

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016년 9월 22일 (22.09.2016)



(10) 국제공개번호
WO 2016/148491 A1

- (51) 국제특허분류:
G06F 21/10 (2013.01) H04L 9/08 (2006.01)
G06F 21/60 (2013.01)
- (21) 국제출원번호: PCT/KR2016/002605
- (22) 국제출원일: 2016년 3월 16일 (16.03.2016)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2015-0037780 2015년 3월 18일 (18.03.2015) KR
- (71) 출원인: 삼성전자 주식회사 (SAMSUNG ELECTRONICS CO., LTD.) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). 서울대학교산학협력단 (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) [KR/KR]; 08826 서울시 관악구 관악로 1, Seoul (KR).
- (72) 발명자: 신준범 (SHIN, Jun-Bum); 16701 경기도 수원시 영통구 봉영로 1526 살구골 7 단지아파트 717 동

104 호, Gyeonggi-do (KR). 백운홍 (PAEK, Yun-Heung); 08826 서울시 관악구 관악로 1, Seoul (KR). 함명주 (HAM, Myung-Joo); 05507 서울시 송파구 올림픽로 435 파크리오아파트 215 동 2905 호, Seoul (KR). 조영필 (CHO, Yeong-Pil); 08826 서울시 관악구 관악로 1, Seoul (KR).

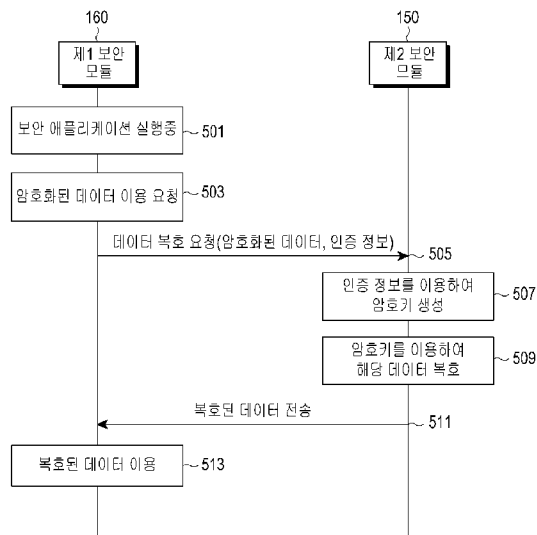
(74) 대리인: 이건주 (LEE, Keon-Joo) 등; 03079 서울시 종로구 대학로 9길 16 미화빌딩, Seoul (KR).

(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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[다음 쪽 계속]

(54) Title: METHOD AND APPARATUS FOR PROTECTING APPLICATION

(54) 발명의 명칭 : 애플리케이션 보호 방법 및 장치



- 150 ... Second security module
160 ... First security module
501 ... During execution of security application
503 ... Request use of encrypted data
505 ... Request data decryption (encrypted data, authentication information)
507 ... Generate encryption key by using authentication information
509 ... Decrypt corresponding data by using encryption key
511 ... Transmit decrypted data
513 ... Use decrypted data

(57) Abstract: The present invention relates to a method for protecting content of an electronic device, comprising the steps of: enabling a first security module to transmit a data encryption request to a second security module when data requiring security is generated according to the execution of a security application by the first security module in a security storage region of a memory; enabling the second security module to generate an encryption key by using the authentication information included in the data encryption request and to encrypt the data included in the data encryption request by using the encryption key; enabling the second security module to transfer the encrypted data to the first security module; and enabling the first security module to store the encrypted data in the security application.

(57) 요약서: 본 발명은 전자 장치의 콘텐츠 보호 방법에 있어서, 메모리의 보안 저장 영역에서, 제 1 보안 모듈에 의해, 보안 애플리케이션이 실행됨에 따라 보안이 필요한 데이터가 생성되면, 상기 제 1 보안 모듈이 제 2 보안 모듈에게 데이터 암호화 요청을 전송하는 과정과, 상기 제 2 보안 모듈이 상기 데이터 암호화 요청에 포함된 인증 정보를 이용해 암호키를 생성하고, 상기 데이터 암호화 요청에 포함된 상기 데이터를 상기 암호키를 이용해 암호화하는 과정과, 상기 제 2 보안 모듈이 상기 암호화된 데이터를 상기 제 1 보안 모듈로 전달하는 과정과, 상기 제 1 보안 모듈이 상기 암호화된 데이터를 상기 보안 애플리케이션에 저장하는 과정을 포함할 수 있다.



(84) **지정국** (별도의 표시가 없는 한, 가능한 모든 종류의 역내 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), 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, 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 제 21 조(3))

명세서

발명의 명칭: 애플리케이션 보호 방법 및 장치

기술분야

- [1] 본 발명은 전자 장치에 관한 것으로, 특히, 전자 장치에 저장된 애플리케이션을 안전하게 보호하는 방법 및 장치에 관한 것이다.

배경기술

- [2] 최근, 모바일 장치는 고품질의 서비스를 처리할 것이 요구된다. 예를 들어, 모바일 장치는 인터넷이나 이동 통신 네트워크로부터 다양한 애플리케이션을 다운로드하여 설치할 수 있으며, 이에 따라, 각 애플리케이션에서 제공되는 서비스를 제공할 수 있게 되었다. 애플리케이션은, 예를 들어, 게임 애플리케이션, SNS(Social Networking Service) 기반의 애플리케이션, 금융 거래 애플리케이션, 이미지 편집 애플리케이션, 지도 애플리케이션 등이 있다.
- [3] 이와 같은 다양한 서비스를 제공할 수 있도록, 모바일 장치는 중앙처리장치(Central Process Unit, CPU)와 운영체제(Operating System, OS)를 채용하고 있다. 모바일 장치는 개방형 애플리케이션 프로그램 인터페이스(Open Application Program Interface)를 구현하기 위해 개방형 운영체제(Open OS)를 채택하고 있다. 개방형 운영체제는 모바일 장치와 모바일 서비스의 경쟁력의 핵심이 되고 있다. 그리고 모바일 장치의 운영체제는 주요 제조사 및 주요 공급자에 의해 전략적으로 개방되어, 애플리케이션 프로그램 인터페이스(Application Program Interface), 소프트웨어 개발 키트(Software Development Kit), 및 소스파일까지 일반에 공개되고 있다.
- [4] 모바일 장치가 인터넷으로부터 다운로드하는 애플리케이션들을 모바일 장치의 제조사에 의해 품질의 검사 및 보장이 된 이후에 이용할 수 있도록 되어있으나, 실질적으로 다양한 애플리케이션들의 모든 기능들이 검사될 수는 없다. 따라서, 이러한 모바일 장치를 타깃으로 하는 악성 코드가 점점 증가하고 있으며, 특히 개방형 운영체제를 사용하는 모바일 장치들이 악성 코드들의 소프트웨어 공격을 받을 수 있는 문제가 있다. 따라서 최근에는 보안 운영체제를 사용하기 위한 방법들이 모색되고 있다.
- [5] 보안 운영체제를 사용하기 위한 방법에는 예를 들어, 하이퍼바이저(Hypervisor) 기반의 보안 방법이 있다. 하이퍼바이저 기반의 보안 방법은 메모리의 저장 영역을 비보안 저장 영역과 보안 저장 영역으로 구분하고, 보안이 요구되는 애플리케이션(이하 '보안 애플리케이션'이라 함)은 보안 저장 영역에서 동작하도록 하는 실행 환경을 제공한다. 다시 말해, 모바일 장치 부팅시 하이퍼바이저가 메모리의 저장 영역을 비보안 저장 영역과 보안 저장 영역으로 구분하고, 보안이 요구되지 않는 일반 애플리케이션은 비보안 저장 영역에서 동작하고, 보안 애플리케이션은 보안 저장 영역에서 동작한다.

- [6] 다른 방법으로 트러스트존(TrustZone) 기반의 보안 방법이 있다. 트러스트존 기반의 보안 방법은 하드웨어 레벨에서 보안 애플리케이션을 보호하기 위한 방법으로, 별도의 보안 하드웨어 칩을 쓰지 않고 하나의 애플리케이션 제어부(예를 들어, CPU, ARM등)에 Secure World와 Normal World가 존재하도록 하여 일반 애플리케이션은 Normal World에서 동작하고 보안이 필요한 애플리케이션은 Secure World에서 안전하게 동작하도록 하는 실행 환경을 제공한다.

발명의 상세한 설명

기술적 과제

- [7] 하이퍼바이저 기반의 보안 방법은 보안기능을 사용하지 않을 때에 성능 저하가 발생하는 문제가 있다.
- [8] 그리고 트러스트존 기반의 보안 방법은 모바일 장치의 제조시 인증된 보안 애플리케이션 이외에 새로운 보안 애플리케이션에 대한 인증 과정이 복잡하기 때문에, 새로운 보안 애플리케이션을 보호하기 힘들다는 문제점이 있다.

과제 해결 수단

- [9] 본 발명은 상기한 문제점을 해결하기 위해, 악성 코드들의 공격으로부터 강건한 애플리케이션 보호 방법 및 장치를 제공한다.
- [10] 그리고 본 발명은 다양한 보안 애플리케이션을 보호할 수 있는 애플리케이션 보호 방법 및 장치를 제공한다.
- [11] 그리고 본 발명은 하이퍼바이저로 인한 성능 저하 문제를 예방하기 위하여 하이퍼바이저를 보안 애플리케이션이 실행되지 않는 동안에는 비활성화 하고, 보안 애플리케이션이 실행되는 동안에만 활성화 하는 특징이 있다.
- [12] 또한 보안 애플리케이션에 대한 실행 지연을 방지할 수 있는 애플리케이션 보호 방법 및 장치를 제공한다.
- [13] 한편, 본 발명은 전자 장치의 애플리케이션 보호 방법에 있어서, 메모리의 보안 저장 영역에서, 제1보안 모듈에 의해, 보안 애플리케이션이 실행됨에 따라 보안이 필요한 데이터가 생성되면, 상기 제1보안 모듈이 제2보안 모듈에게 데이터 암호화 요청을 전송하는 과정과, 상기 제2보안 모듈이 상기 데이터 암호화 요청에 포함된 인증 정보를 이용해 암호키를 생성하고, 상기 데이터 암호화 요청에 포함된 상기 데이터를 상기 암호키를 이용해 암호화하는 과정과, 상기 제2보안 모듈이 상기 암호화된 데이터를 상기 제1보안 모듈로 전달하는 과정과, 상기 제1보안 모듈이 상기 암호화된 데이터를 상기 보안 애플리케이션에 저장하는 과정을 포함할 수 있다.
- [14] 한편 본 발명의 실시예에 따른, 전자 장치에 있어서, 메모리와, 제어부를 포함하며, 상기 제어부는 상기 메모리의 보안 저장 영역에서 보안 애플리케이션을 실행하고, 상기 보안 애플리케이션의 실행에 따라 보안이 필요한 데이터가 생성되면, 제2보안 모듈에게 데이터 암호화 요청을 전송하는

제1보안 모듈과, 상기 데이터 암호화 요청에 포함된 인증 정보를 이용해 암호키를 생성하고, 상기 데이터 암호화 요청에 포함된 상기 데이터를 상기 암호키를 이용해 암호화하고, 상기 암호화된 데이터를 상기 제1보안 모듈로 전달하는 상기 제2보안 모듈을 포함하며, 상기 제1보안 모듈은 상기 암호화된 데이터를 상기 보안 애플리케이션에 저장할 수 있다.

발명의 효과

- [15] 본 발명은 이중의 보안 모듈을 구비함으로써, 악성 코드들의 공격으로부터 애플리케이션을 강하게 보호할 수 있다. 그리고 본 발명은 모바일 장치에 새롭게 추가되는 다양한 보안 애플리케이션을 보호할 수 있다. 또한 본 발명은 보안 애플리케이션에 대한 실행 지연을 방지할 수 있다.

도면의 간단한 설명

- [16] 도1은 본 발명의 일 실시예에 따른 전자 장치의 구성을 나타낸 도면,
 [17] 도2는 본 발명의 다른 실시예에 따른 전자 장치의 구성을 나타낸 도면,
 [18] 도3은 본 발명의 일 실시예에 따른 전자 장치의 부팅 과정을 나타낸 도면,
 [19] 도4는 본 발명의 일 실시예에 따른 새로운 애플리케이션의 설치 과정을 나타낸 도면,
 [20] 도5는 본 발명의 일 실시예에 따른 보안 애플리케이션 실행에 따라 발생하는 데이터 저장 과정을 나타낸 도면,
 [21] 도6은 본 발명의 일 실시예에 따른 보안 애플리케이션에 저장된 데이터 이용 과정을 나타낸 도면,
 [22] 도7은 본 발명의 일 실시예에 따른 보안 애플리케이션의 실행 상태를 나타낸 도면,
 [23] 도8은 본 발명의 일 실시예에 따른 모바일 장치의 구성을 나타낸 도면.

발명의 실시를 위한 형태

- [24] 이하, 본 문서의 다양한 실시예가 첨부된 도면을 참조하여 기재된다. 그러나, 이는 본 문서에 기재된 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 문서의 실시예의 다양한 변경(modifications), 균등물(equivalents), 및/또는 대체물(alternatives)을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다.
- [25] 본 문서에서, '가진다,' '가질 수 있다,' '포함한다,' 또는 '포함할 수 있다' 등의 표현은 해당 특징(예: 수치, 기능, 동작, 또는 부품 등의 구성요소)의 존재를 가리키며, 추가적인 특징의 존재를 배제하지 않는다.
- [26] 본 문서에서, 'A 또는 B,' 'A 또는/및 B 중 적어도 하나,' 또는 'A 또는/및 B 중 하나 또는 그 이상' 등의 표현은 함께 나열된 항목들의 모든 가능한 조합을 포함할 수 있다. 예를 들면, 'A 또는 B,' 'A 및 B 중 적어도 하나,' 또는 'A 또는 B 중 적어도 하나'는, (1) 적어도 하나의 A를 포함, (2) 적어도 하나의 B를 포함, 또는 (3) 적어도 하나의 A 및 적어도 하나의 B 모두를 포함하는 경우를 모두 지칭할 수

있다.

- [27] 본 문서에서 사용된 '제 1,' '제 2,' '첫째,' 또는 '둘째,' 등의 표현들은 다양한 구성요소들을, 순서 및/또는 중요도에 상관없이 수식할 수 있고, 한 구성요소를 다른 구성요소와 구분하기 위해 사용될 뿐 해당 구성요소들을 한정하지 않는다. 예를 들면, 제 1 사용자 기기와 제 2 사용자 기기는, 순서 또는 중요도와 무관하게, 서로 다른 사용자 기기를 나타낼 수 있다. 예를 들면, 본 문서에 기재된 권리 범위를 벗어나지 않으면서 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 바꾸어 명명될 수 있다.
- [28] 어떤 구성요소(예: 제 1 구성요소)가 다른 구성요소(예: 제 2 구성요소)에 '(기능적으로 또는 통신적으로) 연결되어'((operatively or communicatively) coupled with/to)' 있다거나 '접속되어'(connected to)' 있다고 언급된 때에는, 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로 연결되거나, 다른 구성요소(예: 제 3 구성요소)를 통하여 연결될 수 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소(예: 제 1 구성요소)가 다른 구성요소(예: 제 2 구성요소)에 '직접 연결되어' 있다거나 '직접 접속되어' 있다고 언급된 때에는, 상기 어떤 구성요소와 상기 다른 구성요소 사이에 다른 구성요소(예: 제 3 구성요소)가 존재하지 않는 것으로 이해될 수 있다.
- [29] 본 문서에서 사용된 표현 '~하도록 구성된(또는 설정된)(configured to)'은 상황에 따라, 예를 들면, '~에 적합한(suitable for),' '~하는 능력을 가지는(having the capacity to),' '~하도록 설계된(designed to),' '~하도록 변경된(adapted to),' '~하도록 만들어진(made to),' 또는 '~를 할 수 있는(capable of)'과 바꾸어 사용될 수 있다. 용어 '~하도록 구성된(또는 설정된)'은 하드웨어적으로 '특별히 설계된(specifically designed to)' 것만을 반드시 의미하지 않을 수 있다. 대신, 어떤 상황에서는, '~하도록 구성된 장치'라는 표현은, 그 장치가 다른 장치 또는 부품들과 함께 '~할 수 있는' 것을 의미할 수 있다. 예를 들면, 문구 'A, B, 및 C를 수행하도록 구성된(또는 설정된) 제어부'는 해당 동작을 수행하기 위한 전용 제어부(예: 임베디드 제어부), 또는 메모리 장치에 저장된 하나 이상의 소프트웨어 프로그램들을 실행함으로써, 해당 동작들을 수행할 수 있는 범용 제어부(generic-purpose processor)(예: CPU 또는 application processor)를 의미할 수 있다.
- [30] 본 문서에서 사용된 용어들은 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 다른 실시예의 범위를 한정하려는 의도가 아닐 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다. 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 용어들은 본 문서에 기재된 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가질 수 있다. 본 문서에 사용된 용어들 중 일반적인 사전에 정의된 용어들은, 관련 기술의 문맥상 가지는 의미와 동일 또는 유사한 의미로 해석될 수 있으며, 본 문서에서 명백하게 정의되지 않는 한, 이상적이거나

과도하게 형식적인 의미로 해석되지 않는다. 경우에 따라서, 본 문서에서 정의된 용어일지라도 본 문서의 실시예들을 배제하도록 해석될 수 없다.

- [31] 본 문서의 다양한 실시예들에 따른 전자 장치는, 예를 들면, 스마트폰(smartphone), 태블릿 PC(tablet personal computer), 이동 전화기(mobile phone), 영상 전화기, 전자책 리더기(e-book reader), 데스크탑 PC(desktop personal computer), 랩탑 PC(laptop personal computer), 넷북 컴퓨터(netbook computer), 워크스테이션(workstation), 서버, PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 모바일 의료기기, 카메라(camera), 또는 웨어러블 장치(wearable device) 중 적어도 하나를 포함할 수 있다. 다양한 실시예에 따르면, 웨어러블 장치는 액세서리형(예: 시계, 반지, 팔찌, 발찌, 목걸이, 안경, 콘택트 렌즈, 또는 머리 착용형 장치(head-mounted-device(HMD))), 직물 또는 의류 일체형(예: 전자 의복), 신체 부착형(예: 스킨 패드(skin pad) 또는 문신), 또는 생체 이식형(예: implantable circuit) 중 적어도 하나를 포함할 수 있다.
- [32] 어떤 실시예들에서, 전자 장치는 가전 제품(home appliance)일 수 있다. 가전 제품은, 예를 들면, 텔레비전, DVD(digital video disk) 플레이어, 오디오, 냉장고, 에어컨, 청소기, 오븐, 전자레인지, 세탁기, 공기 청정기, 셋톱 박스(set-top box), 홈 오토메이션 컨트롤 패널(home automation control panel), 보안 컨트롤 패널(security control panel), TV 박스(예: 삼성 HomeSync™, 애플TV™, 또는 구글 TV™), 게임 콘솔(예: Xbox™, PlayStation™), 전자 사전, 전자 키, 캠코더(camcorder), 또는 전자 액자 중 적어도 하나를 포함할 수 있다.
- [33] 다른 실시예에서, 전자 장치는, 각종 의료기기(예: 각종 휴대용 의료측정기기(혈당 측정기, 심박 측정기, 혈압 측정기, 또는 체온 측정기 등), MRA(magnetic resonance angiography), MRI(magnetic resonance imaging), CT(computed tomography), 촬영기, 또는 초음파기 등), 네비게이션(navigation) 장치, 위성 항법 시스템(GNSS(global navigation satellite system)), EDR(event data recorder), FDR(flight data recorder), 자동차 인포테인먼트(infotainment) 장치, 선박용 전자 장비(예: 선박용 항법 장치, 자이로 콤파스 등), 항공 전자기기(avionics), 보안 기기, 차량용 헤드 유닛(head unit), 산업용 또는 가정용 로봇, 금융 기관의 ATM(automatic teller's machine), 상점의 POS(point of sales), 또는 사물 인터넷 장치(internet of things)(예: 전구, 각종 센서, 전기 또는 가스 미터기, 스프링클러 장치, 화재경보기, 온도조절기(thermostat), 가로등, 토스터(toaster), 운동기구, 온수탱크, 히터, 보일러 등) 중 적어도 하나를 포함할 수 있다.
- [34] 어떤 실시예에 따르면, 전자 장치는 가구(furniture) 또는 건물/구조물의 일부, 전자 보드(electronic board), 전자 사인 수신 장치(electronic signature receiving device), 프로젝터(projector), 또는 각종 계측 기기(예: 수도, 전기, 가스, 또는 전파 계측 기기 등) 중 적어도 하나를 포함할 수 있다. 다양한 실시예에서, 전자 장치는 전술한 다양한 장치들 중 하나 또는 그 이상의 조합일 수 있다. 어떤 실시예에

다른 전자 장치는 플렉서블 전자 장치일 수 있다. 또한, 본 문서의 실시예에 따른 전자 장치는 전술한 기기들에 한정되지 않으며, 기술 발전에 따른 새로운 전자 장치를 포함할 수 있다.

- [35] 본 발명의 실시예에 따른 전자 장치의 구성을 도1에 도시하였다. 도1은 일 실시예에 따른 전자 장치의 구성을 나타낸 도면이다.
- [36] 도1을 참조하면, 전자장치(100)는 메모리(110)와, 제어부(140)와, 통신 인터페이스(180)와, 디스플레이(190)를 포함할 수 있다.
- [37] 디스플레이(190)는, 예를 들면, 액정 디스플레이(liquid crystal display(LCD)), 발광 다이오드(light-emitting diode(LED)) 디스플레이, 유기 발광 다이오드(organic light-emitting diode(OLED)) 디스플레이, 또는 마이크로 전자기계 시스템(microelectromechanical systems(MEMS)) 디스플레이, 또는 전자종이(electronic paper) 디스플레이를 포함할 수 있다. 디스플레이(190)는, 예를 들면, 사용자에게 각종 정보(예: 텍스트, 이미지, 비디오, 아이콘, 또는 심볼 등)를 표시할 수 있다. 디스플레이(190)는, 터치 스크린을 포함할 수 있으며, 예를 들면, 전자 펜 또는 사용자의 신체의 일부를 이용한 터치, 제스처, 근접, 또는 호버링 입력을 수신할 수 있다.
- [38] 통신 인터페이스(180)는, 예를 들면, 전자 장치(100)와 외부 장치 간의 통신을 설정할 수 있다. 예를 들면, 통신 인터페이스(180)는 무선 통신 또는 유선 통신을 통해서 네트워크에 연결되어 외부 장치와 통신할 수 있다.
- [39] 무선 통신은, 예를 들면, 셀룰러 통신 프로토콜로서, 예를 들면, LTE(long-term evolution), LTE-A(LTE Advance), CDMA(code division multiple access), WCDMA(wideband CDMA), UMTS(universal mobile telecommunications system), WiBro(Wireless Broadband), 또는 GSM(Global System for Mobile Communications) 등 중 적어도 하나를 사용할 수 있다. 또한, 무선 통신은, 예를 들면, 근거리 통신을 포함할 수 있다. 근거리 통신은, 예를 들면, WiFi(wireless fidelity), 블루투스(Bluetooth), NFC(near field communication), 또는 GNSS(global navigation satellite system) 등 중 적어도 하나를 포함할 수 있다. GNSS는 사용 지역 또는 대역폭 등에 따라, 예를 들면, GPS(Global Positioning System), Glonass(Global Navigation Satellite System), Beidou Navigation Satellite System(이하 Beidou) 또는 Galileo, the European global satellite-based navigation system 중 적어도 하나를 포함할 수 있다. 이하, 본 문서에서는, GPS는 GNSS와 혼용되어 사용(interchangeably used)될 수 있다. 유선 통신은, 예를 들면, USB(universal serial bus), HDMI(high definition multimedia interface), RS-232(recommended standard232), 또는 POTS(plain old telephone service) 등 중 적어도 하나를 포함할 수 있다. 네트워크(162)는 통신 네트워크(telecommunications network), 예를 들면, 컴퓨터 네트워크(computer network)(예: LAN 또는 WAN), 인터넷, 또는 전화망(telephone network) 중 적어도 하나를 포함할 수 있다.
- [40] 메모리(110)는, 예를 들면, 전자 장치(100)의 적어도 하나의 다른 구성요소에

관계된 명령 또는 데이터를 저장할 수 있다. 한 실시예에 따르면, 메모리(110)는 디지털 콘텐츠를 저장할 수 있다.

- [41] 디지털 콘텐츠는 메모리(110)에 저장되거나 또는 전자 장치(100)에 설치될 수 있는 디지털 데이터로서, 예를 들어, 각종 정보, 각종 애플리케이션 프로그램(이하, '애플리케이션'이라 함), 멀티미디어 데이터 등을 포함할 수 있다. 멀티미디어 데이터는 예를 들어, 텍스트 데이터, 영상 데이터, 동영상 데이터, 오디오 데이터를 포함할 수 있다. 애플리케이션은 보안 애플리케이션(SCF: Security Critical Function)와 비보안 애플리케이션으로 구분할 수 있다. 보안 애플리케이션은 액세스 권한이 제한되거나, 해킹 또는 악성코드로부터 보호받아야 하는 애플리케이션으로서, 애플리케이션에 보안 애플리케이션임을 나타내는 정보 또는 코드가 포함될 수 있다. 보안 애플리케이션은 각종 금융 거래 애플리케이션과, 개인 정보를 이용하는 애플리케이션(예를 들어, SNS 기반 애플리케이션, 연락처 관리 애플리케이션, 영상 저장 애플리케이션, 동영상 저장 애플리케이션) 등을 포함할 수 있다.
- [42] 메모리(110)의 저장 영역은 일 실시예에 따라, 비보안 저장 영역(120)과 보안 저장 영역(130)을 포함할 수 있다. 비보안 저장 영역(120)에는 비보안 애플리케이션 및 비보안 애플리케이션 실행에 필요한 정보가 저장될 수 있다. 그리고 비보안 저장 영역(120)은 비보안 애플리케이션을 실행하기 위한 워킹 메모리로 동작할 수 있다. 보안 저장 영역(130)에는 보안 모듈만 접근할 수 있는 보안 애플리케이션 및 보안 애플리케이션 실행에 필요한 정보가 저장될 수 있으며, 보안 애플리케이션을 실행하기 위한 워킹 메모리로 동작할 수 있다. 보안 저장 영역(130)은 보안 애플리케이션 리스트를 저장할 수 있으며, 보안 애플리케이션 리스트는 각 보안 애플리케이션의 인증 정보를 포함할 수 있다. 그리고 보안 저장 영역(120)의 크기 및 메모리(110) 내에서 위치는 제어부(140)의 제1보안 모듈(160)에 의해 동적으로 변경될 수 있다.
- [43] 제어부(140)는 범용 프로세서(generic-purpose processor)(예: CPU 또는 애플리케이션 제어부(application processor) 또는, 커뮤니케이션 제어부(communication processor), 장치(100)의 제어를 위한 제어프로그램이 저장된 롬(ROM) 및 장치(100)의 외부로부터 입력되는 신호 또는 데이터를 기억하거나, 장치(100)에서 수행되는 작업을 위한 기억영역으로 사용되는 램(RAM) 등을 포함할 수 있다. 범용 제어부는 싱글 코어, 듀얼 코어, 트리플 코어, 또는 쿼드 코어를 포함할 수 있다.
- [44] 이러한 제어부(140)는 일 실시예에 따라, 하나의 범용 프로세서를 이용하여 비보안 프로세스 또는 비보안 애플리케이션에 대한 비보안 실행을 수행하는 메인모듈(170)과, 보안 프로세스 또는 보안 애플리케이션에 대한 보안 실행을 수행하는 복수의 보안 모듈, 즉 제1보안 모듈(160)과, 제2보안 모듈(150)을 포함할 수 있다.
- [45] 일반 모듈(170)에서는 일반 운영체제(Normal Operating System)(171)가 실행될

수 있고, 복수의 보안 모듈(150,160) 각각에서는 별도의 보안 운영체제(Secure Operating System)(151,161)가 실행될 수 있다. 다시 말해, 제2보안 모듈(150)에서는 제2보안 운영체제(151)가 실행될 수 있고, 제1보안 모듈(160)에서는 제1보안 운영체제(161)가 실행될 수 있다. 보안 운영체제(151,161)에 의해 이용되는 메모리 영역은 보안 저장 영역(130)으로서 일반 운영체제(171)에 의한 접근이 차단된다. 이에 따라, 일반 운영체제(171)가 공개형 운영체제인 경우에도 악성 코드가 보안 운영체제(151,161) 및 보안 운영체제(151,161)가 이용하는 메모리 영역에 접근을 할 수 없게 된다.

- [46] 일반 모듈(170)은 전자 장치(100)의 동작과 관련된 비보안 프로세스를 수행하거나, 비보안 애플리케이션을 수행할 수 있다. 그리고 일반 모듈(170)은 보안 프로세스 또는 보안 애플리케이션의 실행 요청이 있으면, 이를 제1보안 모듈(160)에게 통지할 수 있다.
- [47] 제1보안 모듈(160)은 보안 저장 영역(130)에서 전자 장치(100)의 동작과 관련된 보안 프로세스를 수행하거나, 보안 애플리케이션의 저장, 설치, 실행, 업데이트를 제어할 수 있다. 이에 따라, 보안 애플리케이션을 악성 코드등으로부터 1차적으로 보호될 수 있다.
- [48] 그리고 제1보안 모듈(160)은 보안 애플리케이션 실행 중에 보안이 필요한 데이터가 발생되면 제2보안 모듈(150)에게 상기 데이터에 대한 암호화를 요청한다. 암호화 요청시 제1보안 모듈(160)은 상기 데이터와 함께 보안 애플리케이션의 인증 정보를 제2보안 모듈(150)로 전송한다. 암호키 생성시 이용되는 인증 정보는 상기 보안 애플리케이션의 개발자 식별 정보와, 보안 애플리케이션 식별 정보가 될 수 있다. 이에 따라, 제2보안 모듈(150)은 상기 인증 정보를 이용해 암호키를 생성하고, 생성된 암호키를 이용해 상기 데이터를 암호화하여 제1보안 모듈(160)로 전송할 수 있다. 제1보안 모듈(160)은 암호화된 데이터를 상기 보안 애플리케이션에 저장할 수 있다. 이에 따라, 보안 애플리케이션의 주요 데이터는 2차적으로 보호될 수 있다.
- [49] 제1보안 모듈(160)은 보안 애플리케이션 실행에 따라 상기 암호화된 데이터를 이용해야 하는 경우 제2보안 모듈(150)로 암호화된 데이터에 대한 복호를 요청할 수 있다. 복호 요청시 제1보안 모듈(160)은 상기 암호화된 데이터와 함께 보안 애플리케이션의 인증 정보를 제2보안 모듈(150)로 전송한다. 이에 따라, 제2보안 모듈(150)은 상기 인증 정보를 이용해 암호키를 생성하고, 생성된 암호키를 이용해 상기 암호화된 데이터를 복호하여 제1보안 모듈(160)로 전송할 수 있다.
- [50] 제1보안 모듈(160)은 부팅시 또는 보안 애플리케이션을 실행할 때, 메모리(110)의 보안 저장 영역(130)을 확장하여 설정할 수 있다. 제1보안 모듈(160)은 보안 콘텐츠를 실행하는 동안에만 활성화되고, 보안 콘텐츠의 실행이 중단되거나, 종료되면 비활성화된다. 제1보안 모듈(160)은 비활성화 전에, 제2보안 모듈(150)에게 보안 저장 영역(130)에 대한 보호를 요청할 수 있다. 이에 따라 제2보안 모듈(150)은 보안 저장 영역(130)을 보호 영역으로 설정하여,

제1보안 모듈(160)이 비활성화 상태에서도 일반 모듈(170)이 보안 저장 영역(130)에 접근할 수 없게 한다. 또한 제1보안 모듈(160)의 제1보안 운영체제(161) 로딩을 위한 셋팅 데이터가, 제1보안 모듈(160)이 비활성된 상태에서도 보안 저장 영역(130) 상에 그대로 유지되게 함으로써, 제1보안 모듈(160)의 활성화/ 비활성화 스위칭 속도를 향상시킬 수 있다.

- [51] 제1보안 모듈(160)은 제2보안 모듈(150)과 보안 채널을 형성하여 통신하며, 보안 채널을 형성하기 위한 보안 채널 암호키는 전자 장치(100)의 부팅과정에서 제2보안 모듈(150)과 제1보안 모듈(160) 간에 공유될 수 있다.
- [52] 제1보안 모듈(160)은 새로운 보안 애플리케이션이 다운로드되면, 새로운 보안 애플리케이션으로부터 인증 정보를 추출하여, 보안 저장 영역(130)의 보안 애플리케이션 리스트에 저장함으로써, 보안 애플리케이션 리스트에 새로운 보안 애플리케이션을 등록할 수 있다. 제1보안 모듈(160)은 보안 애플리케이션 리스트 등록이 완료되면 새로운 보안 애플리케이션을 보안 저장 영역(130)에 저장하거나 설치할 수 있다. 보안 애플리케이션 등록시 이용되는 인증 정보는 보안 애플리케이션의 전자 서명, 개발자 식별 정보, 보안 애플리케이션 식별 정보, 버전 정보를 포함할 수 있다. 보안 애플리케이션 리스트에 저장된 인증 정보는 해당 보안 애플리케이션 실행시 보안 애플리케이션을 인증하는 정보로 이용될 수 있다.
- [53] 제2보안 모듈(150)은 제1보안 모듈(160)의 제1보안 운영체제(161)에 대한 해킹을 방지하여, 제1보안 모듈(160)을 보호할 수 있다. 전자 장치(100)의 전원이 온 되면, 일반 모듈(170) 및 제1보안 모듈(160)이 부팅되기 전에 제2보안 모듈(150)이 먼저 부팅된다. 제2보안 모듈은 부팅이 완료되면, 제1보안 모듈(160)의 제1보안 운영체제(161)의 무결성을 체크하고, 오류가 없다면 제1보안 모듈(160)의 부팅을 명령한다.
- [54] 그리고 제2보안 모듈(150)은 보안 저장부(152)를 포함할 수 있다. 보안 저장부(152)는 제1보안 모듈(160)의 제1보안 운영체제(161)에 대한 무결성 확인시 이용되는 정보와, 제2보안 모듈(150)과 제1보안 모듈(160)간의 보안 채널을 형성하는데 이용되는 보안 채널 암호키 생성을 위한 알고리즘을 저장한다. 그리고 보안 저장부(152)는 제1보안 모듈(160)에 의한 보안 콘텐츠 실행 중에 이용되거나 발생하는 데이터에 대한 암호화 및 복호를 위한 알고리즘을 저장한다.
- [55] 상기한 도1의 실시예에서, 제2보안 모듈(150)은 제어부(140)에 포함된 것으로 가정하였으나, 본 발명의 다른 실시예에 따라 제2보안 모듈(150)은 제어부(140)와 별도의 하드웨어 장치로 구현될 수도 있다. 이를 도2에 나타내었다. 도2는 본 발명의 다른 실시예에 따른 전자 장치(100)의 구성을 나타낸 도면이다. 도2와 같이, 제2보안 모듈(150)이 별도의 하드웨어 장치로 구현된다 해도, 제2보안 모듈(150)의 동작은 도1의 실시예와 유사할 것이며, 도2의 실시예에 따른 전자 장치(100)도 도3 내지 도6에 도시된 동작 과정을

수행할 수 있다.

- [56] 도3은 본 발명의 일 실시예에 따른 전자 장치(100)의 부팅 과정을 나타낸 도면이다. 도3을 참조하면, 전자 장치(100)의 전원이 온되면, 제2보안 모듈(150)은 201단계에서 부팅을 수행하고, 부팅이 완료되면 제1보안 모듈(160)의 제1보안 운영체제(161)의 무결성을 체크할 수 있다. 체크 결과, 이상이 없으면 205단계에서 제2보안 모듈(150)은 제1보안 모듈(160)에게 부팅 명령을 전달할 수 있다. 이에 따라, 제2보안 모듈(150)은 제1보안 모듈(160)에 대한 해킹 또는 악성 코드의 침입을 방지할 수 있다.
- [57] 제1보안 모듈(160)은 부팅 명령에 따라 207단계에서 부팅을 시작하고, 부팅이 완료되면 209단계에서 제2보안 모듈(150)에게 보안 채널 형성시 이용할 보안 채널 암호키 생성을 요청할 수 있다.
- [58] 암호키 생성 요청에 따라 제1보안 모듈(160)은 211단계에서 보안 저장부(152)에 저장된 보안 채널 암호키 생성 알고리즘을 이용해 보안 채널 암호키를 생성하고, 저장할 수 있다. 그리고 213단계에서 제2보안 모듈(150)은 보안 채널 암호키를 포함하는 보안 채널 암호키 생성 응답을 제1보안 모듈(160)로 전송한다. 제1보안 모듈(160)은 215단계에서 보안 채널 암호키를 저장할 수 있다. 이와 같이, 제2보안 모듈(150)과 제1보안 모듈(160)은 부팅 과정에서 보안 채널 암호키를 공유하고, 이후 보안 채널을 설정하여 통신을 수행함으로써 보안을 강화할 수 있다. 제1보안 모듈(160)은 219단계에서 제1보안 모듈(219)을 비활성화한다.
- [59] 217단계에서 제1보안 모듈(160)은 일반 모듈(170)에게 부팅을 요청할 수 있고, 221단계에서 일반 모듈(170)은 부팅을 수행한다.
- [60] 도4는 본 발명의 일 실시예에 따라, 새로운 보안 애플리케이션을 설치하는 과정을 나타낸 도면이다. 도4의 실시예에서, 제1보안 모듈(160)은 새로운 보안 애플리케이션의 저장 및 설치 요청을 수신하기 전에 비활성화 상태인 것으로 가정한다. 이에 따라, 보안 저장 영역(130)은 제2보안 모듈(150)에 의해 보호 영역으로 설정된 상태일 것이다.
- [61] 일반 모듈(170)은 새로운 애플리케이션을 다운로드하면, 새로운 애플리케이션이 보안 애플리케이션인지 비보안 애플리케이션인지 확인한다. 새로운 애플리케이션이 비보안 애플리케이션이라면 일반 모듈(170)은 비보안 저장 영역(130)에 비보안 애플리케이션을 저장하고, 설치할 수 있다. 만약, 새로운 애플리케이션이 보안 애플리케이션이라면, 도4의 301단계에서, 일반 모듈(170)은 제1보안 모듈(160)에게 새로운 애플리케이션에 대한 저장 및 설치를 요청할 수 있다. 이때, 제1보안 모듈(160)이 비활성화 상태라면, 303단계에서 제1보안 모듈(160)은 활성화하고, 305단계에서 제2보안 모듈(150)로 보안 저장 영역 보호 해제를 요청할 수 있다.
- [62] 제2보안 모듈(150)은 305단계의 요청에 따라, 307단계에서 보안 저장 영역에 대한 보호 영역 설정 해제한다. 그리고 309단계에서 제2보안 모듈(150)은

제1보안 모듈에게(160) 보안 영역 보호 해제 응답을 전송한다.

- [63] 제1보안 모듈(160)은 311단계에서 새로운 보안 애플리케이션의 인증 정보를 추출한다. 인증 정보는 예를 들어, 보안 애플리케이션의 개발자 식별 정보, 보안 애플리케이션 식별 정보, 전자 서명, 버전 정보 등을 포함할 수 있다. 제1보안 모듈(160)은 추출한 인증 정보를 보안 저장 영역(130)의 보안 애플리케이션 리스트에 저장하여, 새로운 애플리케이션을 보안 애플리케이션 리스트에 등록할 수 있다.
- [64] 그리고 313단계에서 제1보안 모듈(160)은 새로운 보안 애플리케이션을 보안 저장 영역(130) 저장하고, 설치할 수 있다. 새로운 보안 애플리케이션의 설치가 완료되고, 더 이상 보안 프로세스 수행 요청이 없으면 제1보안 모듈(160)은 제2보안모듈(150)에게 315단계에서 보안 저장 영역(130)에 대한 보호 영역 설정을 요청한다.
- [65] 315단계의 요청에 따라 제2보안 모듈(150)은 보안 저장 영역(130)을 보호 영역으로 설정하고, 319단계에서 보안 저장 영역 보호 응답을 제1보안 모듈(160)에게 전송한다.
- [66] 321단계에서 제1보안 모듈(160)은 비활성화한다.
- [67] 이에 따라, 제1보안 모듈(160)이 비활성화되더라도, 보안 저장 영역(130)은 제2보안 모듈(150)에 의해 보호받을 수 있으며, 일반 모듈(170)의 접근을 방지할 수 있다.
- [68] 도5는 본 발명의 일 실시예에 따라, 보안 애플리케이션을 실행하는 과정을 나타낸 도면이다. 도5의 실시예에서, 제1보안 모듈(160)은 보안 애플리케이션의 실행 요청을 수신하기 전에 비활성 상태인 것으로 가정한다. 이에 따라, 보안 저장 영역(130)은 제2보안 모듈(150)에 의해 보호 영역으로 설정된 상태일 것이다.
- [69] 일반 모듈(170)은 보안 애플리케이션의 실행 요청이 있으면, 도5의 401단계에서, 제1보안 모듈(160)에게 애플리케이션에 대한 실행을 요청할 수 있다. 이때, 제1보안 모듈(160)이 비활성화 상태라면, 403단계에서 제1보안 모듈(160)은 활성화하고, 405단계에서 제2보안 모듈(150)로 보안 저장 영역 보호 해제를 요청할 수 있다.
- [70] 제2보안 모듈(150)은 405단계의 요청에 따라, 407단계에서 보안 저장 영역에 대한 보호 영역 설정 해제한다. 그리고 409단계에서 제2보안 모듈(150)은 제1보안 모듈에게(160) 보안 영역 보호 해제 응답을 전송한다.
- [71] 제1보안 모듈(160)은 411단계에서 실행이 요청된 보안 애플리케이션의 인증 정보를 추출한다. 인증 정보는 예를 들어, 보안 애플리케이션의 개발자 식별 정보, 보안 애플리케이션 식별 정보, 전자 서명, 버전 정보 등을 포함할 수 있다. 413단계에서 제1보안 모듈(160)은 추출한 인증 정보와, 보안 저장 영역(130)의 보안 애플리케이션 리스트에 등록된 인증 정보와 비교하고, 일치하는 인증 정보가 보안 애플리케이션 리스트에 존재하면, 415단계에서 상기 보안

- 애플리케이션을 보안 저장 영역(130)에서 실행한다.
- [72] 417단계와 같이, 보안 애플리케이션을 실행하는 과정에 있어서 보안이 필요한 데이터가 발생하면, 제1보안 모듈(160)은 419단계에서 데이터 암호화 요청을 제2보안 모듈(150)로 전송한다. 이때, 제2보안 모듈(150)과 제1보안 모듈(160) 간에는 보안 채널이 형성된다. 데이터 암호화 요청은 암호화 대상이 되는 데이터와, 인증 정보가 포함될 수 있다. 상기 인증 정보는 보안 애플리케이션의 개발자 식별 정보와, 애플리케이션 식별 정보를 포함할 수 있다.
- [73] 421단계에서 제2보안 모듈(150)은 데이터 암호화 요청에 포함된 인증 정보를 이용해 암호키를 생성하고, 423단계에서 상기 암호키를 이용해 데이터 암호화 요청에 포함된 데이터를 암호화한다. 그리고 425단계에서 제2보안 모듈(150)은 제1보안 모듈(160)에게 암호화된 데이터를 전송한다. 암호화된 데이터 역시 보안 채널을 통해 전송된다.
- [74] 제1보안 모듈(160)은 427단계에서 암호화된 데이터를 보안 애플리케이션에 저장함으로써, 보안 애플리케이션에 대한 보호를 강화할 수 있다.
- [75] 이후, 429단계에서 보안 애플리케이션의 종료가 확인되면, 제1보안 모듈(160)은 제2보안모듈(150)에게 431단계에서 보안 저장 영역(130)에 대한 보호 영역 설정을 요청한다.
- [76] 431단계의 요청에 따라, 제2보안 모듈(150)은 433단계에서 보안 저장 영역(130)을 보호 영역으로 설정하고, 435단계에서 보안 저장 영역 보호 응답을 제1보안 모듈(160)에게 전송한다.
- [77] 437단계에서 제1보안 모듈(160)은 비활성화 한다.
- [78] 도6는 본 발명의 다른 실시예에 따라, 보안 애플리케이션 실행 과정에서 암호화된 데이터를 이용하는 경우의 동작과정을 나타낸 것이다. 도6의 실시예에서, 제1보안 모듈(160)은 보안 애플리케이션을 실행중인 것으로 가정한다.
- [79] 501단계와 같이 보안 애플리케이션을 실행하는 중에, 503단계에서 암호화된 데이터의 이용 요청이 발생하면, 제1보안 모듈(160)은 505단계에서 데이터 복호 요청을 제2보안 모듈(150)로 전송한다. 이때, 제2보안 모듈(150)과 제1보안 모듈(160) 간에는 보안 채널이 형성된다. 데이터 복호 요청은 암호화된 데이터와, 인증 정보가 포함될 수 있다. 상기 인증 정보는 보안 애플리케이션의 개발자 식별 정보와, 애플리케이션 식별 정보를 포함할 수 있다.
- [80] 507단계에서 제2보안 모듈(150)은 데이터 복호 요청에 포함된 인증 정보를 이용해 암호키를 생성하고, 509단계에서 상기 암호키를 이용해 데이터 복호 요청에 포함된 데이터를 복호한다. 그리고 511단계에서 제2보안 모듈(150)은 제1보안 모듈(160)에게 복호된 데이터를 전송한다. 복호된 데이터 역시 보안 채널을 통해 전송된다.
- [81] 제1보안 모듈(160)은 513단계에서 복호된 데이터를 이용할 수 있다.
- [82] 상기한 바와 같이, 본 발명은 제2보안 모듈(150)과 제1보안 모듈(160)을 이용해

- 이중으로 보안 콘텐츠를 보호함으로써, 보안 콘텐츠의 보안을 강화할 수 있다.
- [83] 도5 및 도6과 같이 보안 애플리케이션이 실행될 때의 상태를 도7에 도시하였다. 도7은 보안 저장 영역(130)에 제1보안 모듈(160)에 의해 보안 애플리케이션이 실행된 상태를 나타낸 도면이다.
- [84] 상기한 도5 및 도6의 실시예에서는 보안 애플리케이션의 실행 과정에서 생성된 데이터를 암호화하여 저장하기 위해, 또는 암호화된 데이터를 복호하기 위해, 제1보안 모듈(160)이 제2보안 모듈(150)로 해당 데이터(또는 암호화된 데이터)를 인증 정보와 함께 전송하였다. 하지만 본 발명의 다른 실시예에 따라, 제2보안 모듈(150)이 인증 정보를 이용해 생성한 암호키를 제1보안 모듈(160)로 전달하고, 제1보안 모듈(160)이 암호키를 저장하도록 구성할 수도 있다. 이 경우, 제1보안 모듈(160)은 암호키를 저장할 수 있는 보안 저장 영역을 포함하도록 구성될 수 있다.
- [85] 다시 말해, 제1보안 모듈(160)은 도5의 413단계에서 보안 애플리케이션의 인증이 완료되면, 제2보안 모듈(150)로 인증 정보(예를 들어, 보안 애플리케이션의 식별 정보, 개발자 식별 정보)를 포함하는 암호키 생성 요청을 보안 채널을 통해 제2보안 모듈(150)로 전송할 수 있다. 이에 따라, 제2보안 모듈(150)은 제1보안 모듈(150)로부터 수신한 인증 정보를 이용해 암호키를 생성하고, 보안 채널을 통해 암호키를 제1보안 모듈(160)로 전송한다. 제1보안 모듈(160)은 암호키를 보안 저장 영역에 저장한 후에 보안 애플리케이션을 실행 보안 저장 영역(130)에 실행한다. 그리고 보안 애플리케이션의 실행 과정에서 보안이 필요한 데이터가 발생하면 상기 암호키를 이용하여 데이터를 암호화한 후 보안 애플리케이션에 저장한다. 제1보안 모듈(160)은 암호화된 데이터의 복호 역시 보안 저장 영역에 저장하고 있던 암호키를 이용하여 수행할 수 있다.
- [86] 다른 예로, 제2보안 모듈(150)이 425단계에서 암호화된 데이터와 함께 암호키를 제1보안 모듈(160)로 전송하도록 구성할 수도 있다. 제1보안 모듈(160)은 암호키를 보안 저장 영역에 저장한 후에 추후 보안이 필요한 데이터가 발생하면 상기 암호키를 이용하여 데이터를 암호화할 수 있다. 그리고 제1보안 모듈(160)은 암호화된 데이터의 복호 역시 보안 저장 영역에 저장하고 있던 암호키를 이용하여 수행할 수 있다.
- [87] 도 8은 다양한 실시예에 따른 전자 장치(700)의 블록도이다. 전자 장치(700)는, 예를 들면, 도 1에 도시된 전자 장치(100)의 전체 또는 일부를 포함할 수 있다. 특히, 전자 장치(700)의 제어부(710)와 메모리(730)은 도1에 도시된 전자 장치(100)의 제어부(140)와, 메모리(110)와 유사하게 구현될 수 있다. 전자 장치(700)는 하나 이상의 프로세서(예: AP(application processor))를 포함하는 제어부(710), 통신 모듈(720), 가입자 식별 모듈(724), 메모리(730), 센서 모듈(740), 입력 장치(750), 디스플레이(760), 인터페이스(770), 오디오 모듈(780), 카메라 모듈(791), 전력 관리 모듈(795), 배터리(796), 인디케이터(797), 및 모터(798)를 포함할 수 있다.

- [88] 제어부(710)는, 예를 들면, 운영체제 또는 응용 프로그램을 구동하여 제어부(710)에 연결된 다수의 하드웨어 또는 소프트웨어 구성요소들을 제어할 수 있고, 각종 데이터 처리 및 연산을 수행할 수 있다. 제어부(710)는, 예를 들면, SoC(system on chip)로 구현될 수 있다. 한 실시예에 따르면, 제어부(710)는 GPU(graphic processing unit) 및/또는 이미지 신호 제어부(image signal processor)를 더 포함할 수 있다. 제어부(710)는 도 2에 도시된 구성요소들 중 적어도 일부(예: 셀룰러 모듈(721))를 포함할 수도 있다. 제어부(710)는 다른 구성요소들(예: 비휘발성 메모리) 중 적어도 하나로부터 수신된 명령 또는 데이터를 휘발성 메모리에 로드(load)하여 처리하고, 다양한 데이터를 비휘발성 메모리에 저장(store)할 수 있다.
- [89] 통신 모듈(720)은, 도 1의 통신 인터페이스(180)와 동일 또는 유사한 구성을 가질 수 있다. 통신 모듈(720)은, 예를 들면, 셀룰러 모듈(721), WiFi 모듈(723), 블루투스 모듈(725), GNSS 모듈(727)(예: GPS 모듈, Glonass 모듈, Beidou 모듈, 또는 Galileo 모듈), NFC 모듈(728) 및 RF(radio frequency) 모듈(729)를 포함할 수 있다.
- [90] 셀룰러 모듈(721)은, 예를 들면, 통신망을 통해서 음성 통화, 영상 통화, 문자 서비스, 또는 인터넷 서비스 등을 제공할 수 있다. 한 실시예에 따르면, 셀룰러 모듈(721)은 가입자 식별 모듈(예: SIM 카드)(724)을 이용하여 통신 네트워크 내에서 전자 장치(700)의 구별 및 인증을 수행할 수 있다. 한 실시예에 따르면, 셀룰러 모듈(721)은 제어부(710)가 제공할 수 있는 기능 중 적어도 일부 기능을 수행할 수 있다. 한 실시예에 따르면, 셀룰러 모듈(721)은 커뮤니케이션 제어부(CP: communication processor)를 포함할 수 있다.
- [91] WiFi 모듈(723), 블루투스 모듈(725), GNSS 모듈(727) 또는 NFC 모듈(728) 각각은, 예를 들면, 해당하는 모듈을 통해서 송수신되는 데이터를 처리하기 위한 제어부를 포함할 수 있다. 어떤 실시예에 따르면, 셀룰러 모듈(721), WiFi 모듈(723), 블루투스 모듈(725), GNSS 모듈(727) 또는 NFC 모듈(728) 중 적어도 일부(예: 두 개 이상)는 하나의 integrated chip(IC) 또는 IC 패키지 내에 포함될 수 있다.
- [92] RF 모듈(729)은, 예를 들면, 통신 신호(예: RF 신호)를 송수신할 수 있다. RF 모듈(729)은, 예를 들면, 트랜시버(transceiver), PAM(power amp module), 주파수 필터(frequency filter), LNA(low noise amplifier), 또는 안테나 등을 포함할 수 있다. 다른 실시예에 따르면, 셀룰러 모듈(721), WiFi 모듈(723), 블루투스 모듈(725), GNSS 모듈(727) 또는 NFC 모듈(728) 중 적어도 하나는 별개의 RF 모듈을 통하여 RF 신호를 송수신할 수 있다.
- [93] 가입자 식별 모듈(724)은, 예를 들면, 가입자 식별 모듈을 포함하는 카드 및/또는 내장 SIM(embedded SIM)을 포함할 수 있으며, 고유한 식별 정보(예: ICCID(integrated circuit card identifier) 또는 가입자 정보(예: IMSI(international mobile subscriber identity)))를 포함할 수 있다.

- [94] 메모리(730)(예: 메모리(140))는, 예를 들면, 휘발성 메모리(예: DRAM(dynamic RAM), SRAM(static RAM), 또는 SDRAM(synchronous dynamic RAM) 등), 비휘발성 메모리(non-volatile Memory)(예: OTPROM(one time programmable ROM), PROM(programmable ROM), EPROM(erasable and programmable ROM), EEPROM(electrically erasable and programmable ROM), mask ROM, flash ROM, 플래시 메모리(예: NAND flash 또는 NOR flash 등), 하드 드라이브, 또는 솔리드 스테이트 드라이브(solid state drive(SSD)) 중 적어도 하나를 포함할 수 있다.
- [95] 외장 메모리는 플래시 드라이브(flash drive), 예를 들면, CF(compact flash), SD(secure digital), Micro-SD(micro secure digital), Mini-SD(mini secure digital), xD(extreme digital), MMC(multi-media card) 또는 메모리 스틱(memory stick) 등을 더 포함할 수 있다. 외장 메모리는 다양한 인터페이스를 통하여 전자 장치(700)와 기능적으로 및/또는 물리적으로 연결될 수 있다.
- [96] 센서 모듈(740)은, 예를 들면, 물리량을 계측하거나 전자 장치(700)의 작동 상태를 감지하여, 계측 또는 감지된 정보를 전기 신호로 변환할 수 있다. 센서 모듈(740)은, 예를 들면, 제스처 센서(740A), 자이로 센서(740B), 기압 센서(740C), 마그네틱 센서(740D), 가속도 센서(740E), 그림 센서(740F), 근접 센서(740G), 컬러(color) 센서(740H)(예: RGB(red, green, blue) 센서), 생체 센서(740I), 온/습도 센서(740J), 조도 센서(740K), 또는 UV(ultra violet) 센서(740M) 중의 적어도 하나를 포함할 수 있다. 추가적으로 또는 대체적으로(additionally or alternatively), 센서 모듈(740)은, 예를 들면, 후각 센서(E-nose sensor), EMG 센서(electromyography sensor), EEG 센서(electroencephalogram sensor), ECG 센서(electrocardiogram sensor), IR(infrared) 센서, 홍채 센서 및/또는 지문 센서를 포함할 수 있다. 센서 모듈(740)은 그 안에 속한 적어도 하나 이상의 센서들을 제어하기 위한 제어 회로를 더 포함할 수 있다. 어떤 실시예에서는, 전자 장치(700)는 제어부(710)의 일부로서 또는 별도로, 센서 모듈(740)을 제어하도록 구성된 제어부를 더 포함하여, 제어부(710)가 슬립(sleep) 상태에 있는 동안, 센서 모듈(740)을 제어할 수 있다.
- [97] 입력 장치(750)는, 예를 들면, 터치 패널(touch panel)(752),(디지털) 펜 센서(pen sensor)(754), 키(key)(756), 또는 초음파(ultrasonic) 입력 장치(758)를 포함할 수 있다. 터치 패널(752)은, 예를 들면, 정전식, 감압식, 적외선 방식, 또는 초음파 방식 중 적어도 하나의 방식을 사용할 수 있다. 또한, 터치 패널(752)은 제어 회로를 더 포함할 수도 있다. 터치 패널(752)은 텍타일 레이어(tactile layer)를 더 포함하여, 사용자에게 촉각 반응을 제공할 수 있다.
- [98] (디지털) 펜 센서(754)는, 예를 들면, 터치 패널의 일부이거나, 별도의 인식용 쉬트(sheet)를 포함할 수 있다. 키(756)는, 예를 들면, 물리적인 버튼, 광학식 키, 또는 키패드를 포함할 수 있다. 초음파 입력 장치(758)는 마이크(예: 마이크(788))를 통해, 입력 도구에서 발생된 초음파를 감지하여, 상기 감지된 초음파에 대응하는 데이터를 확인할 수 있다.

- [99] 디스플레이(760)(예: 디스플레이(190))는 패널(762), 홀로그램 장치(764), 또는 프로젝터(766)를 포함할 수 있다. 패널(762)은, 도 1의 디스플레이(160)와 동일 또는 유사한 구성을 포함할 수 있다. 패널(762)은, 예를 들면, 유연하게(flexible), 투명하게(transparent), 또는 착용할 수 있게(wearable) 구현될 수 있다. 패널(762)은 터치 패널(752)과 하나의 모듈로 구성될 수도 있다. 홀로그램 장치(764)는 빛의 간섭을 이용하여 입체 영상을 허공에 보여줄 수 있다. 프로젝터(766)는 스크린에 빛을 투사하여 영상을 표시할 수 있다. 스크린은, 예를 들면, 전자 장치(700)의 내부 또는 외부에 위치할 수 있다. 한 실시예에 따르면, 디스플레이(760)는 패널(762), 홀로그램 장치(764), 또는 프로젝터(766)를 제어하기 위한 제어 회로를 더 포함할 수 있다.
- [100] 인터페이스(770)는, 예를 들면, HDMI(high-definition multimedia interface)(772), USB(universal serial bus)(774), 광 인터페이스(optical interface)(776), 또는 D-sub(D-subminiature)(778)를 포함할 수 있다. 인터페이스(770)는, 예를 들면, 도 1에 도시된 통신 인터페이스(180)에 포함될 수 있다. 추가적으로 또는 대체적으로(additionally and alternatively), 인터페이스(770)는, 예를 들면, MHL(mobile high-definition link) 인터페이스, SD(secure digital) 카드/MMC(multi-media card) 인터페이스, 또는 IrDA(infrared data association) 규격 인터페이스를 포함할 수 있다.
- [101] 오디오 모듈(780)은, 예를 들면, 소리(sound)와 전기 신호를 쌍방향으로 변환시킬 수 있다. 오디오 모듈(780)의 적어도 일부 구성요소는, 예를 들면, 도 1에 도시된 입출력 인터페이스(145)에 포함될 수 있다. 오디오 모듈(780)은, 예를 들면, 스피커(782), 리시버(784), 이어폰(786), 또는 마이크(788) 등을 통해 입력 또는 출력되는 소리 정보를 처리할 수 있다.
- [102] 카메라 모듈(791)은, 예를 들면, 정지 영상 및 동영상을 촬영할 수 있는 장치로서, 한 실시예에 따르면, 하나 이상의 이미지 센서(예: 전면 센서 또는 후면 센서), 렌즈, ISP(image signal processor), 또는 플래시(flash)(예: LED 또는 xenon lamp 등)를 포함할 수 있다.
- [103] 전력 관리 모듈(795)은, 예를 들면, 전자 장치(700)의 전력을 관리할 수 있다. 한 실시예에 따르면, 전력 관리 모듈(795)은 PMIC(power management integrated circuit), 충전 IC(charger integrated circuit), 또는 배터리 또는 연료 게이지(battery or fuel gauge)를 포함할 수 있다. PMIC는, 유선 및/또는 무선 충전 방식을 가질 수 있다. 무선 충전 방식은, 예를 들면, 자기공명 방식, 자기유도 방식 또는 전자기파 방식 등을 포함하며, 무선 충전을 위한 부가적인 회로, 예를 들면, 코일 루프, 공진 회로, 또는 정류기 등을 더 포함할 수 있다. 배터리 게이지는, 예를 들면, 배터리(796)의 잔량, 충전 중 전압, 전류, 또는 온도를 측정할 수 있다. 배터리(796)는, 예를 들면, 충전식 전지(rechargeable battery) 및/또는 태양 전지(solar battery)를 포함할 수 있다.
- [104] 인디케이터(797)는 전자 장치(700) 또는 그 일부(예: 제어부(710))의 특정 상태,

예를 들면, 부팅 상태, 메시지 상태 또는 충전 상태 등을 표시할 수 있다. 모터(798)는 전기적 신호를 기계적 진동으로 변환할 수 있고, 진동(vibration), 또는 햅틱(haptic) 효과 등을 발생시킬 수 있다. 도시되지는 않았으나, 전자 장치(700)는 모바일 TV 지원을 위한 처리 장치(예: GPU)를 포함할 수 있다. 모바일 TV 지원을 위한 처리 장치는, 예를 들면, DMB(digital multimedia broadcasting), DVB(digital video broadcasting), 또는 미디어플로(mediaFlo™) 등의 규격에 따른 미디어 데이터를 처리할 수 있다.

- [105] 본 문서에서 기술된 구성요소들 각각은 하나 또는 그 이상의 부품(component)으로 구성될 수 있으며, 해당 구성요소의 명칭은 전자 장치의 종류에 따라서 달라질 수 있다. 다양한 실시예에서, 전자 장치는 본 문서에서 기술된 구성요소 중 적어도 하나를 포함하여 구성될 수 있으며, 일부 구성요소가 생략되거나 또는 추가적인 다른 구성요소를 더 포함할 수 있다. 또한, 다양한 실시예에 따른 전자 장치의 구성요소들 중 일부가 결합되어 하나의 개체(entity)로 구성됨으로써, 결합되기 이전의 해당 구성요소들의 기능을 동일하게 수행할 수 있다.
- [106] 본 문서에서 사용된 용어 "모듈"은, 예를 들면, 하드웨어, 소프트웨어 또는 펌웨어(firmware) 중 하나 또는 둘 이상의 조합을 포함하는 단위(unit)를 의미할 수 있다. "모듈"은, 예를 들면, 유닛(unit), 로직(logic), 논리 블록(logical block), 부품(component), 또는 회로(circuit) 등의 용어와 바꾸어 사용(interchangeably use)될 수 있다. "모듈"은, 일체로 구성된 부품의 최소 단위 또는 그 일부가 될 수 있다. "모듈"은 하나 또는 그 이상의 기능을 수행하는 최소 단위 또는 그 일부가 될 수도 있다. "모듈"은 기계적으로 또는 전자적으로 구현될 수 있다. 예를 들면, "모듈"은, 알려졌거나 앞으로 개발될, 어떤 동작들을 수행하는 ASIC(application-specific integrated circuit) 칩, FPGAs(field-programmable gate arrays) 또는 프로그램 가능 논리 장치(programmable-logic device) 중 적어도 하나를 포함할 수 있다.
- [107] 다양한 실시예에 따른 장치(예: 모듈들 또는 그 기능들) 또는 방법(예: 동작들)의 적어도 일부는, 예컨대, 프로그램 모듈의 형태로 컴퓨터로 읽을 수 있는 저장매체(computer-readable storage media)에 저장된 명령어로 구현될 수 있다. 상기 명령어가 제어부(예: 제어부(140))에 의해 실행될 경우, 상기 하나 이상의 제어부가 상기 명령어에 해당하는 기능을 수행할 수 있다. 컴퓨터로 읽을 수 있는 저장매체는, 예를 들면, 메모리(110)가 될 수 있다.
- [108] 컴퓨터로 판독 가능한 기록 매체는, 하드디스크, 플로피디스크, 마그네틱 매체(magnetic media)(예: 자기테이프), 광기록 매체(optical media)(예: CD-ROM(compact disc read only memory), DVD(digital versatile disc), 자기-광 매체(magneto-optical media)(예: 플롭티컬 디스크(floptical disk)), 하드웨어 장치(예: ROM(read only memory), RAM(random access memory), 또는 플래시 메모리 등) 등을 포함할 수 있다. 또한, 프로그램 명령에는 컴파일러에 의해

만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 상술한 하드웨어 장치는 다양한 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지다.

- [109] 다양한 실시예에 따른 모듈 또는 프로그램 모듈은 전술한 구성요소들 중 적어도 하나 이상을 포함하거나, 일부가 생략되거나, 또는 추가적인 다른 구성요소를 더 포함할 수 있다. 다양한 실시예에 따른 모듈, 프로그램 모듈 또는 다른 구성요소에 의해 수행되는 동작들은 순차적, 병렬적, 반복적 또는 휴리스틱(heuristic)한 방법으로 실행될 수 있다. 또한, 일부 동작은 다른 순서로 실행되거나, 생략되거나, 또는 다른 동작이 추가될 수 있다. 그리고 본 문서에 개시된 실시예는 개시된, 기술 내용의 설명 및 이해를 위해 제시된 것이며, 본 문서에서 기재된 기술의 범위를 한정하는 것은 아니다. 따라서, 본 문서의 범위는, 본 문서의 기술적 사상에 근거한 모든 변경 또는 다양한 다른 실시예를 포함하는 것으로 해석되어야 한다.

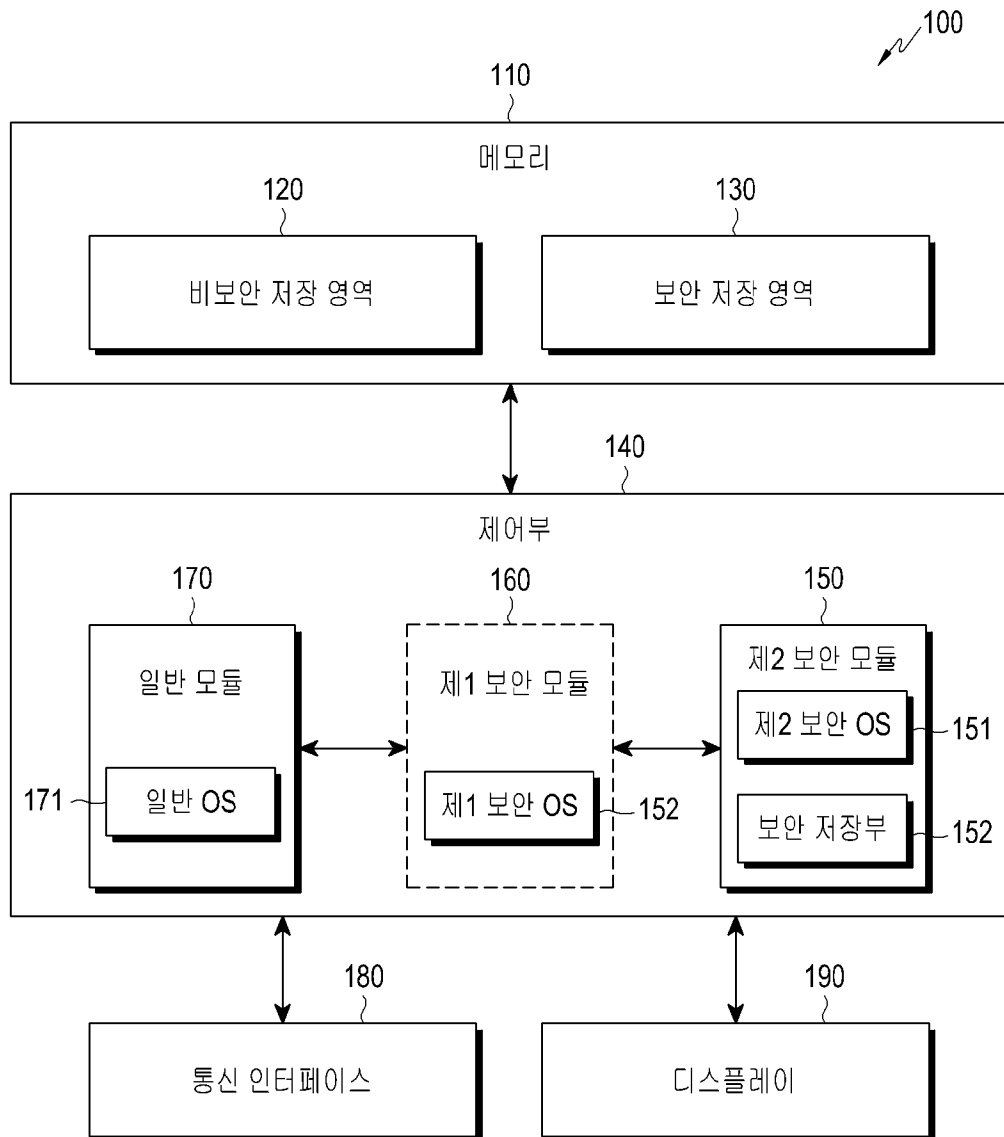
청구범위

- [청구항 1] 전자 장치의 애플리케이션 보호 방법에 있어서,
메모리의 보안 저장 영역에서, 제1보안 모듈에 의해, 보안 애플리케이션이 실행됨에 따라 보안이 필요한 데이터가 생성되면, 상기 제1보안 모듈이 제2보안 모듈에게 데이터 암호화 요청을 전송하는 과정과,
상기 제2보안 모듈이 상기 데이터 암호화 요청에 포함된 인증 정보를 이용해 암호키를 생성하고, 상기 데이터 암호화 요청에 포함된 상기 데이터를 상기 암호키를 이용해 암호화하는 과정과,
상기 제2보안 모듈이 상기 암호화된 데이터를 상기 제1보안 모듈로 전달하는 과정과,
상기 제1보안 모듈이 상기 암호화된 데이터를 상기 보안 애플리케이션에 저장하는 과정을 포함함을 특징으로 하는 콘텐츠 보호 방법.
- [청구항 2] 제1항에 있어서, 상기 보안 애플리케이션이 종료되면, 상기 제1보안 모듈은 상기 제2보안 모듈에게 상기 보안 저장 영역에 대한 보호를 요청하는 과정과,
상기 제2보안 모듈이 상기 보안 저장 영역을 보호 영역으로 설정하는 과정과,
상기 제1보안 모듈이 턴 오프하는 과정을 더 포함하며,
상기 제1보안 모듈에서 제1보안 운영체제(Secure Operating System)가 실행되고, 상기 제2보안 모듈에서 제2보안 운영체제가 실행되고, 일반 운영체제가 실행되는 일반 모듈의 상기 보안 저장 영역의 접근이 금지됨을 특징으로 하는 콘텐츠 보호 방법.
- [청구항 3] 제2항에 있어서, 상기 제1보안 모듈이 턴 오프된 상태에서, 상기 보안 애플리케이션의 실행이 요청되면, 상기 제1보안 모듈이 턴 온하는 과정과,
상기 제1보안 모듈이 상기 제2보안 모듈에게 상기 보안 저장 영역에 대한 보호 영역 설정 해제를 요청하는 과정과,
상기 제2보안 모듈이 상기 보안 저장 영역에 대한 보호 영역 설정을 해제하는 과정과,
상기 제1보안 모듈이 상기 보안 애플리케이션을 인증하고, 상기 보안 저장 영역에서 실행하는 과정을 더 포함함을 특징으로 하는 콘텐츠 보호 방법.
- [청구항 4] 제3항에 있어서, 상기 제1보안 모듈이 상기 보안 애플리케이션을 인증하는 과정은
상기 보안 애플리케이션의 인증 정보와, 상기 보안 저장 영역에 저장된 보안 애플리케이션 리스트에 등록된 인증 정보를 비교하는 과정임을

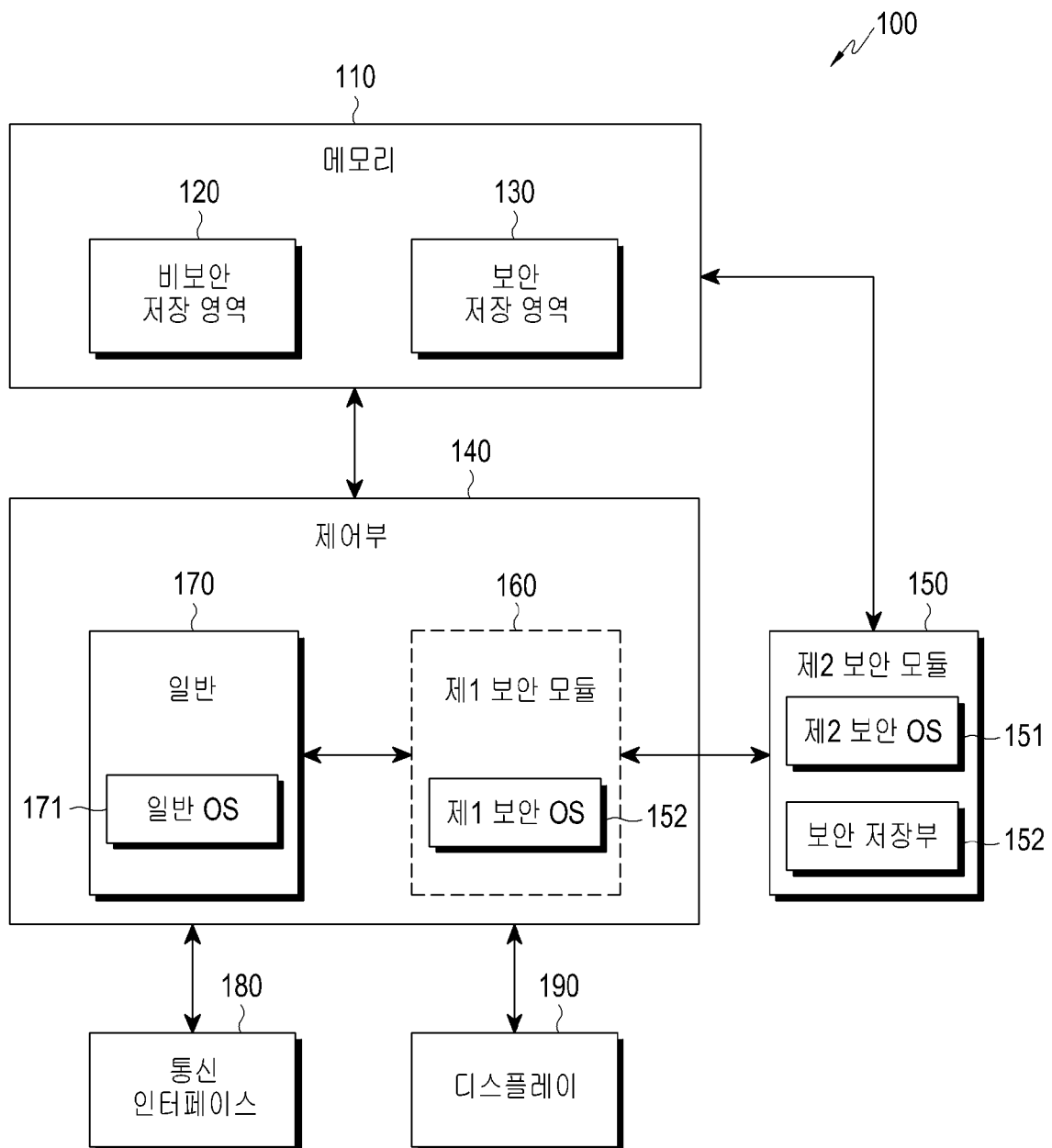
- 특징으로 하는 콘텐츠 보호 방법.
- [청구항 5] 제4항에 있어서, 상기 전자 장치의 전원이 온되면, 상기 제1보안 모듈이 부팅되고, 상기 제1보안 모듈이 상기 제2보안 모듈의 상기 제2보안 운영체제의 무결성을 체크한 후에 상기 제2보안 모듈로 부팅 명령을 전송함을 특징으로 하는 콘텐츠 보호 방법.
- [청구항 6] 제5항에 있어서, 상기 제1보안 모듈과 상기 제2보안 모듈의 부팅 과정에서 상기 제1보안 모듈과 상기 제2보안 모듈 간에 보안 채널을 형성을 위한 보안 채널 암호키가 공유됨을 특징으로 하는 콘텐츠 보호 방법.
- [청구항 7] 제6항에 있어서, 상기 제2보안 모듈은 상기 보안 채널 암호키 생성에 이용되는 알고리즘과, 상기 데이터 암호화에 이용되는 상기 암호키 생성에 이용되는 알고리즘을 저장하는 보안 저장부를 포함함을 특징으로 하는 콘텐츠 보호 방법.
- [청구항 8] 전자 장치에 있어서,
메모리와,
제어부를 포함하며,
상기 제어부는 상기 메모리의 보안 저장 영역에서 보안 애플리케이션을 실행하고, 상기 보안 애플리케이션의 실행에 따라 보안이 필요한 데이터가 생성되면, 제2보안 모듈에게 데이터 암호화 요청을 전송하는 제1보안 모듈과,
상기 데이터 암호화 요청에 포함된 인증 정보를 이용해 암호키를 생성하고, 상기 데이터 암호화 요청에 포함된 상기 데이터를 상기 암호키를 이용해 암호화하고, 상기 암호화된 데이터를 상기 제1보안 모듈로 전달하는 상기 제2보안 모듈을 포함하며,
상기 제1보안 모듈은 상기 암호화된 데이터를 상기 보안 애플리케이션에 저장함을 포함함을 특징으로 하는 전자 장치.
- [청구항 9] 제8항에 있어서,
상기 제1보안 모듈에서 제1보안 운영체제(Secure Operating System)가 실행되고, 상기 제1보안 모듈은 상기 보안 애플리케이션이 종료되면, 상기 제1보안 모듈은 상기 제2보안 모듈에게 상기 보안 저장 영역에 대한 보호를 요청한 후에 턴 오프하고,
상기 제2보안 모듈에서 제2보안 운영체제가 실행되고, 상기 제2보안 모듈은 상기 보호 요청에 따라, 상기 보안 저장 영역을 보호 영역으로 설정하고,
일반 운영체제가 실행되는 일반 모듈의 상기 보안 저장 영역의 접근이 금지됨을 특징으로 하는 전자 장치.
- [청구항 10] 제9항에 있어서, 상기 제1보안 모듈이 턴 오프된 상태에서, 상기 보안 애플리케이션의 실행이 요청되면, 상기 제1보안 모듈이 턴 온하고, 상기

- 제1보안 모듈이 상기 제2보안 모듈에게 상기 보안 저장 영역에 대한 보호 영역 설정 해제를 요청하고, 상기 제2보안 모듈에 의해 상기 보안 저장 영역에 대한 보호 영역 설정이 해제되면, 상기 보안 애플리케이션을 인증하고, 상기 보안 저장 영역에서 실행함을 특징으로 하는 전자 장치.
- [청구항 11] 제10항에 있어서, 상기 제1보안 모듈은 상기 보안 애플리케이션의 인증 정보와, 상기 보안 저장 영역에 저장된 보안 애플리케이션 리스트에 등록된 인증 정보를 비교하여, 상기 보안 애플리케이션을 인증함을 특징으로 하는 전자 장치.
- [청구항 12] 제11항에 있어서, 상기 전자 장치의 전원이 온되면, 상기 제1보안 모듈이 부팅되고, 상기 제1보안 모듈이 상기 제2보안 모듈의 상기 제2보안 운영체제의 무결성을 체크한 후에 상기 제2보안 모듈로 부팅 명령을 전송함을 특징으로 하는 전자 장치.
- [청구항 13] 제12항에 있어서, 상기 제1보안 모듈과 상기 제2보안 모듈의 부팅 과정에서 상기 제1보안 모듈과 상기 제2보안 모듈 간에 보안 채널을 형성을 위한 보안 채널 암호키가 공유됨을 특징으로 하는 전자 장치.
- [청구항 14] 제13항에 있어서, 상기 제2보안 모듈은 상기 보안 채널 암호키 생성에 이용되는 알고리즘과, 상기 데이터 암호화에 이용되는 상기 암호키 생성에 이용되는 알고리즘을 저장하는 보안 저장부를 포함함을 특징으로 하는 전자 장치.

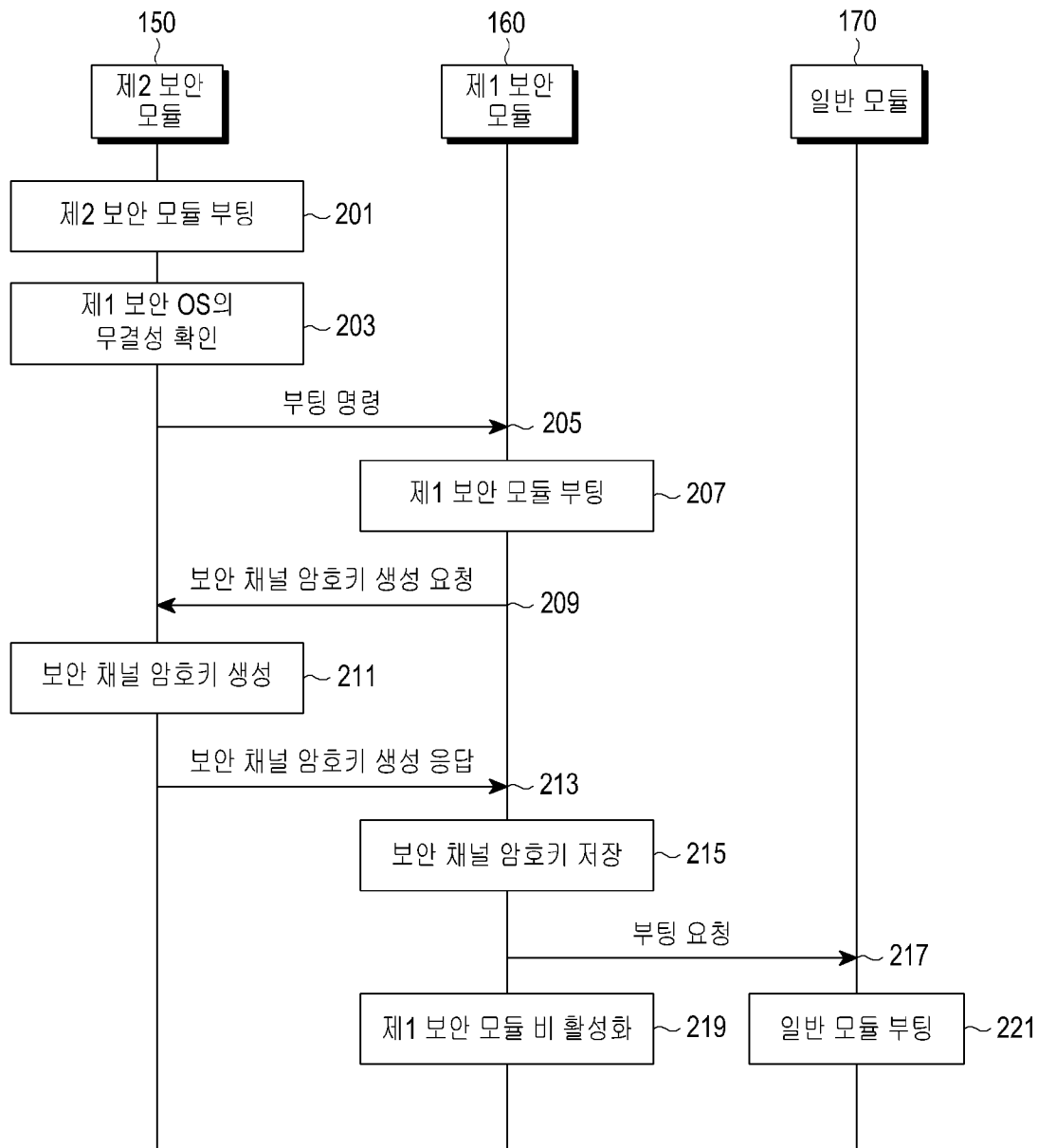
[도 1]



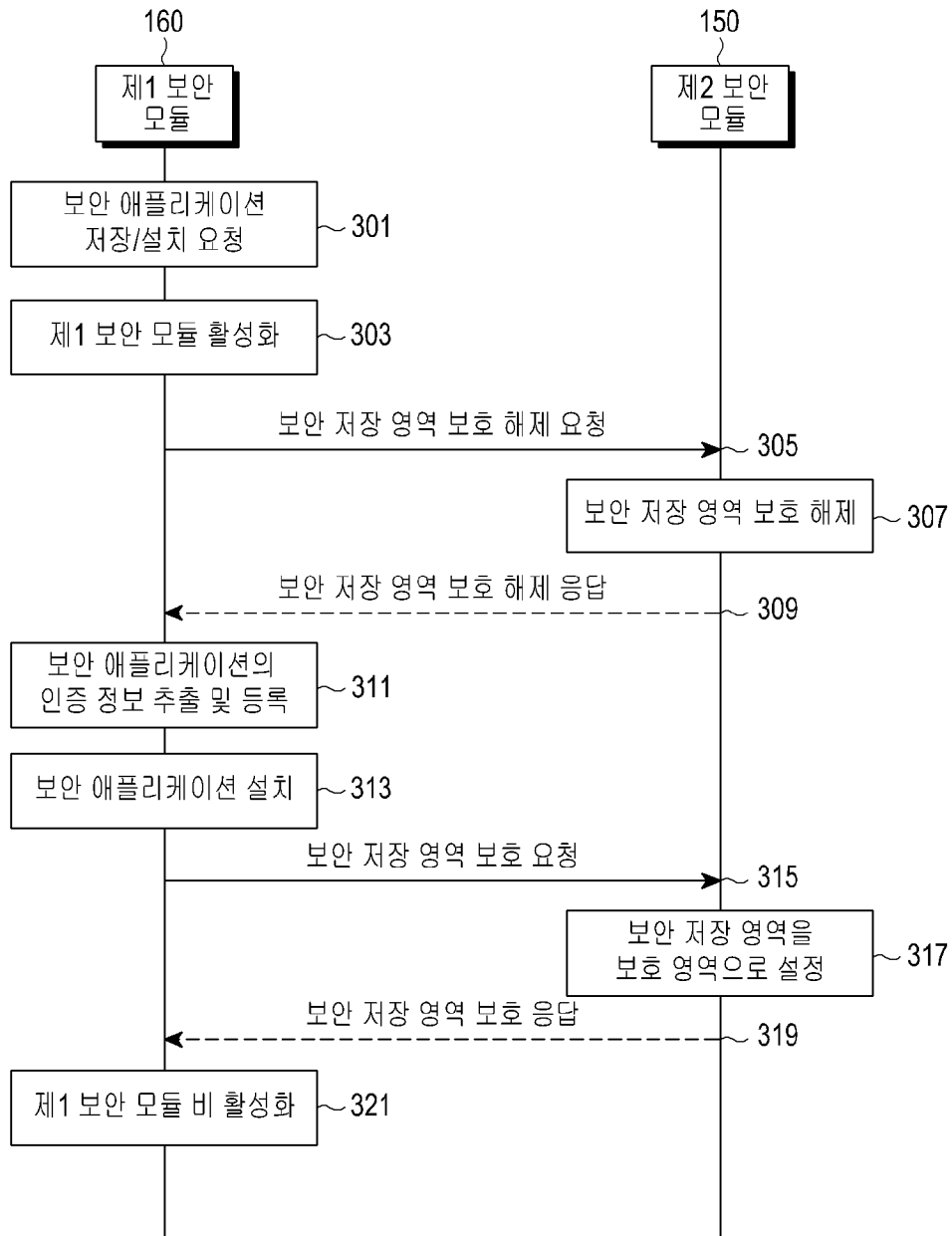
[도2]



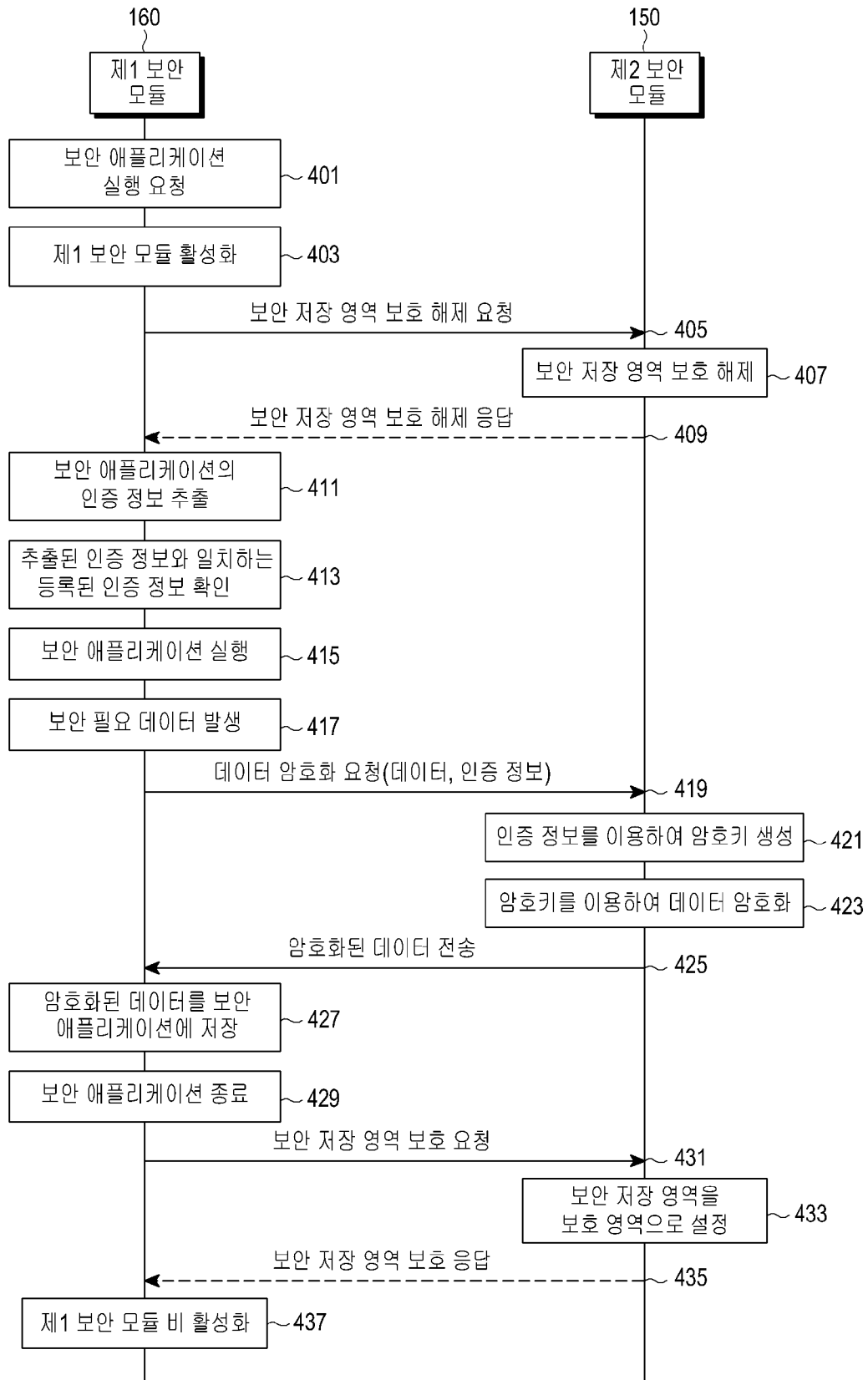
[도3]



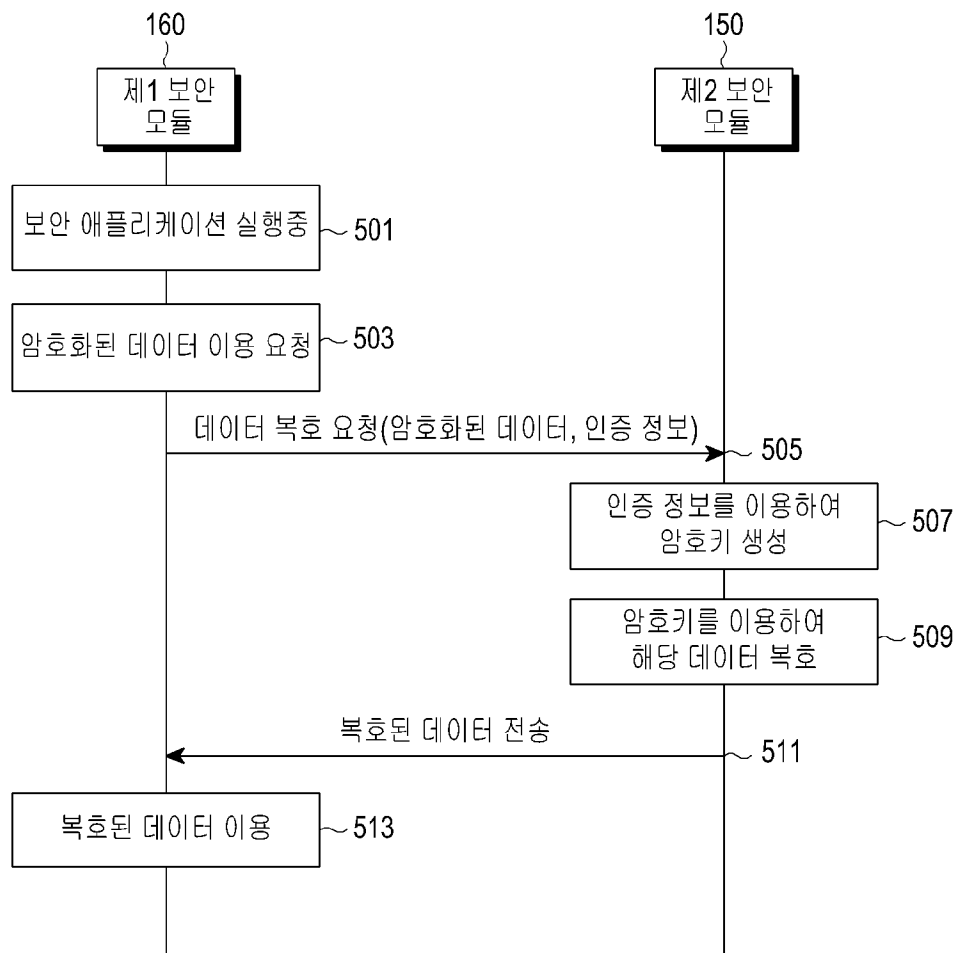
[도4]



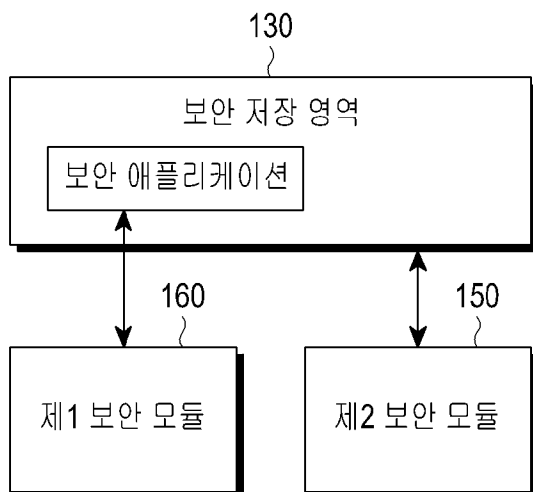
[도5]



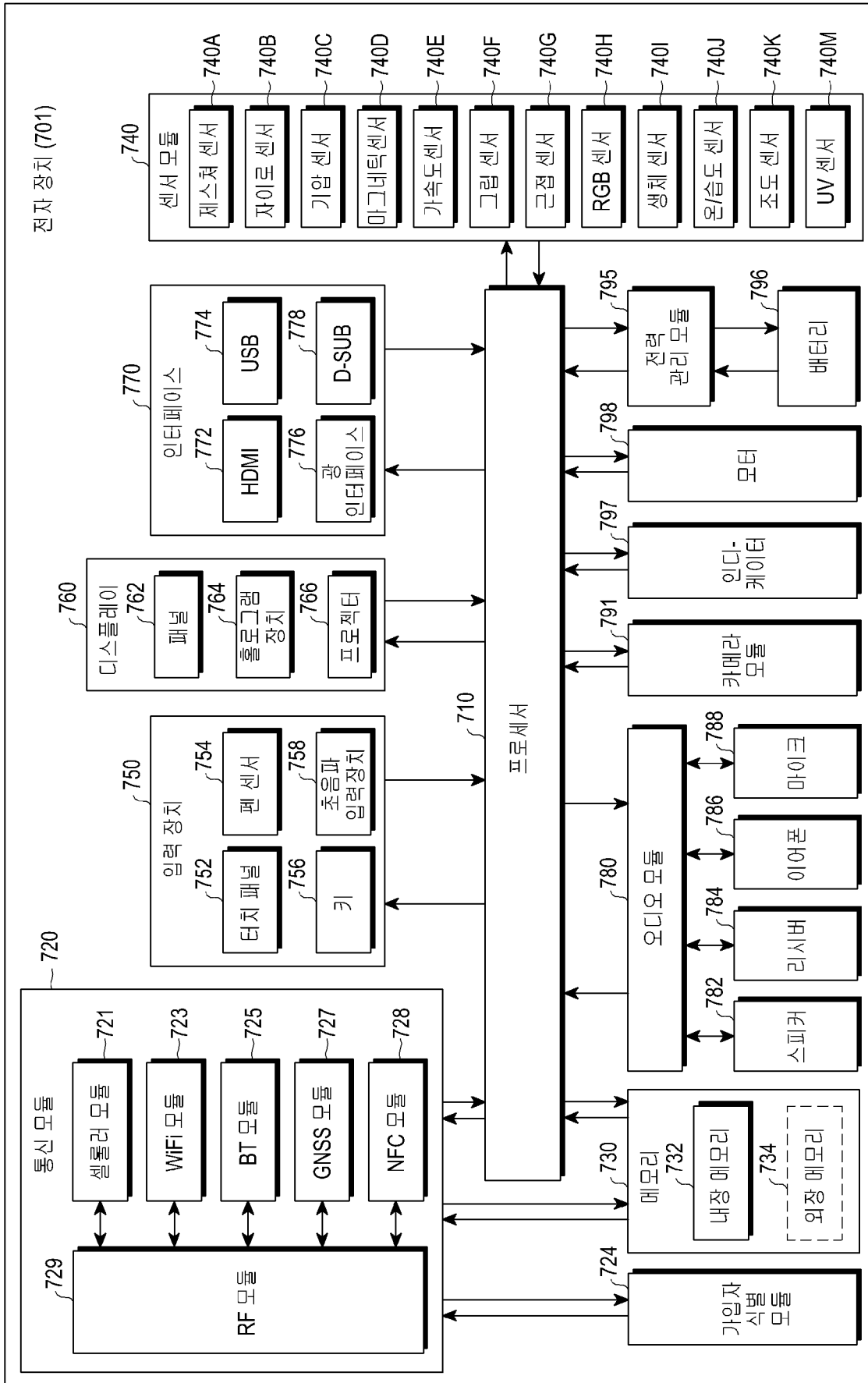
[도6]



[도7]



[도8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2016/002605

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/10(2013.01)i, G06F 21/60(2013.01)i, H04L 9/08(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 21/10; H04L 9/14; G06F 21/56; G06F 21/62; H04L 29/06; G06F 9/455; G06F 21/60; H04L 9/08

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: application, secure operating system, contents protection, security module, encoding

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014-0282543 A1 (OLOGN TECHNOLOGIES AG.) 18 September 2014 See paragraphs [0015], [0020], [0063]-[0076]; claim 21 and figures 1, 4A-5.	1-14
Y	KR 10-2014-0044972 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 16 April 2014 See paragraphs [0019]-[0026]; and figure 1.	1-14
Y	KR 10-1317496 B1 (CHOU, Che - Yang) 21 November 2013 See paragraph [0041]; and figures 1-4.	6-7,13-14
A	US 2014-0337918 A1 (SIDDIQI, Faraz A. et al.) 13 November 2014 See paragraphs [0017]-[0033]; and figures 1-7.	1-14
A	US 2014-0053245 A1 (TOSA, Raul V. et al.) 20 February 2014 See paragraphs [0030]-[0044]; and figures 3-6.	1-14



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

“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

28 JUNE 2016 (28.06.2016)

Date of mailing of the international search report

29 JUNE 2016 (29.06.2016)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2016/002605

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2014-0282543 A1	18/09/2014	NONE	
KR 10-2014-0044972 A	16/04/2014	US 2014-0082690 A1 US 9239934 B2	20/03/2014 19/01/2016
KR 10-1317496 B1	21/11/2013	EP 2398208 A3 JP 2012-005129 A US 2011-0314284 A1	11/03/2015 05/01/2012 22/12/2011
US 2014-0337918 A1	13/11/2014	CN 105122260 A EP 2973171 A1 KR 10-2015-0106937 A WO 2014-142904 A1	02/12/2015 20/01/2016 22/09/2015 18/09/2014
US 2014-0053245 A1	20/02/2014	US 2014-0137115 A1 US 8656482 B1	15/05/2014 18/02/2014

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/10(2013.01)i, G06F 21/60(2013.01)i, H04L 9/08(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/10; H04L 9/14; G06F 21/56; G06F 21/62; H04L 29/06; G06F 9/455; G06F 21/60; H04L 9/08

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: 어플리케이션, 보안 운영체제, 콘텐츠 보호, 보안 모듈, 암호화

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	US 2014-0282543 A1 (OLOGN TECHNOLOGIES AG.) 2014.09.18 단락 [0015], [0020], [0063]- [0076]; 청구항 21 및 도면 1, 4A-5 참조.	1-14
Y	KR 10-2014-0044972 A (한국전자통신연구원) 2014.04.16 단락 [0019]-[0026]; 및 도면 1 참조.	1-14
Y	KR 10-1317496 B1 (초우 체-양) 2013.11.21 단락 [0041]; 및 도면 1-4 참조.	6-7, 13-14
A	US 2014-0337918 A1 (FARAZ A. SIDDIQI 등) 2014.11.13 단락 [0017]-[0033]; 및 도면 1-7 참조.	1-14
A	US 2014-0053245 A1 (RAUL V. TOSA 등) 2014.02.20 단락 [0030]-[0044]; 및 도면 3-6 참조.	1-14

☐ 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

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2016년 06월 28일 (28.06.2016)

국제조사보고서 발송일

2016년 06월 29일 (29.06.2016)

ISA/KR의 명칭 및 우편주소

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

팩스 번호 +82-42-481-8578

심사관

김기호

전화번호 +82-42-481-8691



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2014-0282543 A1	2014/09/18	없음	
KR 10-2014-0044972 A	2014/04/16	US 2014-0082690 A1 US 9239934 B2	2014/03/20 2016/01/19
KR 10-1317496 B1	2013/11/21	EP 2398208 A3 JP 2012-005129 A US 2011-0314284 A1	2015/03/11 2012/01/05 2011/12/22
US 2014-0337918 A1	2014/11/13	CN 105122260 A EP 2973171 A1 KR 10-2015-0106937 A WO 2014-142904 A1	2015/12/02 2016/01/20 2015/09/22 2014/09/18
US 2014-0053245 A1	2014/02/20	US 2014-0137115 A1 US 8656482 B1	2014/05/15 2014/02/18