정될 수 있다.

[82] 하나 또는 그 이상의 실시 예에서, 상기 제1 프로세서는, 상기 암호화 된 적어도 일부의 보안 데이터(611), 상기 암호화 된 ARC 테이블(612), 및 상기 암호화 된 태그 테이블(613)을 파일 형태(610)로 상기 제1 메모리에 저장하도록 설정될 수 있다.

[83] 하나 또는 그 이상의 실시 예에서, 상기 제1 정보는 마스터 ARC(641)이고, 상기 제2 정보는 마스터 태그(642)일 수 있다.

[84] 하나 또는 그 이상의 실시 예에서, 상기 제1 프로세서는, 상기 보안 환경에서 상기 신뢰된 어플리케이션이 실행됨에 따라, 상기 제1 메모리에 저장된 상기 암호화 된 적어도 일부의 보안 데이터를 복사하여 상기 제3 메모리에 저장하며, 상기 제2 프로세서는, 상기 제1 정보 및 상기 제2 정보를 이용하여, 상기 제3 메모리에 저장된 상기 암호화 된 적어도 일부의 보안 데이터를 복호화 하도록 설정될 수 있다.

[85] 하나 또는 그 이상의 실시 예에서, 상기 제3 메모리에 저장된 암호화 된 적어도 일부의 보안 데이터는, 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하는 과정에서 사용된 ARC(anti-replay counter)값들이 저장된 암호화 된 ARC 테이블(622), 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하는 과정에서 생성된 태그 값들이 저장된 암호화 된 태그 테이블(623)을 포함하며, 상기 제2 프로세서는, 상기 제1 정보 및 상기 제2 정보를 이용하여 상기 암호화 된 ARC 테이블을 복호화 하고, 상기 태그 테이블을 복호화 하고, 상기 복호화 된 ARC 테이블 및 상기 복호화 된 태그 테이블을 이용하여 상기 블록 단위로 암호화 된 상기 적어도 일부의 보안 데이터를 복호화 하도록 설정될 수 있다.

[86] 하나 또는 그 이상의 실시 예에서, 상기 제1 프로세서는, 상기 제1 메모리로부터 상기 암호화 된 보안 데이터, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 포함하는 파일(610)을 독출하고, 상기 암호화 된 보안 데이터, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 각각 분리하여 상기 제3 메모리에 저장하도록 설정될 수 있다.

[87] 하나 또는 그 이상의 실시 예에서, 상기 제2 프로세서는, 상기 보안 데이터 중 적어도 일부와, 상기 ARC 테이블을 암호화 할 때, AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 암호화 하도록 설정될 수 있다.

[88] 하나 또는 그 이상의 실시 예에서, 상기 제2 프로세서는, 상기 암호화 된 보안 데이터 중 적어도 일부를 AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 복호화 하도록 설정될 수 있다.

[89] 하나 또는 그 이상의 실시 예에서, 상기 제2 프로세서는, 상기 태그 테이블을 암호화 할 때, AES(advanced encryption standard)- ECB(electronic code block) 방식으로 암호화 하도록 설정될 수 있다.

[90] 하나 또는 그 이상의 실시 예에 따른 전자 장치의 동작 방법은, 보안 환경(420)에서 동작하는 제1 프로세서(322)에 의해, 상기 보안 환경에서 신뢰된 어플리케이션을 실행하고 보안 데이터를 생성하는 동작(501)을 포함할 수 있다. 상기 방법은, 상기 제1 프로세서에 의해, 상기 생성된 보안 데이터 중 적어도 일부를 암호화 하고, 상기 보안 환경과 일반 환경(410)에서 공유되는 제1 메모리(332)에 저장하는 동작(503)을 포함할 수 있다. 상기 방법은, 상기 제1 프로세서에 의해, 상기 보안 데이터 중 적어도 일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보

안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를, 상기 보안 영역에 할당된 제2 메모리(334)에 저장하는 동작(503)을 포함할 수 있다. 상기 방법은, 상기 일반 환경에서 동작하는 제2 프로세서(321)에 의해, 상기 제1 메모리에 저장된, 상기 암호화 된 적어도 일부의 보안 데이터를 상기 일반 환경에 할당된 제3 메모리(331)에 저장하는 동작(505)을 포함할 수 있다.

[91] 하나 또는 그 이상의 실시 예에서, 상기 암호화 하는 동작(503)은, 상기 제1 프로세서에 의해, 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하되, 상기 블록 별로 서로 다른 ARC(anti-replay counter) 값들을 사용하여 암호화 하는 동작(601), 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하는 과정에서 생성되는 태그값들이 저장된 태그 테이블을 암호화 하는 동작(603), 및 상기 ARC 값들이 저장된 ARC 테이블을 암호화 하는 동작(605)을 포함할 수 있다.

[92] 하나 또는 그 이상의 실시 예에서, 상기 제3 메모리에 저장하는 동작(505)은, 상기 제2 프로세서에 의해, 상기 암호화 된 적어도 일부의 보안 데이터, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 파일 형태(610)로 상기 제1 메모리에 저장(607)하는 동작을 포함할 수 있다.

[93] 하나 또는 그 이상의 실시 예에서, 상기 제1 정보는 마스터 ARC(641)이고, 상기 제2 정보는 마스터 태그(642)일 수 있다.

[94] 하나 또는 그 이상의 실시 예에서, 상기 보안 환경에서 상기 신뢰된 어플리케이션이 실행됨에 따라(701), 상기 제2 프로세서에 의해, 상기 제1 메모리에 저장된 상기 암호화 된 적어도 일부의 보안 데이터를 복사하여 상기 제1 메모리에 저장하는 동작(703), 상기 제1 프로세서에 의해, 상기 제1 정보 및 상기 제2 정보를 이용하여, 상기 제1 메모리에 저장된 상기 암호화 된 적어도 일부의 보안 데이터를 복호화 하는 동작(705)을 더 포함할 수 있다.

[95] 하나 또는 그 이상의 실시 예에서, 상기 제1 메모리에 저장된 암호화 된 적어도 일부의 보안 데이터는, 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하는 과정에서 사용된 ARC(anti-replay counter)값들이 저장된 암호화 된 ARC 테이블(621), 상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하는 과정에서 생성된 태그 값들이 저장된 암호화 된 태그 테이블(623)을 포함하며, 상기 복호화 하는 동작(705)은, 상기 제1 프로세서에 의해, 상기 제1 정보 및 상기 제2 정보를 이용하여 상기 암호화 된 ARC 테이블을 복호화 하는 동작(803), 상기 태그 테이블을 복호화 하는 동작(805), 및 상기 복호화 된 ARC 테이블 및 상기 복호화 된 태그 테이블을 이용하여 상기 블록 단위로 암호화 된 상기 적어도 일부의 보안 데이터를 복호화 하는 동작(805)을 포함할 수 있다.

[96] 하나 또는 그 이상의 실시 예에서, 상기 제2 프로세서에 의해, 상기 제3 메모리로부터 상기 암호화 된 보안 데이터, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 포함하는 파일(610)을 독출하고(801), 상기 암호화 된 보안 데이터(621), 상기 암호화 된 ARC 테이블(622), 및 상기 암호화 된 태그 테이블(623)을 각각 분리하여 상기 제1 메모리에 저장하는 동작을 더 포함할 수 있다.

[97] 하나 또는 그 이상의 실시 예에서, 상기 암호화 하는 동작(601,605)은, 상기 보안 데이터 중 적어도 일부와, 상기 ARC 테이블을 암호화 할 때, AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 암호화 할 수 있다.

[98] 하나 또는 그 이상의 실시 예에서, 상기 복호화 하는 동작(705)은, 상기 암호화 된 보안 데이터 중 적어도 일부를 AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 복호화 할 수 있다.

[99] 하나 또는 그 이상의 실시 예에서, 상기 태그 테이블을 암호화 하는 동작(603)은, AES(advanced encryption standard)- ECB(electronic code block) 방식으로 암호화 할 수 있다.

[100] 본 문서에 개시된 하나 또는 그 이상의 실시 예에 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 하나 또는 그 이상의 실시 예에 따른 전자 장치는 전술한 기기들에 한정되지 않는다.

[101] 본 문서의 일 실시 예 및 이에 사용된 용어들은 본 문서에 기재된 기술적 특징들을 특정한 실시 예들로 한정하려는 것이 아니며, 해당 실시 예의 다양한 변경, 균등물, 또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 또는 관련된 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 아이템에 대응하는 명사의 단수 형은 관련된 문맥상 명백하게 다르게 지시하지 않는 한, 상기 아이템 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. "제 1", "제 2", 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: 제 1) 구성요소가 다른(예: 제 2) 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 제 3 구성요소를 통하여 연결될 수 있다는 것을 의미한다.

[102] 본 문서의 일 실시 예에서 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, 하나 또는 그 이상의 실시 예에 따르면, 모듈은 ASIC(application-specific integrated circuit)의 형태로 구현될 수 있다.

[103] 본 문서의 하나 또는 그 이상의 실시 예는 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 명령을 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.

[104] 하나 또는 그 이상의 실시 예에 따르면, 본 문서에 개시된 하나 또는 그 이상의 실시 예에 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 스토어TM)를 통해 또는 두 개의 사용자 장치들(예: 스마트 폰들) 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.

[105] 하나 또는 그 이상의 실시 예에 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. 하나 또는 그 이상의 실시 예에 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. 일 실시 예에 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 장치(101)에 있어서,
일반 비보안 환경(410)에서 동작하는 제1 프로세서(321);
보안 환경(420)에서 동작하는 제2 프로세서(322);
상기 일반 비보안 환경에 할당된 제1 메모리(331);
상기 보안 환경에 할당된 제2 메모리(334); 및
상기 일반 비보안 환경과 상기 보안 환경에서 공유되는 제3 메모리(332)를 포함하며,
상기 제2 프로세서는,
암호화 된 부분을 생성하기 위해 보안 데이터 중 적어도 일부를 암호화 하고, 상기 보안 데이터는 상기 보안 환경에서 실행되는 신뢰된 어플리케이션에 의해 생성되고,
상기 암호화 된 부분을 상기 제3 메모리에 저장하고,
상기 보안 데이터 중 적어도 일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를 상기 제2 메모리에 저장하고,
상기 제1 프로세서는,
상기 제3 메모리에 저장된, 상기 암호화 된 부분을 상기 제1 메모리에 저장하도록 설정된 전자 장치.

[청구항 2] 제1항에 있어서,
상기 제2 프로세서는,
상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하되, 상기 블록 별로 서로 다른 ARC(anti-replay counter) 값들을 사용하여 암호화 하고,
상기 블록 별로 상기 ARC 값들이 저장된 ARC 테이블(432)을 암호화 하며,
상기 적어도 일부의 보안 데이터를 상기 블록 단위로 암호화 하는 과정에서 생성되는 태그값들(651)이 저장된 태그 테이블을 암호화 하도록 설정되는 것을 특징으로 하는 전자 장치.

[청구항 3] 제2항에 있어서,
상기 제1 프로세서는,
상기 암호화 된 적어도 일부의 보안 데이터(611), 상기 암호화 된 ARC 테이블(612), 및 상기 암호화 된 태그 테이블(613)을 파일 형태(610)로 상기 제1 메모리에 저장하도록 설정되는 것을 특징으로 하는 전자 장치.

[청구항 4] 제2항 또는 제3항에 있어서,
상기 제1 정보는 마스터 ARC(641)이고, 상기 제2 정보는 마스터 태그(642)임을 특징으로 하는 전자 장치.

[청구항 5] 제1항 내지 제4항 중 어느 한 항에 있어서,

상기 제1 프로세서는,
상기 보안 환경에서 상기 신뢰된 어플리케이션이 실행됨에 따라, 상기 제1 메모리에 저장된 상기 암호화 된 부분을 복사된 부분으로서 복사하고,
상기 복사된 부분을 상기 제3 메모리에 저장하며,
상기 제2 프로세서는,
상기 제1 정보 및 상기 제2 정보를 이용하여, 상기 제3 메모리에 저장된 상기 암호화 된 부분을 복호화 하도록 설정되는 전자 장치.

[청구항 6] 제5항에 있어서,
상기 제3 메모리에 저장된 상기 암호화 된 부분은,
상기 적어도 일부의 보안 데이터를 상기 블록 단위로 암호화 하는 과정에서 사용된 ARC(anti-replay counter)값들이 저장된 암호화 된 ARC 테이블(622), 상기 적어도 일부의 보안 데이터를 상기 블록 단위로 암호화 하는 과정에서 생성된 태그 값들이 저장된 암호화 된 태그 테이블(623)을 포함하며,
상기 제2 프로세서는,
상기 제1 정보 및 상기 제2 정보를 이용하여 상기 암호화 된 ARC 테이블을 복호화 하고,
상기 암호화 된 태그 테이블을 복호화 하고,
상기 복호화 된 ARC 테이블 및 상기 복호화 된 태그 테이블을 이용하여 상기 암호화 된 부분을 복호화 하도록 설정되는 전자 장치.

[청구항 7] 제5항 또는 제6항에 있어서,
상기 제1 프로세서는,
상기 제1 메모리로부터 상기 암호화 된 부분, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 포함하는 파일(610)을 독출하고, 상기 암호화 된 부분, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 각각 상기 제3 메모리에 저장하도록 설정된 전자 장치.

[청구항 8] 제2항 내지 제7항 중 어느 한 항에 있어서,
상기 제2 프로세서는,
상기 보안 데이터 중 적어도 일부와, 상기 ARC 테이블을 암호화 할 때, AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 암호화 하도록 설정된 전자 장치.

[청구항 9] 제5항 내지 제8항 중 어느 한 항에 있어서,
상기 제2 프로세서는,
상기 암호화 된 부분을 AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 복호화 하도록 설정된 전자 장치.

[청구항 10] 제2항 내지 제9항 중 어느 한 항에 있어서,
상기 제2 프로세서는,

상기 태그 테이블을 암호화 할 때, AES(advanced encryption standard)-ECB(electronic code block) 방식으로 암호화 하도록 설정된 전자 장치.

[청구항 11] 전자 장치(101)의 동작 방법에 있어서,

보안 환경(420)에서 동작하는 제1 프로세서(322)에 의해, 상기 보안 환경에서 신뢰된 어플리케이션을 실행하고 보안 데이터를 생성하는 동작(501),

상기 제1 프로세서에 의해, 암호화 된 부분을 생성하기 위해 상기 생성된 보안 데이터 중 적어도 일부를 암호화 하고, 상기 암호화된 부분을 상기 보안 환경과 일반 비보안 환경(410)에서 공유되는 제1 메모리(332)에 저장하는 동작(503),

상기 제1 프로세서에 의해, 상기 보안 데이터 중 적어도 일부를 암호화 하기 위하여 사용되는 제1 정보 및 상기 보안 데이터 중 적어도 일부를 암호화 하는 과정에서 생성되는 제2 정보를, 상기 보안 환경에 할당된 제2 메모리(334)에 저장하는 동작(503), 및

상기 일반 비보안 환경에서 동작하는 제2 프로세서(321)에 의해, 상기 제1 메모리에 저장된, 상기 암호화 된 부분을 상기 일반 비보안 환경에 할당된 제3 메모리(331)에 저장하는 동작(505)을 포함하는 방법.

[청구항 12] 제11항에 있어서,

상기 제1 프로세서에 의해 상기 암호화 하는 동작(503)은,

상기 적어도 일부의 보안 데이터를 블록 단위로 암호화 하되, 상기 블록 별로 서로 다른 ARC(anti-replay counter) 값들을 사용하여 암호화 하는 동작(601),

상기 적어도 일부의 보안 데이터를 상기 블록 단위로 암호화 하는 과정에서 생성되는 태그값들이 저장된 태그 테이블을 암호화 하는 동작(603), 및

상기 블록 별로 상기 ARC 값들이 저장된 ARC 테이블을 암호화 하는 동작(605)을 포함하고,

상기 제2 프로세서에 의해 상기 제3 메모리에 저장하는 동작(505)은,

상기 암호화 된 부분, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 파일 형태(610)로 상기 제1 메모리에 저장(607)하는 동작을 포함하고,

상기 제1 정보는 마스터 ARC(641)이고, 상기 제2 정보는 마스터 태그(642)임을 특징으로 하는 방법.

[청구항 13] 제11항 또는 제12항에 있어서,

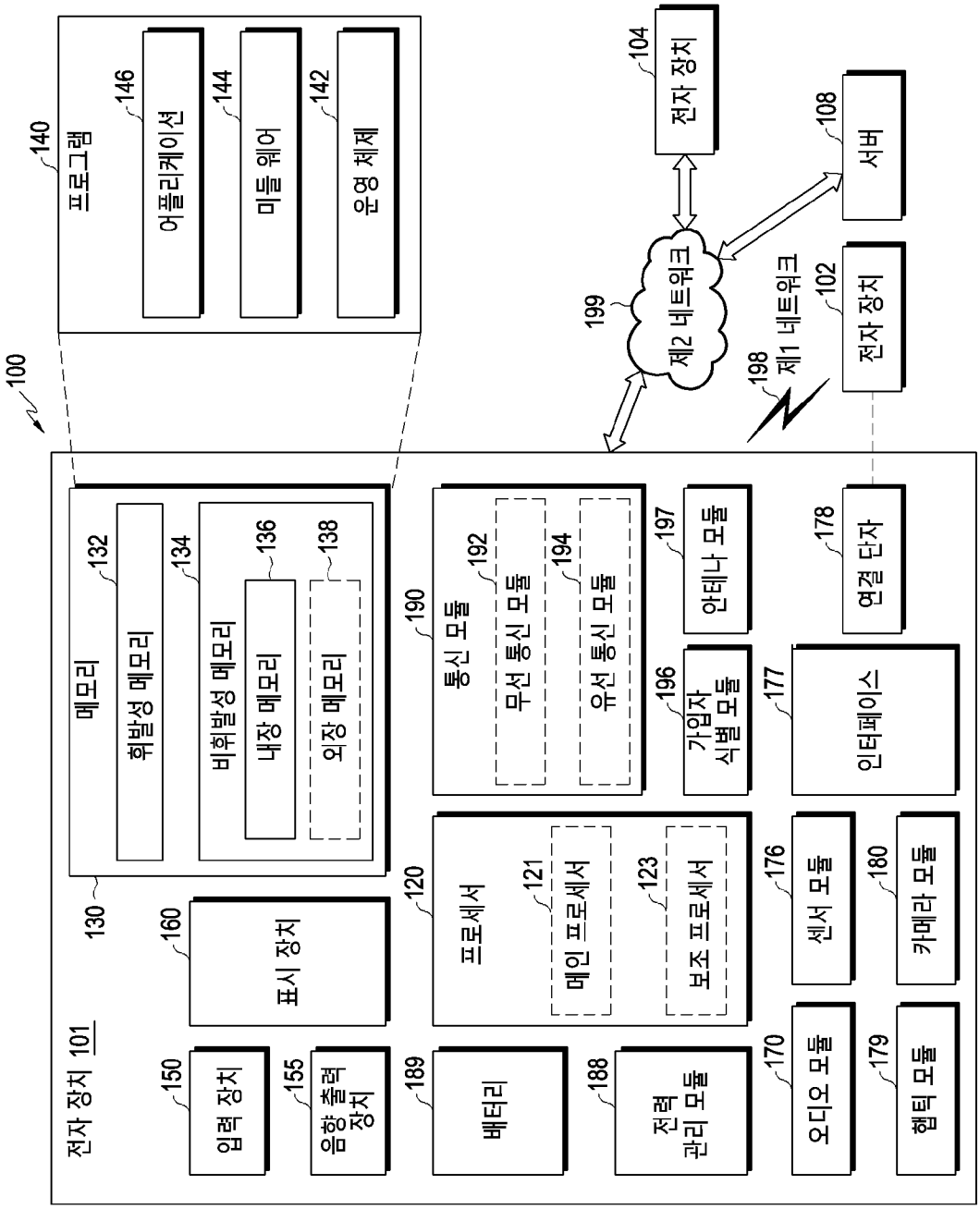
상기 보안 환경에서 상기 신뢰된 어플리케이션이 실행됨에 따라(701), 상기 제2 프로세서에 의해, 상기 제1 메모리에 저장된 상기 암호화 된 부분을 복사하고, 상기 복사된 부분을 상기 제1 메모리에 저장하는 동작(703),

상기 제1 프로세서에 의해, 상기 제1 정보 및 상기 제2 정보를 이용하여, 상기 제1 메모리에 저장된 상기 암호화 된 부분을 복호화 하는 동작(705)을 더 포함하고,
상기 제1 메모리에 저장된 암호화 된 부분은,
상기 적어도 일부의 보안 데이터를 상기 블록 단위로 암호화 하는 과정에서 사용된 ARC(anti-replay counter)값들이 저장된 암호화 된 ARC 테이블(621), 상기 적어도 일부의 보안 데이터를 상기 블록 단위로 암호화 하는 과정에서 생성된 태그 값들이 저장된 암호화 된 태그 테이블(623)을 포함하며,
상기 제1 프로세서에 의해 상기 복호화 하는 동작(705)은,
상기 제1 정보 및 상기 제2 정보를 이용하여 상기 암호화 된 ARC 테이블을 복호화 하는 동작(803),
상기 태그 테이블을 복호화 하는 동작(805), 및
상기 복호화 된 ARC 테이블 및 상기 복호화 된 태그 테이블을 이용하여 상기 암호화 된 부분을 복호화 하는 동작(805)을 포함하는 방법.

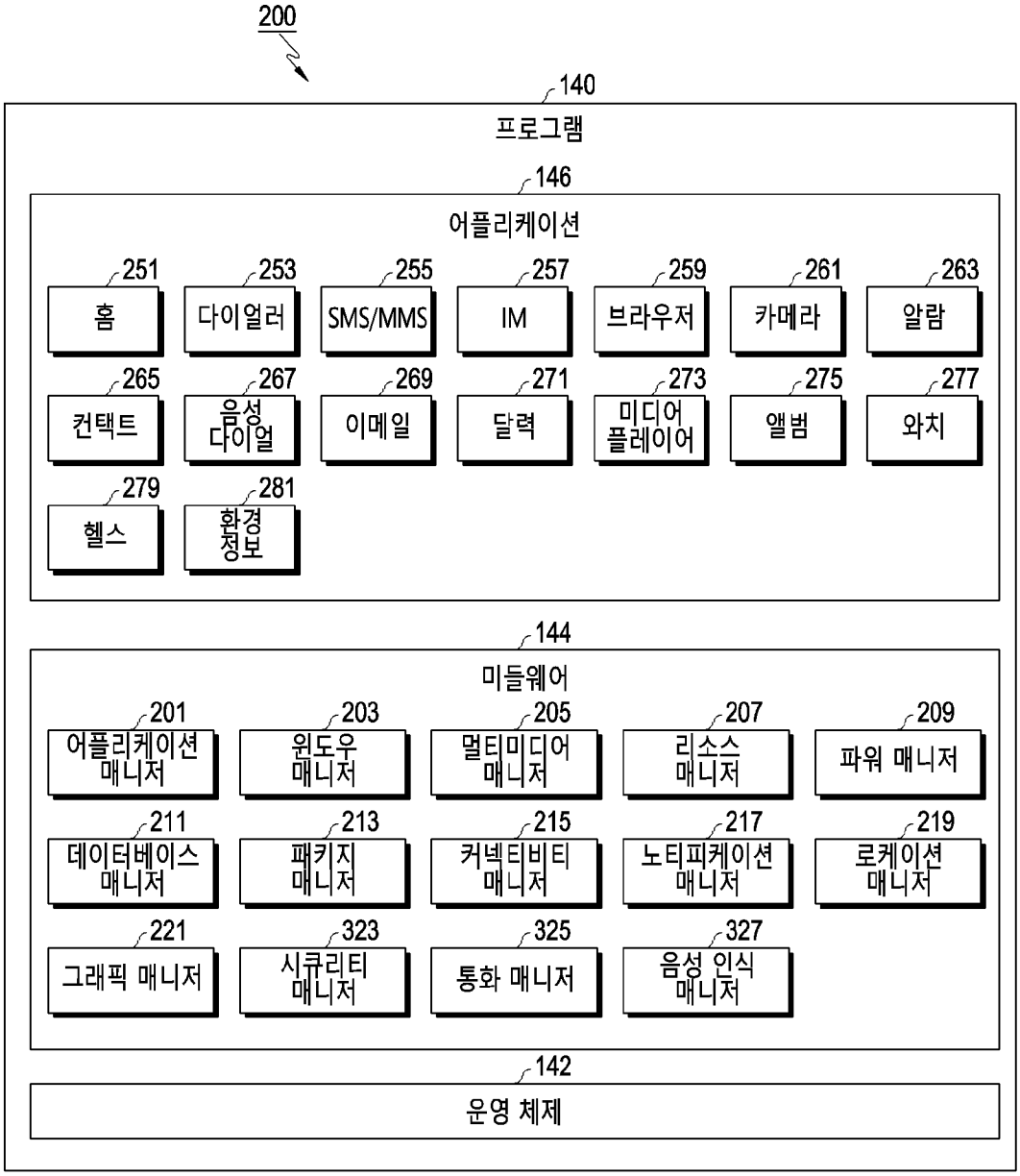
[청구항 14] 제13항에 있어서,
상기 제2 프로세서에 의해,
상기 제3 메모리로부터 상기 암호화 된 보안 데이터, 상기 암호화 된 ARC 테이블, 및 상기 암호화 된 태그 테이블을 포함하는 파일(610)을 독출하고(801), 상기 암호화 된 부분(621), 상기 암호화 된 ARC 테이블(622), 및 상기 암호화 된 태그 테이블(623)을 각각 상기 제1 메모리에 저장하는 동작을 더 포함하는 방법.

[청구항 15] 제12항 내지 제14항 중 어느 한 항에 있어서,
상기 암호화 하는 동작(601,605)은,
상기 보안 데이터 중 적어도 일부와, 상기 ARC 테이블을 암호화 할 때, AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 암호화 하고,
상기 복호화 하는 동작(705)은,
상기 암호화 된 부분을 AES(advanced encryption standard)-GCM(galois/counter mode) 방식으로 복호화 하고,
상기 태그 테이블을 암호화 하는 동작(603)은,
AES(advanced encryption standard)- ECB(electronic code block) 방식으로 암호화 하는 방법.

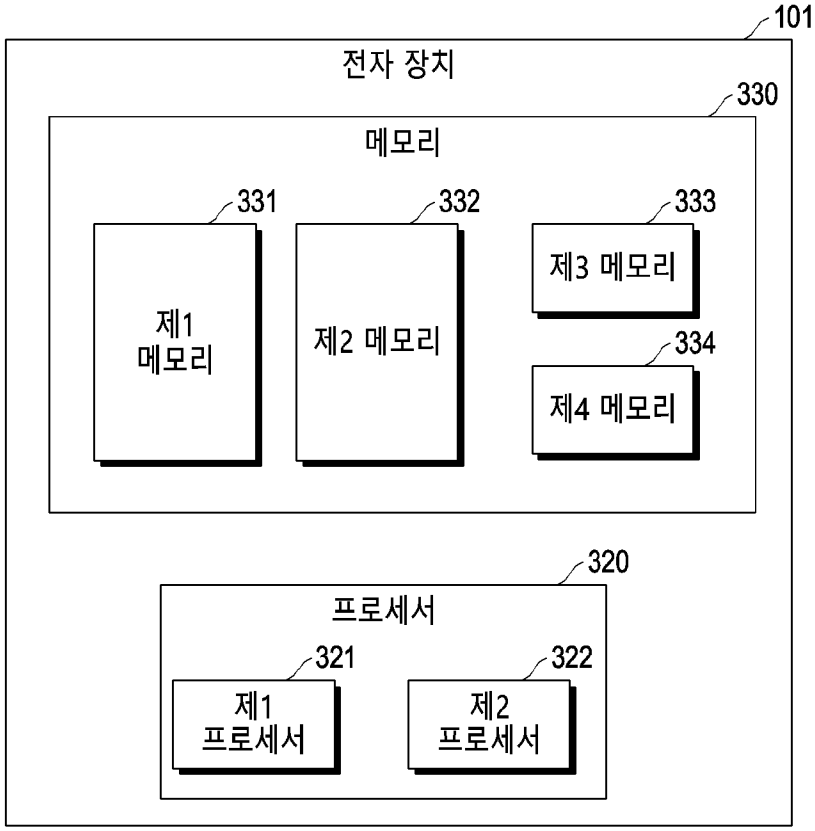
[도1]


100
전자 장치 101
프로그램 140
어플리케이션 146
미들 웨어 144
운영 체제 142
메모리 130
휘발성 메모리 132
비휘발성 메모리 134
내장 메모리 136
외장 메모리 138
표시 장치 160
입력 장치 150
음향 출력 장치 155
프로세서 120
메인 프로세서 121
보조 프로세서 123
배터리 189
전력 관리 모듈 188
통신 모듈 190
무선 통신 모듈 192
유선 통신 모듈 194
가입자 식별 모듈 196
안테나 모듈 197
인터페이스 177
연결 단자 178
센서 모듈 176
카메라 모듈 180
오디오 모듈 170
햅틱 모듈 179
전자 장치 104
제2 네트워크 199
제1 네트워크 198
서버 108
전자 장치 102

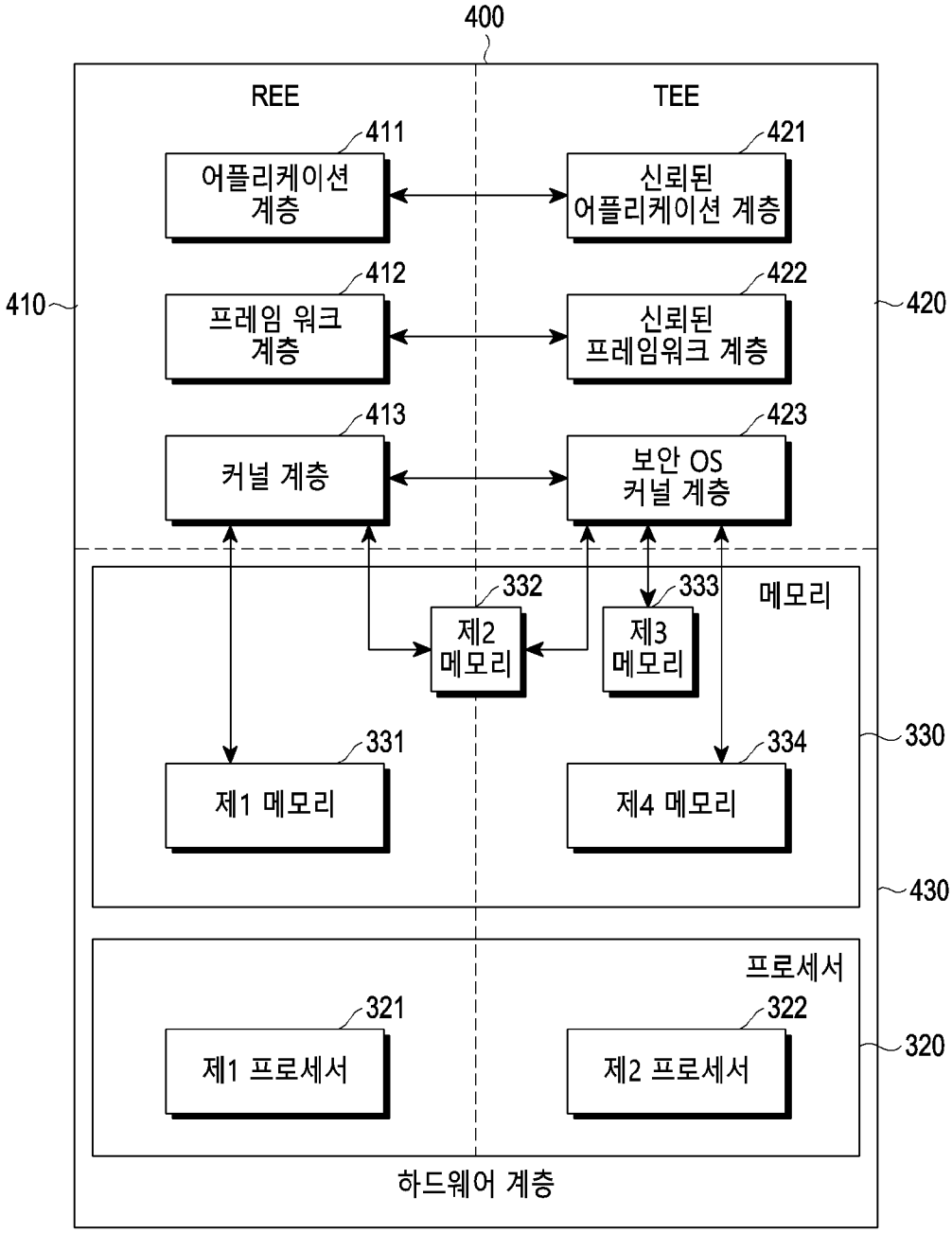
[도2]


200
140
프로그램
146
어플리케이션
251
홈
253
다이얼러
255
SMS/MMS
257
IM
259
브라우저
261
카메라
263
알람
265
컨택트
267
음성 다이얼
269
이메일
271
달력
273
미디어 플레이어
275
앨범
277
와치
279
헬스
281
환경 정보
144
미들웨어
201
어플리케이션 매니저
203
윈도우 매니저
205
멀티미디어 매니저
207
리소스 매니저
209
파워 매니저
211
데이터베이스 매니저
213
패키지 매니저
215
커넥티비티 매니저
217
노티피케이션 매니저
219
로케이션 매니저
221
그래픽 매니저
323
시큐리티 매니저
325
통화 매니저
327
음성 인식 매니저
142
운영 체제

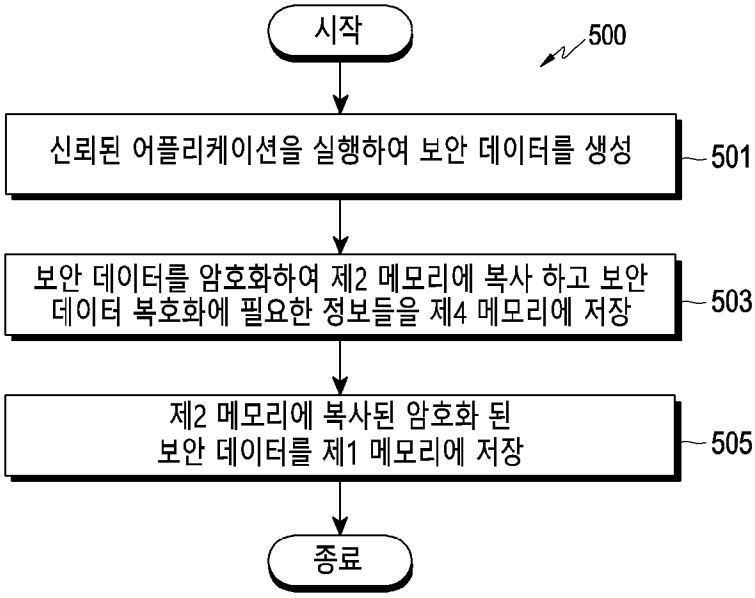
[도3]


101
전자 장치
330
메모리
331
제1 메모리
332
제2 메모리
333
제3 메모리
334
제4 메모리
320
프로세서
321
제1 프로세서
322
제2 프로세서

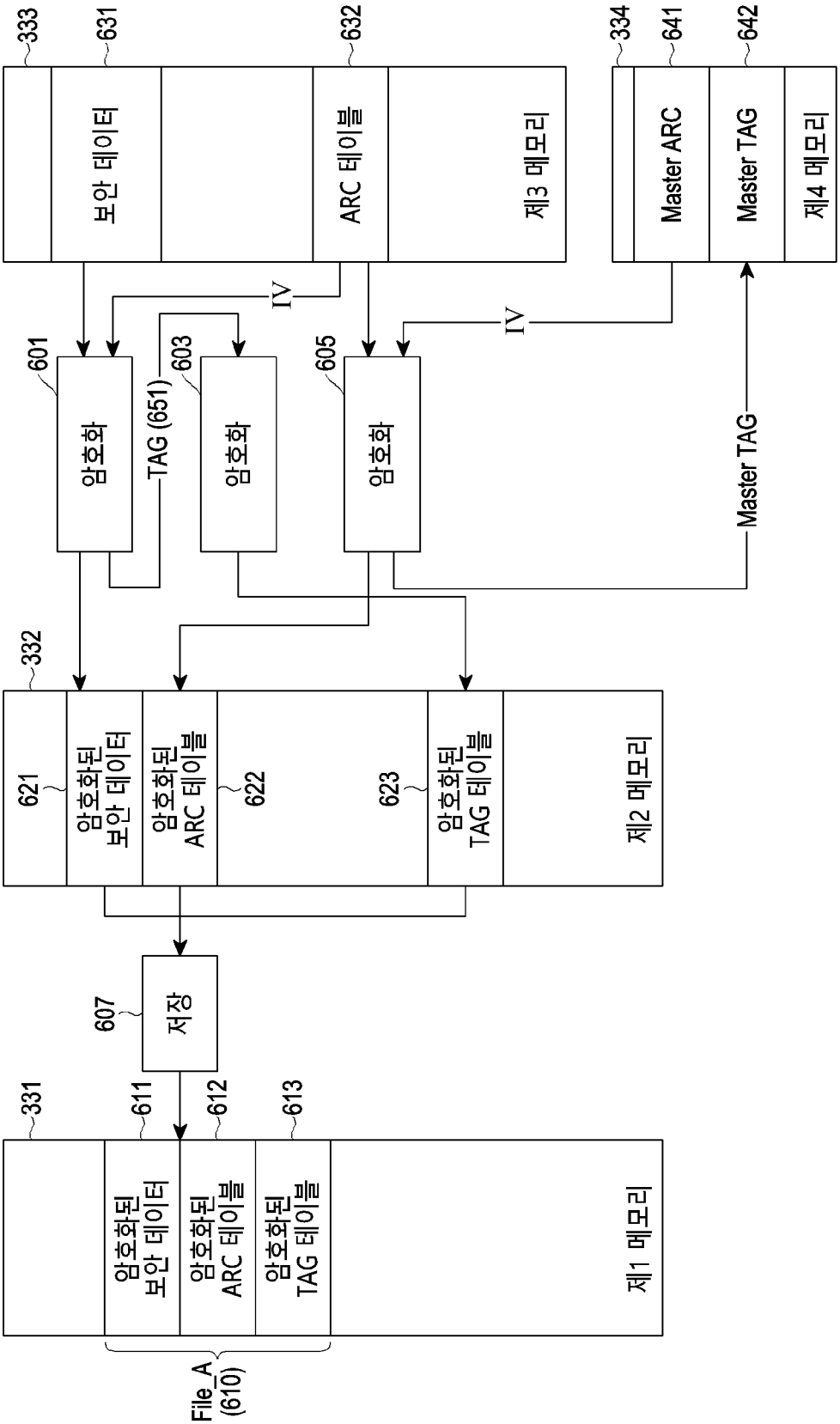
[도4]


400
REE
TEE
411
어플리케이션 계층
421
신뢰된 어플리케이션 계층
412
프레임 워크 계층
422
신뢰된 프레임워크 계층
410
420
413
커널 계층
423
보안 OS 커널 계층
332
제2 메모리
333
제3 메모리
메모리
331
제1 메모리
334
제4 메모리
330
430
프로세서
321
제1 프로세서
322
제2 프로세서
320
하드웨어 계층

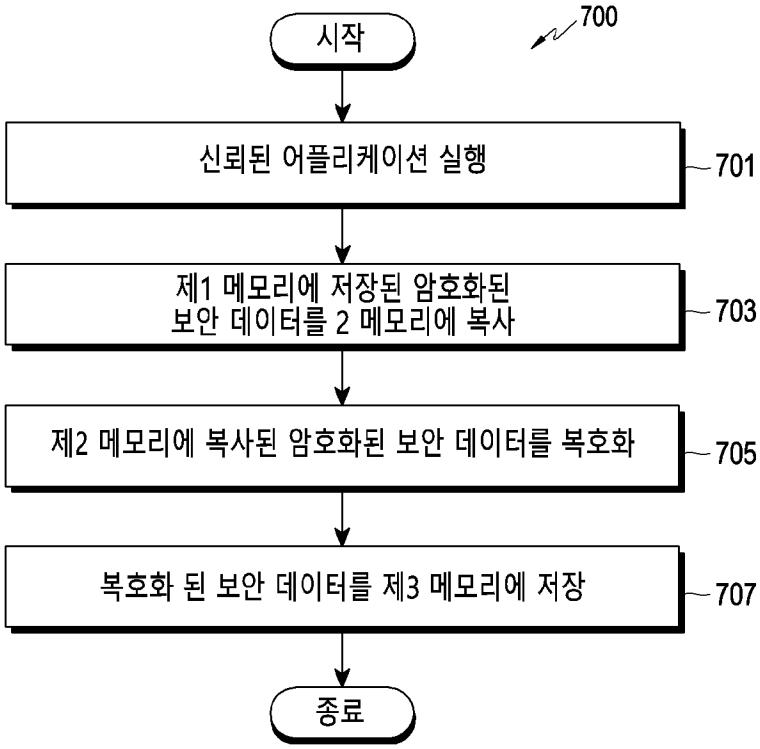
[도5]


시작
500
신뢰된 어플리케이션을 실행하여 보안 데이터를 생성
501
보안 데이터를 암호화하여 제2 메모리에 복사 하고 보안 데이터 복호화에 필요한 정보들을 제4 메모리에 저장
503
제2 메모리에 복사된 암호화 된 보안 데이터를 제1 메모리에 저장
505
종료

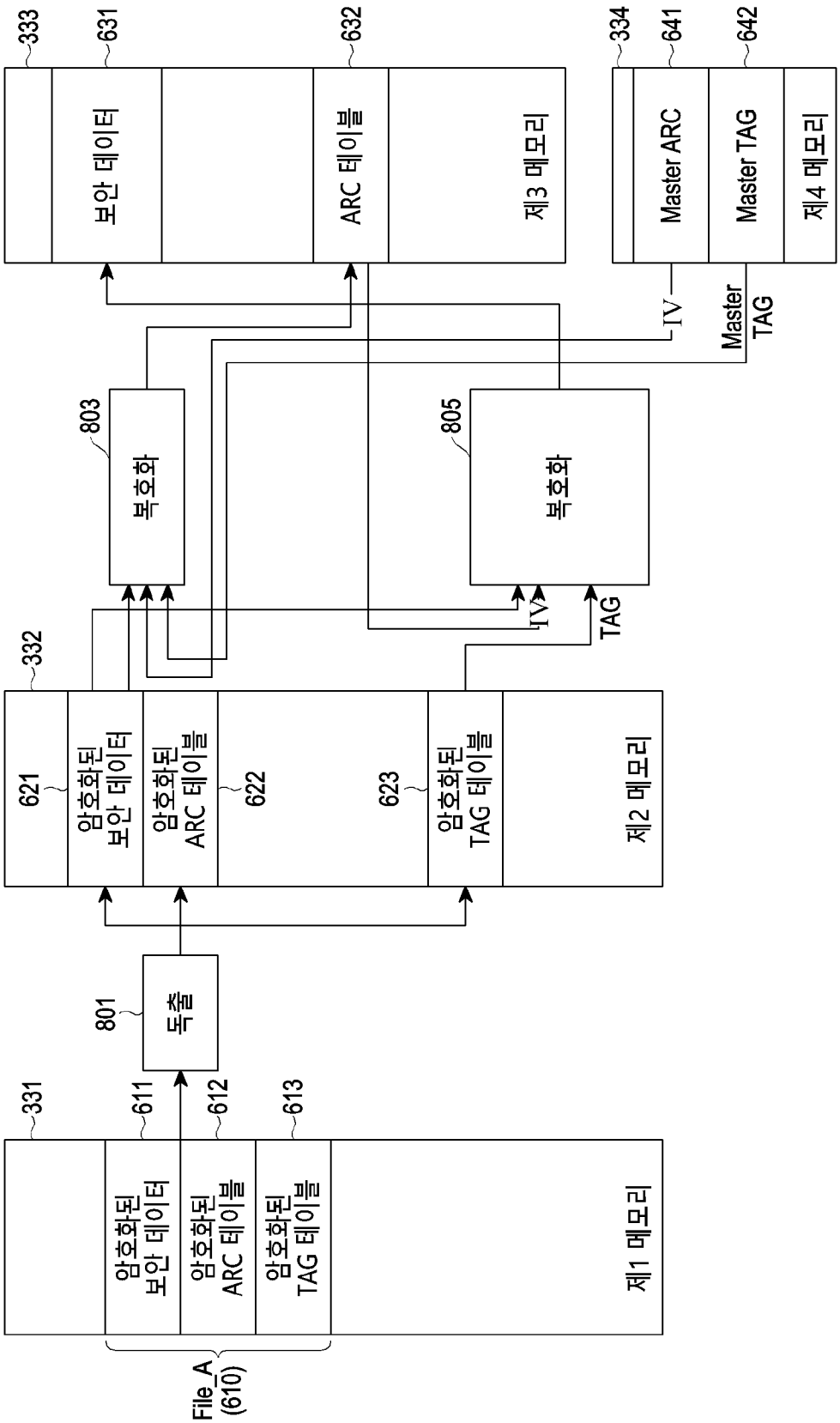
[도6]


333
631
632
334
641
642
보안 데이터
ARC 테이블
제3 메모리
Master ARC
Master TAG
제4 메모리
IV
IV
601
603
605
암호화
TAG (651)
암호화
암호화
Master TAG
332
621
암호화된 보안 데이터
암호화된 ARC 테이블
622
623
암호화된 TAG 테이블
제2 메모리
607
저장
331
611
612
613
암호화된 보안 데이터
암호화된 ARC 테이블
암호화된 TAG 테이블
제1 메모리
File_A (610)

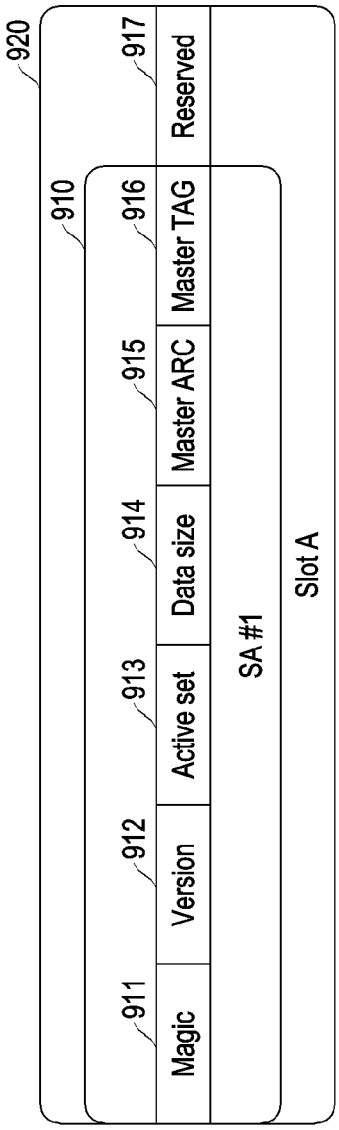
[도7]


700
시작
신뢰된 어플리케이션 실행
701
제1 메모리에 저장된 암호화된
보안 데이터를 2 메모리에 복사
703
제2 메모리에 복사된 암호화된 보안 데이터를 복호화
705
복호화 된 보안 데이터를 제3 메모리에 저장
707
종료

[도8]


333
631
632
334
641
642
보안 데이터
ARC 테이블
제3 메모리
Master ARC
Master TAG
제4 메모리
IV
Master TAG
803
805
복호화
복호화
IV
TAG
332
621
622
623
암호화된 보안 데이터
암호화된 ARC 테이블
암호화된 TAG 테이블
제2 메모리
801
독출
331
611
612
613
암호화된 보안 데이터
암호화된 ARC 테이블
암호화된 TAG 테이블
제1 메모리
File_A (610)

[도9]


920
910
911
Magic
912
Version
913
Active set
914
Data size
915
Master ARC
916
Master TAG
917
Reserved
SA #1
Slot A

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2023/018740

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/79(2013.01)i; **G06F 21/53**(2013.01)i; **G06F 21/60**(2013.01)i; **H04W 12/03**(2021.01)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 21/79(2013.01); G06F 12/14(2006.01); G06F 21/60(2013.01); G06F 9/50(2006.01); G06F 9/54(2006.01); H04L 9/08(2006.01); H04N 5/907(2006.01); H04W 12/02(2009.01); H04W 12/08(2009.01)

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: 보안(secure), TEE(trusted execution environment), REE(rich execution environment), 암호화(encrypt), 공유(share), 메모리(memory), 블록(block), ARC(anti-replay counter), 태그(tag), 테이블(table)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2017-0124360 A (SAMSUNG ELECTRONICS CO., LTD.) 10 November 2017 (2017-11-10) See paragraphs [0021]-[0054]; claim 1; and figures 1-2.	1-15
A	US 2020-0304295 A1 (JPMORGAN CHASE BANK, N.A.) 24 September 2020 (2020-09-24) See paragraphs [0036] and [0039]-[0053]; claims 1 and 4; and figure 1.	1-15
A	US 2008-0320263 A1 (NEMIROFF, Daniel et al.) 25 December 2008 (2008-12-25) See paragraphs [0022]-[0036]; and figures 2-5.	1-15
A	CN 113553204 A (ALIPAY (HANGZHOU) TECHNOLOGY CO., LTD.) 26 October 2021 (2021-10-26) See paragraphs [0027]-[0038]; claim 1; and figures 1A-1B.	1-15
A	KR 10-2022-0062866 A (HANWHA TECHWIN CO., LTD.) 17 May 2022 (2022-05-17) See paragraphs [0024]-[0037]; claim 1; and figure 2.	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	Date of mailing of the international search report
26 February 2024	**26 February 2024**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2023/018740

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2017-0124360 A	10 November 2017	KR 10-2425368 B1	27 July 2022
		US 10469462 B2	05 November 2019
		US 2017-0317990 A1	02 November 2017
US 2020-0304295 A1	24 September 2020	US 11641274 B2	02 May 2023
		WO 2020-198099 A1	01 October 2020
US 2008-0320263 A1	25 December 2008	CN 101388053 A	18 March 2009
		CN 101388053 B	13 July 2011
		DE 102008025197 A1	08 January 2009
		JP 2009-003933 A	08 January 2009
CN 113553204 A	26 October 2021	CN 113553204 B	28 December 2021
KR 10-2022-0062866 A	17 May 2022	None	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2023/018740

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/79(2013.01)i; **G06F 21/53**(2013.01)i; **G06F 21/60**(2013.01)i; **H04W 12/03**(2021.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/79(2013.01); G06F 12/14(2006.01); G06F 21/60(2013.01); G06F 9/50(2006.01); G06F 9/54(2006.01); H04L 9/08(2006.01); H04N 5/907(2006.01); H04W 12/02(2009.01); H04W 12/08(2009.01)

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: 보안(secure), TEE(trusted execution environment), REE(rich execution environment), 암호화(encrypt), 공유(share), 메모리(memory), 블록(block), ARC(anti-replay counter), 태그(tag), 테이블(table)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2017-0124360 A (삼성전자주식회사) 2017.11.10 단락 [0021]-[0054]; 청구항 1; 및 도면 1-2	1-15
A	US 2020-0304295 A1 (JPMORGAN CHASE BANK, N.A.) 2020.09.24 단락 [0036], [0039]-[0053]; 청구항 1, 4; 및 도면 1	1-15
A	US 2008-0320263 A1 (DANIEL NEMIROFF 등) 2008.12.25 단락 [0022]-[0036]; 및 도면 2-5	1-15
A	CN 113553204 A (ALIPAY (HANGZHOU) TECHNOLOGY CO., LTD.) 2021.10.26 단락 [0027]-[0038]; 청구항 1; 및 도면 1A-1B	1-15
A	KR 10-2022-0062866 A (한화테크윈 주식회사) 2022.05.17 단락 [0024]-[0037]; 청구항 1; 및 도면 2	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 문헌과조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.
"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2024년02월26일(26.02.2024)	**2024년02월26일(26.02.2024)**

ISA/KR의 명칭 및 우편주소

대한민국 특허청
(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)

팩스 번호 **+82-42-481-8578**

심사관

김성희

전화번호 **+82-42-481-3516**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2023/018740

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2017-0124360 A	2017/11/10	KR 10-2425368 B1	2022/07/27
		US 10469462 B2	2019/11/05
		US 2017-0317990 A1	2017/11/02
US 2020-0304295 A1	2020/09/24	US 11641274 B2	2023/05/02
		WO 2020-198099 A1	2020/10/01
US 2008-0320263 A1	2008/12/25	CN 101388053 A	2009/03/18
		CN 101388053 B	2011/07/13
		DE 102008025197 A1	2009/01/08
		JP 2009-003933 A	2009/01/08
CN 113553204 A	2021/10/26	CN 113553204 B	2021/12/28
KR 10-2022-0062866 A	2022/05/17	없음	