(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0098075
(43) 공개일자 2015년08월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/83 (2013.01) *G06F 3/00* (2006.01)
G06F 9/06 (2006.01) *G06F 9/54* (2006.01)
(21) 출원번호 10-2014-0019186
(22) 출원일자 2014년02월19일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
유희준
서울특별시 양천구 신월로15길 25 신월대성유니드아파트 105동 601호
김태호
서울특별시 마포구 와우산로32길 5-5 201호
(뒷면에 계속)
(74) 대리인
윤동열

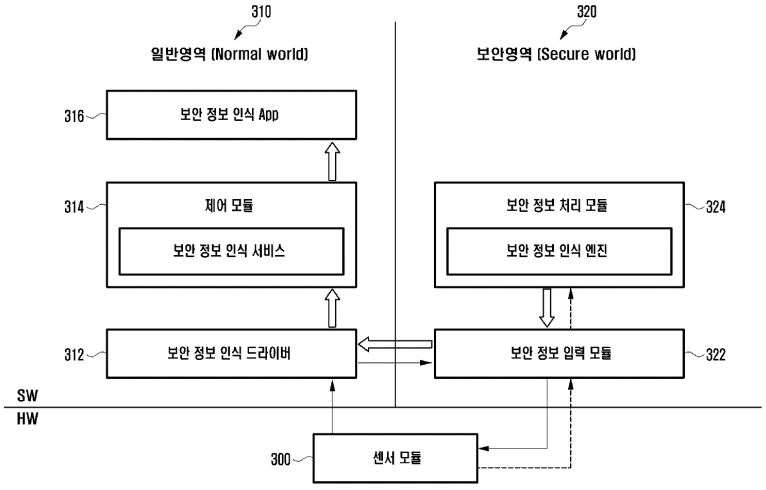
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **전자 장치의 보안 정보 입출력 방법 및 이를 사용하는 전자 장치**

(57) 요 약

전자 장치에 보안 정보(Security information)를 입력하는 방법에 있어서, 센서 모듈를 이용하여 보안 정보 입력 동작을 감지하는 동작; 상기 보안 정보 입력 동작에 대응하여 인터럽트(Interrupt)를 발생시키는 동작; 및 보안 정보 입력 모듈을 이용하여 상기 인터럽트에 대응하는 상기 보안 정보를 읽는 동작을 포함한다.

대 표 도



(72) 발명자

김형준

경기도 화성시 메타폴리스로 6 시범다은마을삼성래미안아파트 309동 802호

박슬한

경기도 용인시 기흥구 덕영대로2077번길 20 신일아파트 109동 1306호

박종훈

경기도 수원시 영통구 매탄로126번길 66 주공그린빌아파트 202동 1703호

안태인

경기도 화성시 동탄중앙로 189 시범다은마을월드메르디앙반도유보라아파트 343동 802호

이양수

경기도 용인시 수지구 죽전로 267 건영캐스빌아파트 705동 104호

장문수

경기도 수원시 영통구 인계로189번길 14 주공4단지아파트 410동 510호

현진호

경기도 용인시 수지구 풍덕천로 17 진흥아파트 625동 1203호

김승환

경기도 용인시 기흥구 보정로 91 현대아이파크1차아파트 206동 1106호

특허청구의 범위

청구항 1

전자 장치에 보안 정보(Security information)를 입력하는 방법에 있어서,

센서 모듈을 이용하여 보안 정보 입력 동작을 감지하는 동작;

상기 보안 정보 입력 동작에 대응하여 인터럽트(Interrupt)를 발생시키는 동작; 및

보안 정보 입력 모듈을 이용하여 상기 인터럽트에 대응하여 상기 보안 정보를 읽는 동작을 포함하는 전자 장치의 보안 정보 입력 방법.

청구항 2

제 1항에 있어서,

상기 보안 정보 입력 모듈은 보안 영역(Secure World) 내에 위치하는 것을 특징으로 하는 전자 장치의 보안 정보 입력 방법.

청구항 3

제 2항에 있어서,

상기 인터럽트를 일반 영역(Normal World) 내 보안 정보 인식 드라이버로 전달하는 동작; 및

상기 인터럽트를 상기 보안 정보 입력 모듈로 전달하는 동작을 더 포함하는 전자 장치의 보안 정보 입력 방법.

청구항 4

제 2항에 있어서,

상기 인터럽트를 상기 보안 정보 입력 모듈로 전달하는 동작을 더 포함하는 전자 장치의 보안 정보 입력 방법.

청구항 5

제 3항에 있어서,

상기 보안 정보를 보안 정보 처리 모듈로 전달하는 동작을 더 포함하는 전자 장치의 보안 정보 입력 방법.

청구항 6

제 5항에 있어서,

상기 보안 정보 처리 모듈은 보안 영역(Secure World) 내에 위치하는 것을 특징으로 하는 전자 장치의 보안 정보 입력 방법.

청구항 7

제 5항에 있어서,

상기 보안 정보 처리 모듈은 일반 영역(Normal World) 내에 위치하는 것을 특징으로 하는 전자 장치의 보안 정

보 입력 방법.

청구항 8

제 1항에 있어서,

상기 보안 정보는 지문 정보, 홍채 정보, 안면 정보, 음성 정보, 정맥 정보 및 서명 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 전자 장치의 보안 정보 입력 방법.

청구항 9

제 2항에 있어서,

상기 보안 정보 입력 동작을 감지하기 위한 신호를 수신하는 동작을 포함하고,

상기 신호는 키 또는 터치 입력, 음성 입력 및 제스처 입력 중 적어도 하나에 대응하는 것을 특징으로 하는 전자 장치의 보안 정보 입력 방법.

청구항 10

센서 모듈; 및

프로세서를 포함하며,

상기 프로세서는 상기 센서 모듈을 이용하여 보안 정보 입력 동작을 감지하고, 상기 보안 정보 입력 동작에 대응하여 인터럽트(Interrupt)를 발생시키고, 보안 정보 입력 모듈을 이용하여 상기 인터럽트에 대응하는 상기 보안 정보를 읽는 전자 장치.

청구항 11

제 10항에 있어서,

상기 보안 정보 입력 모듈은 보안 영역(Secure World) 내에 위치하는 것을 특징으로 하는 전자 장치.

청구항 12

제 11항에 있어서,

상기 프로세서는 상기 인터럽트를 일반 영역(Normal World) 내 보안 정보 인식 드라이버로 전달하고, 상기 인터럽트를 상기 보안 정보 입력 모듈로 전달하는 전자 장치.

청구항 13

제 11항에 있어서,

상기 프로세서는 상기 인터럽트를 상기 보안 정보 입력 모듈로 전달하는 전자 장치.

청구항 14

제 12항에 있어서,

상기 프로세서는 상기 보안 정보를 보안 정보 처리 모듈로 전달하는 전자 장치.

청구항 15

제 14항에 있어서,

상기 보안 정보 처리 모듈은 보안 영역(Secure World) 내에 위치하는 것을 특징으로 하는 전자 장치.

청구항 16

제 14항에 있어서,

상기 보안 정보 처리 모듈은 일반 영역(Normal World) 내에 위치하는 것을 특징으로 하는 전자 장치.

청구항 17

제 10항에 있어서,

상기 보안 정보는 지문 정보, 홍채 정보, 안면 정보, 음성 정보, 정맥 정보 및 서명 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 전자 장치.

청구항 18

제 11항에 있어서,

상기 프로세서는 상기 보안 정보 입력 동작을 감지하기 위한 신호를 수신하고,

상기 신호는 키 또는 터치 입력, 음성 입력 및 제스처 입력 중 적어도 하나에 대응하는 것을 특징으로 하는 전자 장치.

청구항 19

센서 모듈을 이용하여 보안 정보 입력 동작을 감지하는 동작, 상기 보안 정보 입력 동작에 대응하여 인터럽트(Interrupt)를 발생시키는 동작 및 보안 정보 입력 모듈을 이용하여 상기 인터럽트에 대응하는 상기 보안 정보를 읽는 동작을 실행시키기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

청구항 20

제 19항에 있어서,

상기 보안 정보 입력 모듈은 보안 영역(Secure World) 내에 위치하는 것을 특징으로 하는 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

명 세 서

기 술 분 야

[0001] 본 명세서에 개시된 다양한 실시예들은 전자 장치의 보안 정보 입출력 방법 및 이를 사용하는 전자 장치에 관한 것이다.

배 경 기 술

[0002] 전자 장치는 스마트폰(Smart Phone)과 같은 휴대 단말기의 형태로 진화하면서 다양한 기능을 제공하는 애플리케

이션들을 통해 사용자에게 여러 가지 유용한 기능을 제공하고 있다. 한편, 특정 애플리케이션이 실행되는 경우, 해당 애플리케이션과 관련하여 일정 수준 이상의 보안을 요구하는 경우가 존재한다. 그 중에서도 사용자의 생체 정보(Biometric information)를 이용하여 전자 장치의 보안을 유지하는 방법이 떠오르고 있다. 이러한 생체 정보의 예로는 지문, 음성, 얼굴, 홍채, 손금, 정맥 분포 등 매우 다양하다.

발명의 내용

해결하려는 과제

[0003] 종래에는 사용자의 보안 정보(Security information)를 읽음에 있어서, 보안 영역(Secure World)이 아닌 일반 영역(Normal World)에서 사용자의 보안 정보를 읽었다. 따라서, 사용자의 보안 정보에 관한 원본 데이터(Raw data)가 보안 정보 처리 모듈에서 암호화되기 이전에 악의적인 목적으로 외부에 노출 될 가능성이 높았다.

[0004] 본 명세서에 개시된 다양한 실시예들은 사용자의 보안 정보를 읽을 때, 보안 정보에 관한 원본 데이터(Raw data)가 보안 정보 처리 모듈에서 암호화되기까지의 중간 과정을 보안 영역(Secure World)에서 처리하여, 보안 정보에 관한 원본 데이터(Raw data)를 보안 정보 입력 초기부터 악의적인 유출을 막을 수 있다.

[0005] 본 명세서에 개시된 다양한 실시예들은 사용자의 보안 정보를 출력할 때, 해당 보안 정보를 보안 영역(Secure World) 내 버퍼(Buffer)를 통해 처리하여, 사용자의 보안 정보를 악의적인 유출로부터 막을 수 있다. 따라서, 사용자에게 보안 정보를 안전하게 입출력하는 방법 및 이를 이용하는 전자 장치를 제공한다.

과제의 해결 수단

[0006] 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 정보 입력 방법은 센서 모듈을 이용하여 보안 정보 입력 동작을 감지하는 동작; 상기 보안 정보 입력 동작에 대응하여 인터럽트(Interrupt)를 발생시키는 동작; 및 보안 정보 입력 모듈을 이용하여 상기 인터럽트에 대응하는 상기 보안 정보를 읽는 동작을 포함할 수 있다.

[0007] 본 명세서에 개시된 다양한 실시예들 중 다른 하나에 따른 전자 장치는 센서 모듈; 및 상기 센서 모듈을 이용하여 보안 정보 입력 동작을 감지하고, 상기 보안 정보 입력 동작에 대응하여 인터럽트(Interrupt)를 발생시키고, 보안 정보 입력 모듈을 이용하여 상기 인터럽트에 대응하는 상기 보안 정보를 읽는 프로세서를 포함할 수 있다.

발명의 효과

[0008] 본 명세서에 개시된 다양한 실시예들은 전자 장치의 보안 영역(Secure World) 내에서 보안 정보(Security information)를 입출력함으로써 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 외부로부터의 악의적인 유출로부터 막을 수 있으며 이로 인해 전자 장치의 보안 정보(예: 생체 정보) 활용도를 향상시킬 수 있다.

도면의 간단한 설명

[0009] 도 1은 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치를 포함하는 네트워크 환경에 관한 도면,

도 2는 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치에 관한 블록도,

도 3은 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 영역에서 보안 정보를 읽는 방법 및 읽은 보안 정보를 보안 영역 내 보안 정보 처리 모듈로 전달하는 과정에 관한 도면,

도 4는 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 영역에서 보안 정보를 읽는 방법 및 읽은 보안 정보를 일반 영역 내 보안 정보 처리 모듈로 전달하는 과정에 관한 도면,

도 5는 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치가 보안 정보를 읽고, 해당 보안 정보를 보안 정보 처리 모듈로 전달하는 방법을 나타내는 순서도,

도 6은 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 정보 처리 모듈의 블록도,

도 7는 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 정보 등록 방법에 관한 도면,

도 8는 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 정보 인증 방법에 관한 도

면이다.

발명을 실시하기 위한 구체적인 내용

[0010] 이하, 첨부된 도면들을 참조하여 본 개시(present disclosure)의 다양한 실시예들을 상세히 설명한다. 이때, 첨부된 도면들에서 동일한 구성 요소는 가능한 동일한 부호로 나타내고 있음에 유의해야 한다. 또한 본 명세서에 개시된 다양한 실시예들의 요지를 흐리게 할 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략할 것이다. 하기의 설명에서는 본 명세서에 개시된 다양한 실시예들에 따른 동작을 이해하는데 필요한 부분만이 설명되며, 그 이외 부분의 설명은 본 명세서에 개시된 다양한 실시예들의 요지를 흩트리지 않도록 생략될 것이라는 것을 유의하여야 한다.

[0011] 본 발명 가운데 사용될 수 있는 “포함한다” 또는 “포함할 수 있다” 등의 표현은 발명된 해당 기능, 동작 또는 구성요소 등의 존재를 가리키며, 추가적인 하나 이상의 기능, 동작 또는 구성요소 등을 제한하지 않는다. 또한, 본 발명에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0012] 본 발명에서 “또는” 등의 표현은 함께 나열된 단어들의 어떠한, 그리고 모든 조합을 포함한다. 예를 들어, “A 또는 B”는, A를 포함할 수도, B를 포함할 수도, 또는 A 와 B 모두를 포함할 수도 있다.

[0013] 본 발명 가운데 “제 1,” “제2,” “첫째,” 또는 “둘째,” 등의 표현들이 본 발명의 다양한 구성요소들을 수식할 수 있지만, 해당 구성요소들을 한정하지 않는다. 예를 들어, 상기 표현들은 해당 구성요소들의 순서 및/또는 중요도 등을 한정하지 않는다. 상기 표현들은 한 구성요소를 다른 구성요소와 구분 짓기 위해 사용될 수 있다. 예를 들어, 제1 사용자 기기와 제 2 사용자 기기는 모두 사용자 기기이며, 서로 다른 사용자 기기를 나타낸다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[0014] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해될 수 있어야 할 것이다.

[0015] 본 발명에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0016] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 발명에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0017] 본 개시에 따른 전자 장치(100)는, 생체 센서가 포함된 장치일 수 있다. 예를 들면, 스마트폰(smartphone), 태블릿 PC(tablet personal computer), 이동전화기(mobile phone), 화상전화기, 전자북 리더기(e-book reader), 데스크탑 PC(desktop personal computer), 랩탑 PC(laptop personal computer), 넷북 컴퓨터(netbook computer), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 모바일 의료 장치, 전자 팔찌, 전자 목걸이, 전자 앱세서리(appcessory), 카메라(camera), 웨어러블 장치(wearable device), 전자 시계(electronic clock), 손목 시계(wrist watch), 가전 제품(home appliance)(예: 냉장고, 에어컨, 청소기, 오븐, 전자레인식, 세탁기, 공기 청정기 등), 인공 지능 로봇, TV, DVD(digital video disk) 플레이어, 오디오, 각종 의료기기(예: MRA(magnetic resonance angiography), MRI(magnetic resonance imaging), CT(computed tomography), 촬영기, 초음파기 등), 네비게이션(navigation) 장치, GPS 수신기(global positioning system receiver), EDR(event data recorder), FDR(flight data recorder), 셋톱 박스(set-top box), TV 박스(예를 들면, 삼성 HomeSync™, 애플TV™, 또는 구글 TV™), 전자 사전, 자동차 인포테인먼트(infotainment) 장치, 선박용 전자 장비(electronic equipment for ship, 예를 들면, 선박용 항법 장치, 자이로 콤파스 등), 항공 전자장치(avionics), 보안 장치, 전자 의복, 전자 키, 캠코더(camcorder), 게임 콘솔

(game consoles), HMD(head-mounted display), 평판표시장치(flat panel display device), 전자 액자, 전자 앨범, 통신 기능을 포함한 가구(furniture) 또는 건물/구조물의 일부, 전자 보드(electronic board), 전자 사인 입력장치(electronic signature receiving device) 또는 프로젝터(projector) 등의 다양한 장치들 중 하나 또는 그 이상의 조합일 수 있다. 본 개시에 따른 전자 장치는 전술한 장치들에 한정되지 않음은 당업자에게 자명하다.

[0018] 도 1은 본 개시의 실시예에 따른 전자 장치(100)를 포함하는 네트워크 환경(101)을 도시한다.

[0019] 도 1을 참조하면, 전자 장치(100)는 버스(110), 프로세서(120), 메모리(130), 입출력 인터페이스(140), 디스플레이(150), 통신 인터페이스(160) 및 애플리케이션 제어 모듈(170)을 포함할 수 있다.

[0020] 버스(110)는 전술한 구성요소들을 서로 연결하고, 전술한 구성요소들 간의 통신(예: 제어 메시지)을 전달하는 회로일 수 있다.

[0021] 프로세서(120)는 버스(110)를 통해 전술한 다른 구성요소들(예: 메모리(130), 입출력 인터페이스(140), 디스플레이(150), 통신 인터페이스(160) 및 애플리케이션 제어 모듈(170))로부터 명령을 수신하여, 수신된 명령을 해독하고, 해독된 명령에 따른 연산이나 데이터 처리를 실행할 수 있다.

[0022] 메모리(130)는 프로세서(120) 또는 다른 구성요소들(예: 입출력 인터페이스(140), 디스플레이(150), 통신 인터페이스(160) 및 애플리케이션 제어 모듈(170))로부터 수신되거나 프로세서(120) 또는 다른 구성요소들에 의해 생성된 명령 또는 데이터를 저장할 수 있다. 메모리(130)는 커널(131), 미들웨어(132), 애플리케이션 프로그래밍 인터페이스(API: application programming interface, 133) 또는 애플리케이션(134) 등의 프로그래밍 모듈들을 포함할 수 있다. 전술한 각각의 프로그래밍 모듈들은 소프트웨어, 펌웨어, 하드웨어 또는 이들 중 적어도 둘 이상의 조합으로 구성될 수 있다.

[0023] 커널(131)은 나머지 다른 프로그래밍 모듈들 미들웨어(132), API(133) 또는 애플리케이션(134)에 구현된 동작 또는 기능을 실행하는 데 사용되는 시스템 리소스들(예: 버스 (110), 프로세서(120) 또는 메모리(130))을 제어 또는 관리할 수 있다. 또한, 커널(131)은 미들웨어(132), API(133) 또는 애플리케이션(134)에서 전자 장치(100)의 개별 구성요소에 접근하여 제어 또는 관리할 수 있는 인터페이스를 제공할 수 있다.

[0024] 미들웨어(132)는 API(133) 또는 애플리케이션(134)이 커널(131)과 통신하여 데이터를 주고받을 수 있도록 중개 역할을 수행할 수 있다. 또한, 미들웨어(132)는 애플리케이션(134)으로부터 수신된 작업 요청들과 관련하여, 예를 들면, 애플리케이션(134) 중 적어도 하나의 애플리케이션에 전자 장치(100)의 시스템 리소스(예: 버스(110), 프로세서(120) 또는 메모리(130))를 사용할 수 있는 우선 순위를 배정하는 등의 방법을 이용하여 작업 요청에 대한 제어(예: 스케쥴링 또는 로드 밸런싱)을 수행할 수 있다.

[0025] API(133)는 애플리케이션(134)이 커널(131) 또는 미들웨어(132)에서 제공되는 기능을 제어하기 위한 인터페이스로, 예를 들면, 파일 제어, 창 제어, 화상 처리 또는 문자 제어 등을 위한 적어도 하나의 인터페이스 또는 함수(예: 명령어)를 포함할 수 있다.

[0026] 다양한 실시예에 따르면, 애플리케이션(134)은 SMS/MMS 애플리케이션, 이메일 애플리케이션, 달력 애플리케이션, 알람 애플리케이션, 건강 관리(health care) 애플리케이션(예: 운동량 또는 혈당 등을 측정하는 어플리케이션) 또는 환경 정보 애플리케이션(예: 기압, 습도 또는 온도 정보 등을 제공하는 애플리케이션) 등을 포함할 수 있다. 추가적으로 또는 대체적으로, 애플리케이션(134)은 전자 장치(100)와 외부 전자 장치(예: 전자 장치 104) 사이의 정보 교환과 관련된 애플리케이션일 수 있다. 정보 교환과 관련된 애플리케이션은, 예를 들어, 상기 외부 전자 장치에 특정 정보를 전달하기 위한 알림 전달(notification relay) 애플리케이션, 또는 외부 전자 장치를 관리하기 위한 장치 관리(device management) 애플리케이션을 포함할 수 있다.

[0027] 예를 들면, 알림 전달 애플리케이션은 전자 장치(100)의 다른 애플리케이션(예: SMS/MMS 애플리케이션, 이메일 애플리케이션, 건강 관리 애플리케이션 또는 환경 정보 애플리케이션 등)에서 발생한 알림 정보를 외부 전자 장치(예: 전자 장치 104)로 전달하는 기능을 포함할 수 있다. 추가적으로 또는 대체적으로, 알림 전달 애플리케이션은, 예를 들면, 외부 전자 장치(예: 전자 장치 104)로부터 알림 정보를 수신하여 사용자에게 제공할 수 있다. 장치 관리 애플리케이션은, 예를 들면, 전자 장치(100)와 통신하는 외부 전자 장치(예: 전자 장치 104)의 적어도 일부에 대한 기능(예: 외부 전자 장치 자체(또는, 일부 구성 부품)의 턴온/턴오프 또는 디스플레이의 밝기(또는, 해상도) 조절), 외부 전자 장치에서 동작하는 어플리케이션 또는 외부 전자 장치에서 제공되는 서비스(예: 통화 서비스 또는 메시지 서비스)를 관리(예: 설치, 삭제 또는 업데이트)할 수 있다.

[0028] 다양한 실시예에 따르면, 애플리케이션(134)은 외부 전자 장치(예: 전자 장치 104)의 속성(예: 전자 장치의 종류)에 따라 지정된 애플리케이션을 포함할 수 있다. 예를 들어, 외부 전자 장치가 MP3 플레이어인 경우, 애플리케이션(134)은 음악 재생과 관련된 애플리케이션을 포함할 수 있다. 유사하게, 외부 전자 장치가 모바일 의료기기인 경우, 애플리케이션(134)은 건강 관리와 관련된 애플리케이션을 포함할 수 있다. 일 실시예에 따르면, 애플리케이션(134)은 전자 장치(100)에 지정된 애플리케이션 또는 외부 전자 장치(예: 서버 106 또는 전자 장치 104)로부터 수신된 애플리케이션 중 적어도 하나를 포함할 수 있다.

[0029] 입출력 인터페이스(140)는, 입출력 장치(예: 센서, 키보드 또는 터치 스크린)를 통하여 사용자로부터 입력된 명령 또는 데이터를, 예를 들면, 버스(110)를 통해 프로세서(120), 메모리(130), 통신 인터페이스(160), 또는 애플리케이션 제어 모듈(170)에 전달할 수 있다. 예를 들면, 입출력 인터페이스(140)는 터치 스크린을 통하여 입력된 사용자의 터치에 대한 데이터를 프로세서(120)로 제공할 수 있다. 또한, 입출력 인터페이스(140)는, 예를 들면, 버스(110)를 통해 프로세서(120), 메모리(130), 통신 인터페이스(160), 또는 애플리케이션 제어 모듈(170)로부터 수신된 명령 또는 데이터를 입출력 장치(예: 스피커 또는 디스플레이)를 통하여 출력할 수 있다. 예를 들면, 입출력 인터페이스(140)는 프로세서(120)를 통하여 처리된 음성 데이터를 스피커를 통하여 사용자에게 출력할 수 있다.

[0030] 디스플레이(150)는 사용자에게 각종 정보(예: 멀티미디어 데이터 또는 텍스트 데이터 등)을 표시할 수 있다.

[0031] 통신 인터페이스(160)는 전자 장치(100)와 외부 장치(예: 전자 장치 104 또는 서버 106) 간의 통신을 연결할 수 있다. 예를 들면, 통신 인터페이스(160)는 무선 통신 또는 유선 통신을 통해서 네트워크(162)에 연결되어 외부 장치와 통신할 수 있다. 무선 통신은, 예를 들어, Wifi(wireless fidelity), BT(Bluetooth), NFC(near field communication), GPS(global positioning system) 또는 cellular 통신(예: LTE, LTE-A, CDMA, WCDMA, UMTS, WiBro 또는 GSM 등) 중 적어도 하나를 포함할 수 있다. 유선 통신은, 예를 들어, USB(universal serial bus), HDMI(high definition multimedia interface), RS-232(recommended standard 232) 또는 POTS(plain old telephone service) 중 적어도 하나를 포함할 수 있다.

[0032] 일 실시예에 따르면, 네트워크(162)는 통신 네트워크(telecommunications network)일 수 있다. 통신 네트워크는 컴퓨터 네트워크(computer network), 인터넷(internet), 사물 인터넷(internet of things) 또는 전화망(telephone network) 중 적어도 하나를 포함할 수 있다. 일 실시예에 따르면, 전자 장치(100)와 외부 장치 간의 통신을 위한 프로토콜(예: transport layer protocol, data link layer protocol 또는 physical layer protocol))은 애플리케이션(134), 애플리케이션 프로그래밍 인터페이스(133), 미들웨어(132), 커널(131) 또는 통신 인터페이스(160) 중 적어도 하나에서 지원될 수 있다.

[0033] 애플리케이션 제어 모듈(170)은, 다른 구성요소들(예: 프로세서(120), 메모리(130), 입출력 인터페이스(140), 또는 통신 인터페이스(160))로부터 획득된 정보 중 적어도 일부를 처리하고, 이를 다양한 방법으로 사용자에게 제공할 수 있다. 예를 들면, 애플리케이션 제어 모듈(170)은, 전자 장치(100)에 구비된 접속 부품의 정보를 인식하고, 접속 부품의 정보를 메모리(130)에 저장하고, 접속 부품의 정보에 기반하여, 애플리케이션(134)을 실행시킬 수 있다.

[0034] 도 2는 본 개시의 실시예들에 따른 전자 장치(200)의 블록도를 도시한다. 예를 들어, 전자 장치(200)는 도 1에 도시된 전자 장치(100)의 전체 또는 일부를 구성할 수 있다.

[0035] 도 2를 참조하면, 전자 장치(200)는 하나 이상의 애플리케이션 프로세서(AP: application processor, 210), 통신 모듈(220), SIM(subscriber identification module) 카드(224), 메모리(230), 센서 모듈(240), 입력 장치(250), 디스플레이(260), 인터페이스(270), 오디오 모듈(280), 카메라 모듈(291), 전력관리 모듈(295), 배터리(296), 인디케이터(297) 및 모터(298)를 포함할 수 있다.

[0036] AP(210)는 운영체제 또는 응용 프로그램을 구동하여 AP(210)에 연결된 다수의 하드웨어 또는 소프트웨어 구성요소들을 제어할 수 있고, 멀티미디어 데이터를 포함한 각종 데이터 처리 및 연산을 수행할 수 있다. 예를 들어, AP(210)는 SoC(system on chip) 로 구현될 수 있다. 일 실시예에 따르면, AP(210)는 GPU(graphic processing unit, 미도시)를 더 포함할 수 있다.

[0037] 통신 모듈(220)(예: 통신 인터페이스(160))은 전자 장치(200)(예: 도 1의 전자 장치(100))와 네트워크를 통해 연결된 다른 전자 장치들(예: 도 1의 전자 장치(104) 또는 서버(106)) 간의 통신에서 데이터 송수신을 수행할 수 있다. 일 실시예에 따르면, 통신 모듈(220)은 셀룰러 모듈(221), Wifi 모듈(223), BT 모듈(225), GPS 모듈(227), NFC 모듈(228) 및 RF(radio frequency) 모듈(229)을 포함할 수 있다.

[0038] 셀룰러 모듈(221)은 통신망(예: LTE, LTE-A, CDMA, WCDMA, UMTS, WiBro 또는 GSM 등)을 통해서 음성 통화, 영상 통화, 문자 서비스 또는 인터넷 서비스 등을 제공할 수 있다. 예를 들어, 셀룰러 모듈(221)은 가입자 식별 모듈(예: SIM 카드(224))을 이용하여 통신 네트워크 내에서 전자 장치의 구별 및 인증을 수행할 수 있다. 일 실시예에 따르면, 셀룰러 모듈(221)은 AP(210)가 제공할 수 있는 기능 중 적어도 일부 기능을 수행할 수 있다. 예를 들면, 셀룰러 모듈(221)은 멀티 미디어 제어 기능의 적어도 일부를 수행할 수 있다.

[0039] 일 실시예에 따르면, 셀룰러 모듈(221)은 커뮤니케이션 프로세서(CP: communication processor)를 포함할 수 있다. 예를 들어, 셀룰러 모듈(221)은 SoC로 구현될 수 있다. 셀룰러 모듈(221)은(예: 커뮤니케이션 프로세서) 메모리(230) 또는 전력관리 모듈(295) 등의 구성요소들이 AP(210)와 별개의 구성요소로 도시되어 있으나, 일 실시예에 따르면, AP(210)가 전술한 구성요소들의 적어도 일부(예: 셀룰러 모듈(221))를 포함하도록 구현될 수 있다.

[0040] 일 실시예에 따르면, AP(210) 또는 셀룰러 모듈(221)(예: 커뮤니케이션 프로세서)은 각각에 연결된 비휘발성 메모리 또는 다른 구성요소 중 적어도 하나로부터 수신한 명령 또는 데이터를 휘발성 메모리에 로드(load)하여 처리할 수 있다. 또한, AP(210) 또는 셀룰러 모듈(221)은 다른 구성요소 중 적어도 하나로부터 수신하거나 다른 구성요소 중 적어도 하나에 의해 생성된 데이터를 비휘발성 메모리에 저장(store)할 수 있다. AP(210) 및/또는 셀룰러 모듈(221)은 도 1에서 전술한 프로세서(120)의 전체 또는 일부를 구성할 수 있다.

[0041] 예를 들어, Wifi 모듈(223), BT 모듈(225), GPS 모듈(227) 또는 NFC 모듈(228) 각각은 해당하는 모듈을 통해서 송수신되는 데이터를 처리하기 위한 프로세서를 포함할 수 있다.

[0042] 셀룰러 모듈(221), Wifi 모듈(223), BT 모듈(225), GPS 모듈(227) 또는 NFC 모듈(228)이 각각 별개의 블록으로 도시되었으나, 일 실시예에 따르면, 셀룰러 모듈(221), Wifi 모듈(223), BT 모듈(225), GPS 모듈(227) 또는 NFC 모듈(228) 중 적어도 일부(예: 두 개 이상)는 하나의 integrated chip(IC) 또는 IC 패키지 내에 포함될 수 있다. 예를 들면, 셀룰러 모듈(221), Wifi 모듈(223), BT 모듈(225), GPS 모듈(227) 또는 NFC 모듈(228) 각각에 대응하는 프로세서들 중 적어도 일부(예: 셀룰러 모듈(221)에 대응하는 커뮤니케이션 프로세서 및 Wifi 모듈(223)에 대응하는 Wifi 프로세서)는 하나의 SoC로 구현될 수 있다.

[0043] RF 모듈(229)은 데이터의 송수신, 예를 들면, RF 신호의 송수신을 할 수 있다. 예를 들어, RF 모듈(229)은 트랜시버(transceiver), PAM(power amp module), 주파수 필터(frequency filter) 또는 LNA(low noise amplifier) 등을 포함할 수 있다. 예를 들어, RF 모듈(229)은 무선 통신에서 자유 공간상의 전자파를 송수신하기 위한 부품 도체 또는 도선 등을 더 포함할 수 있다. 셀룰러 모듈(221), Wifi 모듈(223), BT 모듈(225), GPS 모듈(227) 또는 NFC 모듈(228)이 하나의 RF 모듈(229)을 서로 공유하는 것으로 도시되어 있으나, 일 실시예에 따르면, 셀룰러 모듈(221), Wifi 모듈(223), BT 모듈(225), GPS 모듈(227) 또는 NFC 모듈(228) 중 적어도 하나는 별개의 RF 모듈을 통하여 RF 신호의 송수신을 수행할 수 있다.

[0044] SIM 카드(224_1~N)는 가입자 식별 모듈을 포함하는 카드일 수 있으며, 전자 장치(200)의 특정 위치에 형성된 슬롯(225_1~N)에 삽입될 수 있다. SIM 카드(224_1~N)는 고유한 식별 정보(예: ICCID(integrated circuit card identifier)) 또는 가입자 정보(예: IMSI(international mobile subscriber identity))를 포함할 수 있다.

[0045] 메모리(230)(예: 도 1의 메모리(130))는 내장 메모리(232) 또는 외장 메모리(234)를 포함할 수 있다. 예를 들어, 내장 메모리(232)는 휘발성 메모리(예를 들면, DRAM(dynamic RAM), SRAM(static RAM), SDRAM(synchronous dynamic RAM) 등) 또는 비휘발성 메모리(non-volatile Memory, 예를 들면, OTPROM(one time programmable ROM), PROM(programmable ROM), EPROM(erasable and programmable ROM), EEPROM(electrically erasable and programmable ROM), mask ROM, flash ROM, NAND flash memory, NOR flash memory 등) 중 적어도 하나를 포함할 수 있다.

[0046] 일 실시예에 따르면, 내장 메모리(232)는 Solid State Drive (SSD)일 수 있다. 외장 메모리(234)는 flash drive, 예를 들면, CF(compact flash), SD(secure digital), Micro-SD(micro secure digital), Mini-SD(mini secure digital), xD(extreme digital) 또는 Memory Stick 등을 더 포함할 수 있다. 외장 메모리(234)는 다양한 인터페이스를 통하여 전자 장치(200)과 기능적으로 연결될 수 있다. 일 실시예에 따르면, 전자 장치(200)는 하드 드라이브와 같은 저장 장치(또는 저장 매체)를 더 포함할 수 있다.

[0047] 센서 모듈(240)은 물리량을 계측하거나 전자 장치(200)의 작동 상태를 감지하여, 계측 또는 감지된 정보를 전기 신호로 변환할 수 있다. 예를 들어, 센서 모듈(240)은 제스처 센서(240A), 자이로 센서(240B), 기압 센서(240C), 마그네틱 센서(240D), 가속도 센서(240E), 그립 센서(240F), 근접 센서(240G), 컬러(color) 센서

(240H)(예: RGB(red, green, blue) 센서), 생체 센서(240I), 온/습도 센서(240J), 조도 센서(240K) 또는 UV(ultra violet) 센서(240M) 중의 적어도 하나를 포함할 수 있다. 추가적으로 또는 대체적으로, 센서 모듈(240)은 후각 센서(E-nose sensor, 미도시), EMG 센서(electromyography sensor, 미도시), EEG 센서(electroencephalogram sensor, 미도시), ECG 센서(electrocardiogram sensor, 미도시), IR(infrared) 센서(미도시), 홍채 센서(미도시) 또는 지문 센서(미도시) 등을 포함할 수 있다. 센서 모듈(240)은 그 안에 속한 적어도 하나 이상의 센서들을 제어하기 위한 제어 회로를 더 포함할 수 있다.

[0048] 입력 장치(250)는 터치 패널(touch panel, 252), 펜 센서(pen sensor, 254), 키(key, 256) 또는 초음파(ultrasonic) 입력 장치(258)를 포함할 수 있다. 예를 들어, 터치 패널(252)은 정전식, 감압식, 적외선 방식 또는 초음파 방식 중 적어도 하나의 방식으로 터치 입력을 인식할 수 있다. 터치 패널(252)은 제어 회로를 더 포함할 수도 있다. 정전식의 경우, 물리적 접촉 또는 근접 인식이 가능하다. 터치 패널(252)은 택타일 레이어(tactile layer)를 더 포함할 수도 있다. 이 경우, 터치 패널(252)은 사용자에게 촉각 반응을 제공할 수 있다.

[0049] 예를 들어, 펜 센서(254)는 사용자의 터치 입력을 받는 것과 동일 또는 유사한 방법 또는 별도의 인식용 쉬트(sheet)를 이용하여 구현될 수 있다. 예를 들어, 키 (256)는 물리적인 버튼, 광학식 키 또는 키패드를 포함할 수 있다. 초음파(ultrasonic) 입력 장치(258)는 초음파 신호를 발생하는 입력 도구를 통해, 전자 장치(200)에서 마이크(예: 마이크(288))로 음파를 감지하여 데이터를 확인할 수 있는 장치로서, 무선 인식이 가능하다. 일 실시예에 따르면, 전자 장치(200)는 통신 모듈(220)을 이용하여 이와 연결된 외부 장치(예: 컴퓨터 또는 서버)로부터 사용자 입력을 수신할 수도 있다.

[0050] 디스플레이(260)(예: 도 1의 디스플레이(150))는 패널(262), 홀로그램 장치(264) 또는 프로젝터(266)를 포함할 수 있다. 예를 들어, 패널(262)은 LCD(liquid-crystal display) 또는 AM-OLED(active-matrix organic light-emitting diode) 등일 수 있다. 예를 들어, 패널(262)은 유연하게(flexible), 투명하게(transparent) 또는 착용할 수 있게(wearable) 구현될 수 있다. 패널(262)은 터치 패널(252)과 하나의 모듈로 구성될 수도 있다. 홀로그램 장치(264)는 빛의 간섭을 이용하여 입체 영상을 허공에 보여줄 수 있다. 프로젝터(266)는 스크린에 빛을 투사하여 영상을 표시할 수 있다. 예를 들어, 스크린은 전자 장치(200)의 내부 또는 외부에 위치할 수 있다. 일 실시예에 따르면, 디스플레이(260)는 패널(262), 홀로그램 장치(264), 또는 프로젝터(266)를 제어하기 위한 제어 회로를 더 포함할 수 있다.

[0051] 예를 들어, 인터페이스(270)는 HDMI(high-definition multimedia interface, 272), USB(universal serial bus, 274), 광 인터페이스(optical interface, 276) 또는 D-sub(D-subminiature, 278)를 포함할 수 있다. 예를 들어, 인터페이스(270)는 도 1에 도시된 통신 인터페이스(160)에 포함될 수 있다. 추가적으로 또는 대체적으로, 인터페이스(270)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.

[0052] 오디오 모듈(280)은 소리(sound)와 전기신호를 쌍방향으로 변환시킬 수 있다. 예를 들어, 오디오 모듈(280)의 적어도 일부 구성요소는 도 1 에 도시된 입출력 인터페이스(140)에 포함될 수 있다. 예를 들어, 오디오 모듈(280)은 스피커(282), 리시버(284), 이어폰(286) 또는 마이크(288) 등을 통해 입력 또는 출력되는 소리 정보를 처리할 수 있다.

[0053] 일 실시예에 따르면, 카메라 모듈(291)은 정지 영상 및 동영상을 촬영할 수 있는 장치로서 하나 이상의 이미지 센서(예: 전면 센서 또는 후면 센서), 렌즈(미도시), ISP(image signal processor, 미도시) 또는 플래쉬(flash, 미도시)(예: LED 또는 xenon lamp)를 포함할 수 있다.

[0054] 전력 관리 모듈(295)은 전자 장치(200)의 전력을 관리할 수 있다. 도시하지는 않았으나, 전력 관리 모듈(295)은, 예를 들면, PMIC(power management integrated circuit), 충전 IC(charger integrated circuit) 또는 배터리 또는 연료 게이지(battery or fuel gauge)를 포함할 수 있다.

[0055] 예를 들어, PMIC는 집적회로 또는 SoC 반도체 내에 탑재될 수 있다. 충전 방식은 유선과 무선으로 구분될 수 있다. 충전 IC는 배터리를 충전시킬 수 있으며, 충전기로부터의 과전압 또는 과전류 유입을 방지할 수 있다. 일 실시예에 따르면, 충전 IC는 유선 충전 방식 또는 무선 충전 방식 중 적어도 하나를 위한 충전 IC를 포함할 수 있다. 무선 충전 방식으로는, 예를 들면, 자기공명 방식, 자기유도 방식 또는 전자기파 방식 등이 있으며, 무선 충전을 위한 부가적인 회로, 예를 들면, 코일 루프, 공진 회로 또는 정류기 등의 회로가 추가될 수 있다.

[0056] 예를 들어, 배터리 게이지는 배터리(296)의 잔량, 충전 중 전압, 전류 또는 온도를 측정할 수 있다. 배터리

(296)는 전기를 저장 또는 생성할 수 있고, 그 저장 또는 생성된 전기를 이용하여 전자 장치(200)에 전원을 공급할 수 있다. 예를 들어, 배터리(296)는 충전식 전지(rechargeable battery) 또는 태양 전지(solar battery)를 포함할 수 있다.

[0057] 인디케이터(297)는 전자 장치(200) 혹은 그 일부(예: AP(210))의 특정 상태, 예를 들면, 부팅 상태, 메시지 상태 또는 충전 상태 등을 표시할 수 있다. 모터(298)는 전기적 신호를 기계적 진동으로 변환할 수 있다. 도시되지는 않았으나, 전자 장치(200)는 모바일 TV 지원을 위한 처리 장치(예: GPU)를 포함할 수 있다. 예를 들어, 모바일 TV지원을 위한 처리 장치는 DMB(digital multimedia broadcasting), DVB(digital video broadcasting) 또는 미디어 플로우(media flow) 등의 규격에 따른 미디어 데이터를 처리할 수 있다.

[0058] 본 발명의 실시예에 따른 전자 장치의 전술한 구성요소들 각각은 하나 또는 그 이상의 부품(component)으로 구성될 수 있으며, 해당 구성 요소의 명칭은 전자 장치의 종류에 따라서 달라질 수 있다. 본 개시에 따른 전자 장치는 전술한 구성요소 중 적어도 하나를 포함하여 구성될 수 있으며, 일부 구성요소가 생략되거나 또는 추가적인 다른 구성요소를 더 포함할 수 있다. 또한, 본 개시에 따른 전자 장치의 구성 요소들 중 일부가 결합되어 하나의 개체(entity)로 구성됨으로써, 결합되기 이전의 해당 구성 요소들의 기능을 동일하게 수행할 수 있다.

[0059] 본 발명에 사용된 용어 "모듈"은, 예를 들어, 하드웨어, 소프트웨어 또는 펌웨어(firmware) 중 하나 또는 둘 이상의 조합을 포함하는 단위(unit)를 의미할 수 있다. "모듈"은 예를 들어, 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, 본 개시에 따른 "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.

[0060] 도 3은 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 영역(Secure World)에서 보안 정보(Security information)를 읽는(read) 방법 및 해당 보안 정보를 보안 영역 내 보안 정보 처리 모듈로 전달하는 과정에 관한 도면이다.

[0061] 도 2 및 도 3을 참조하면, 전자 장치(200)는 센서 모듈(240)을 포함할 수 있다. 센서 모듈(240)은 생체 센서(300)를 이용하여 사용자의 생체 정보를 감지할 수 있다. 생체 센서(300)는 지문 센서, 홍채 센서, 정맥 센서, 음성 센서 및 안면 센서 중 하나일 수 있다. 생체 센서(300)는 사용자의 생체 정보, 예를 들어, 지문 정보, 홍채 정보, 정맥 정보, 음성 정보 및 안면 정보 등을 검출할 수 있다.

[0062] 전자 장치(200)는 일반 영역(Normal World, 310) 및 보안 영역(Secure World, 320)으로 구분될 수 있다. 구체적으로, 일반 영역에서는 기존의 운영체제들, 예를 들어, 리눅스(Linux), 안드로이드(Android), 아이오에스(iOS) 등이 동작하며, 운영체제의 제어 하에 프레임워크 및 애플리케이션이 동작한다. 이러한 일반 영역(Normal World, 310)에서는 악성 소프트웨어의 동작을 제한하기 어렵기 때문에, 높은 수준의 보안이 필요한 동작을 하는데 위험이 따르게 된다.

[0063] 한편, 보안 영역(Secure World, 320)에서는 기존의 운영체제 및 프레임워크 동작이 제한되며, 일반 영역과 구분됨에 따라 기존의 악성 소프트웨어로 인한 보안 문제를 방지할 수 있다. 보안 영역에서도 SoC(System On Chip) 및 각종 하드웨어 자원을 사용할 수 있다.

[0064] 센서 모듈(300)은 사용자가 보안 정보를 입력하는 동작을 인식할 수 있다. 이를 위해 전자 장치(200)는 보안 정보를 입력하는 동작을 인식하기 위한 예비 동작을 수행할 수 있다. 예를 들어, 사용자가 해당 센서 모듈에 대응하는 키 또는 터치 신호를 입력할 수 있고, 음성 명령을 입력할 수 있고, 제스처를 입력하여 사용자의 보안 정보를 입력하는 화면으로 전환할 수 있다.

[0065] 센서 모듈(300)은 사용자가 보안 정보를 입력하는 동작을 인식하는 경우, 인터럽트(Interrupt)를 발생시킬 수 있다. 예를 들어, 센서 모듈(300) 중 지문 센서는 사용자가 손가락을 센서와 접촉하는 동작을 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(300) 중 홍채 센서는 사용자의 눈이 센서에 접근하면 홍채를 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(300) 중 정맥 센서는 사용자의 손이 센서에 접근하면 정맥 분포를 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(300) 중 음성 센서는 사용자가 음성을 입력하기 위한 신호를 입력 하면 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(300) 중 안면 센서는 사용자의 얼굴이 센서에 접근하면 눈, 코 및 입을 포함한 얼굴 윤곽을 인

식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다.

[0066] 한편, 상기의 예들은 본 개시의 이해를 돕기 위한 것으로 본 개시를 이에 한정하는 것은 아니다.

[0067] 센서 모듈(300)은 발생한 인터럽트를 일반 영역(Normal World, 310) 내 위치하는 보안 정보 인식 드라이버(312)로 전달할 수 있다.

[0068] 보안 정보 인식 드라이버(312)는 수신한 인터럽트를 보안 영역(Secure World, 320) 내 위치하는 보안 정보 입력 모듈(322)로 전달할 수 있다.

[0069] 보안 정보 입력 모듈(322)는 수신한 인터럽트에 대응하여 센서 모듈(300)로부터 사용자의 보안 정보(Security information)에 관한 원본 데이터(Raw data)를 읽을 수 있다. 보안 정보 입력 모듈(322)은 보안 영역(Secure World, 320) 내 위치하므로 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 입력 초기부터 외부의 악성 해킹 툴로부터 보호할 수 있다.

[0070] 보안 정보 입력 모듈(322)은 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 보안 영역(Secure World, 320) 내 보안 정보 처리 모듈(324)로 전달할 수 있다. 이렇게 전달된 보안 정보에 관한 원본 데이터(Raw data)는 보안 정보의 형판(Template)을 생성하고, 암호화(Encrypt)하는데 이용될 수 있으며, 궁극적으로는 제어 모듈(314)의 보안 정보 인식 서비스를 통해 입력된 보안 정보를 기반으로 사용자를 식별할 수 있다.

[0071] 한편, 보안 정보 입력 모듈(322)를 이용하여 보안 정보에 관한 원본 데이터(Raw data)를 읽음에 있어서, 상기의 실시예와 같이 일반 영역(Normal World, 310) 내 보안 정보 인식 드라이버(312)를 통한 간접적인 인터럽트 전달이 아닌, 보안 영역(Secure World, 320) 내 보안 정보 입력 모듈(322)로 직접 인터럽트를 전달하여 센서 모듈(300)로부터 사용자의 보안 정보를 읽을 수도 있다.

[0072] 일 실시예에서, 전자 장치(200)는 센서 모듈이 아닌 별도의 입력 장치(예: 250)를 구비할 수 있고 입력 장치를 통해 사용자의 보안 정보를 입력 받을 수 있다. 예를 들어, 개인 서명을 입력하는 입력 장치로부터 사용자의 서명 정보를 입력 받을 수 있다. 이렇게 입력 받은 사용자의 서명 정보는 보안 정보(Security information)에 포함될 수 있다.

[0073] 입력 장치(250)는 사용자가 보안 정보를 입력하는 동작을 인식할 수 있다. 한편, 전자 장치(200)는 보안 정보를 입력하는 동작을 인식하기 위한 예비 동작을 수행할 수 있다. 예를 들어, 사용자가 해당 입력 장치(250)에 대응하는 키 또는 터치 신호를 입력할 수 있고, 음성 명령을 입력할 수 있고, 제스처를 입력하여 사용자의 보안 정보를 입력하는 화면으로 전환할 수 있다.

[0074] 입력 장치(250)는 사용자가 보안 정보를 입력하는 동작을 인식하는 경우, 인터럽트(Interrupt)를 발생시킬 수 있다. 예를 들어, 사용자가 터치 패널(252)에 개인 서명을 입력하는 동작을 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 한편, 상기의 예들은 본 개시의 이해를 돕기 위한 것으로 본 개시를 이에 한정하는 것은 아니다.

[0075] 입력 장치(250)는 발생한 인터럽트를 일반 영역(Normal World, 310) 내 위치하는 보안 정보 인식 드라이버(312)로 전달할 수 있다.

[0076] 보안 정보 인식 드라이버(312)는 수신한 인터럽트를 보안 영역(Secure World, 320) 내 위치하는 보안 정보 입력 모듈(322)로 전달할 수 있다.

[0077] 보안 정보 입력 모듈(322)는 수신한 인터럽트에 대응하여 입력 장치(250)로부터 사용자의 보안 정보(Security information)에 관한 원본 데이터(Raw data)를 읽을 수 있다. 보안 정보 입력 모듈(322)은 보안 영역(Secure World, 320) 내 위치하므로 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 입력 초기부터 외부의 악성 해킹 툴로부터 보호할 수 있다.

[0078] 한편, 보안 정보 입력 모듈(322)를 이용하여 보안 정보에 관한 원본 데이터(Raw data)를 읽음에 있어서, 상기의 실시예와 같이 일반 영역(Normal World, 310) 내 보안 정보 인식 드라이버(312)를 통한 간접적인 인터럽트 전달이 아닌, 보안 영역(Secure World, 320) 내 보안 정보 입력 모듈(322)로 직접 인터럽트를 전달하여 입력 장치(250)로부터 사용자의 보안 정보를 읽을 수도 있다.

[0079] 일 실시예에서, 전자 장치(200)는 사용자의 보안 정보를 출력 장치(예: 디스플레이 모듈 또는 오디오 모듈)를 통해 출력할 수 있다. 구체적으로, 보안 영역에 별도의 버퍼(Buffer)를 구비하여 출력되는 보안 정보를 외부 노출의 위험으로부터 보호할 수 있다.

[0080] 도 4는 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치의 보안 영역(Secure World)에서 보안 정보(Security information)를 읽는 방법 및 해당 보안 정보를 일반 영역(Normal World) 내 보안 정보 인식 엔진으로 전달하는 과정에 관한 도면이다.

[0081] 도 2 및 도 4를 참조하면, 전자 장치(200)는 센서 모듈(240)을 포함할 수 있다. 센서 모듈(240)은 생체 센서(400)를 이용하여 사용자의 생체 정보를 감지할 수 있다. 생체 센서(400)는 지문 센서, 홍채 센서, 정맥 센서, 음성 센서 및 안면 센서 중 하나일 수 있다. 생체 센서(400)은 사용자의 생체 정보, 예를 들어, 지문 정보, 홍채 정보, 정맥 정보, 음성 정보 및 안면 정보 등을 검출할 수 있다.

[0082] 전자 장치(200)는 일반 영역(Normal World, 410) 및 보안 영역(Secure World, 420)으로 구분될 수 있다. 구체적으로, 일반 영역에서는 기존의 운영체제들, 예를 들어, 리눅스(Linux), 안드로이드(Android), 아이오에스(iOS) 등이 동작하며, 운영체제의 제어 하에 프레임워크 및 애플리케이션이 동작한다. 이러한 일반 영역(Normal World, 410)에서는 악성 소프트웨어의 동작을 제한하기 어렵기 때문에, 높은 수준의 보안이 필요한 동작을 하는데 위험이 따르게 된다.

[0083] 한편, 보안 영역(Secure World, 420)에서는 기존의 운영체제 및 프레임워크 동작이 제한되며, 일반 영역과 구분됨에 따라 기존의 악성 소프트웨어로 인한 보안 문제를 방지할 수 있다. 보안 영역에서도 SoC(System On Chip) 및 각종 하드웨어 자원을 사용할 수 있다.

[0084] 센서 모듈(400)은 사용자가 보안 정보를 입력하는 동작을 인식할 수 있다. 이를 위해 전자 장치(200)는 보안 정보를 입력하는 동작을 인식하기 위한 예비 동작을 수행할 수 있다. 예를 들어, 사용자가 해당 센서 모듈에 대응하는 키 또는 터치 신호를 입력할 수 있고, 음성 명령을 입력할 수 있고, 제스처를 입력하여 사용자의 생체 정보를 입력하는 화면으로 전환할 수 있다.

[0085] 센서 모듈(400)은 사용자가 보안 정보를 입력하는 동작을 인식하는 경우, 인터럽트(Interrupt)를 발생시킬 수 있다. 예를 들어, 센서 모듈(400) 중 지문 센서는 사용자가 손가락을 센서와 접촉하는 동작을 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(400) 중 홍채 센서는 사용자의 눈이 센서에 접근하면 홍채를 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(400) 중 정맥 센서는 사용자의 손이 센서에 접근하면 정맥 분포를 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(400) 중 음성 센서는 사용자가 음성을 입력하기 위한 신호를 입력 하면 이에 대응하는 인터럽트를 발생시킬 수 있다. 센서 모듈(400) 중 안면 센서는 사용자의 얼굴이 센서에 접근하면 눈, 코 및 입을 포함한 얼굴 윤곽을 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다.

[0086] 한편, 상기의 예는 본 개시의 이해를 돕기 위한 것으로 본 개시를 이에 한정하는 것은 아니다.

[0087] 센서 모듈(400)은 발생한 인터럽트를 일반 영역(Normal World, 410) 내 위치하는 보안 정보 인식 드라이버(412)로 전달할 수 있다.

[0088] 보안 정보 인식 드라이버(412)는 수신한 인터럽트를 보안 영역(Secure World, 420) 내 위치하는 보안 정보 입력 모듈(422)로 전달할 수 있다.

[0089] 보안 정보 입력 모듈(422)은 수신한 인터럽트에 대응하여 센서 모듈(400)로부터 사용자의 보안 정보(Security information)에 관한 원본 데이터(Raw data)를 읽을 수 있다.

[0090] 보안 정보 입력 모듈(422)는 보안 영역(Secure World, 420) 내 위치하므로 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 입력 초기부터 외부의 악성 해킹 툴로부터 보호할 수 있다.

[0091] 보안 정보 입력 모듈(422)은 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 일반 영역(Normal World, 410) 내 보안 정보 처리 모듈(424)로 전달할 수 있다.

[0092] 이렇게 전달된 보안 정보에 관한 원본 데이터(Raw data)는 보안 정보의 형판(Template)을 생성하고, 암호화(Encrypt)하는데 이용될 수 있으며, 궁극적으로는 제어 모듈(416)의 보안 정보 인식 서비스를 통해 입력된 보안 정보를 기반으로 사용자를 식별할 수 있다.

[0093] 한편, 보안 정보 입력 모듈(422)를 이용하여 보안 정보에 관한 원본 데이터(Raw data)를 읽음에 있어서, 상기의 실시예와 같이 일반 영역(Normal World, 410) 내 보안 정보 인식 드라이버(412)를 통한 간접적인 인터럽트 전달이 아닌, 보안 영역(Secure World, 420) 내 보안 정보 입력 모듈(422)로 직접 인터럽트를 전달하여 센서 모듈(400)로부터 사용자의 보안 정보를 읽을 수도 있다.

[0094] 일 실시예에서, 전자 장치(200)는 센서 모듈이 아닌 별도의 입력 장치(예: 250)를 구비할 수 있고 입력 장치를 통해 사용자의 보안 정보를 입력 받을 수 있다. 예를 들어, 개인 서명을 입력하는 입력 장치로부터 사용자의 서명 정보를 입력 받을 수 있다. 이렇게 입력 받은 사용자의 서명 정보는 보안 정보(Security information)에 포함될 수 있다.

[0095] 입력 장치(250)는 사용자가 보안 정보를 입력하는 동작을 인식할 수 있다. 한편, 전자 장치(200)는 보안 정보를 입력하는 동작을 인식하기 위한 예비 동작을 수행할 수 있다. 예를 들어, 사용자가 해당 입력 장치(250)에 대응하는 키 또는 터치 신호를 입력할 수 있고, 음성 명령을 입력할 수 있고, 제스처를 입력하여 사용자의 보안 정보를 입력하는 화면으로 전환할 수 있다.

[0096] 입력 장치(250)는 사용자가 보안 정보를 입력하는 동작을 인식하는 경우, 인터럽트(Interrupt)를 발생시킬 수 있다. 예를 들어, 사용자가 터치 패널(252)에 개인 서명을 입력하는 동작을 인식할 수 있고 이에 대응하는 인터럽트를 발생시킬 수 있다. 한편, 상기의 예들은 본 개시의 이해를 돕기 위한 것으로 본 개시를 이에 한정하는 것은 아니다.

[0097] 입력 장치(250)는 발생한 인터럽트를 일반 영역(Normal World, 410) 내 위치하는 보안 정보 인식 드라이버(412)로 전달할 수 있다.

[0098] 보안 정보 인식 드라이버(412)는 수신한 인터럽트를 보안 영역(Secure World, 420) 내 위치하는 보안 정보 입력 모듈(422)로 전달할 수 있다.

[0099] 보안 정보 입력 모듈(422)는 수신한 인터럽트에 대응하여 입력 장치(250)로부터 사용자의 보안 정보(Security information)에 관한 원본 데이터(Raw data)를 읽을 수 있다. 보안 정보 입력 모듈(422)은 보안 영역(Secure World, 420) 내 위치하므로 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 입력 초기부터 외부의 악성 해킹 툴로부터 보호할 수 있다.

[0100] 한편, 보안 정보 입력 모듈(422)를 이용하여 보안 정보에 관한 원본 데이터(Raw data)를 읽음에 있어서, 상기의 실시예와 같이 일반 영역(Normal World, 310) 내 보안 정보 인식 드라이버(412)를 통한 간접적인 인터럽트 전달이 아닌, 보안 영역(Secure World, 420) 내 보안 정보 입력 모듈(422)로 직접 인터럽트를 전달하여 입력 장치(250)로부터 사용자의 보안 정보를 읽을 수도 있다.

[0101] 일 실시예에서, 전자 장치(200)는 사용자의 보안 정보를 출력 장치(예: 디스플레이 모듈 또는 오디오 모듈)를 통해 출력할 수 있다. 구체적으로, 보안 영역에 별도의 버퍼(Buffer)를 구비하여 출력되는 보안 정보를 외부 노출의 위험으로부터 보호할 수 있다.

[0102] 도 5는 본 명세서에 개시된 다양한 실시예들 중 어느 하나에 따른 전자 장치가 보안 정보(Security information)를 읽고, 해당 보안 정보를 보안 정보 처리 모듈로 전달하는 과정을 나타내는 순서도이다.

[0103] 전자 장치(200)는, 510 과정에서, 센서 모듈을 이용하여 사용자의 보안 정보(Security information) 입력 동작을 인식할 수 있다. 예를 들어, 전자 장치(200)는 지문 센서를 이용하여 사용자가 손가락을 센서와 접촉하는 동작을 인식할 수 있다. 전자 장치(200)는 홍채 센서를 이용하여 사용자의 눈이 센서에 접근하는 동작을 인식할 수 있다. 전자 장치(200)는 정맥 센서를 이용하여 사용자의 손이 센서에 접근하는 동작을 인식할 수 있다. 전자 장치(200)는 음성 센서를 이용하여 사용자가 음성을 입력하는 동작을 인식할 수 있다. 전자 장치(200)는 안면 센서를 이용하여 사용자의 얼굴이 센서에 접근하는 동작을 인식할 수 있다.

[0104] 한편, 전자 장치(200)는 보안 정보 입력 동작을 인식하기 위한 예비 동작을 수행할 수 있다. 예를 들어, 전자 장치(200)는, 사용자가 해당 센서 모듈에 대응하는 키 또는 터치 신호를 입력하거나, 음성 명령을 입력하거나, 제스처를 입력하는 경우, 사용자 보안 정보를 입력하는 화면으로 전환할 수 있다.

[0105] 또한, 전자 장치(200)는, 510 과정에서, 별도의 입력 장치(예: 250)를 이용하여 사용자의 보안 정보 입력 동작을 인식할 수 있다. 예를 들어, 전자 장치(200)는 입력 장치(250)를 이용하여 사용자가 개인 서명 정보를 입력하는 동작을 인식할 수 있다.

[0106] 한편, 전자 장치(200)는 보안 정보를 입력하는 동작을 인식하기 위한 예비 동작을 수행할 수 있다. 예를 들어, 사용자가 해당 입력 장치(250)에 대응하는 키 또는 터치 신호를 입력할 수 있고, 음성 명령을 입력할 수 있고, 제스처를 입력하여 사용자의 보안 정보를 입력하는 화면으로 전환할 수 있다.

[0107] 상기의 예들은 본 개시의 이해를 돕기 위한 것으로 본 개시를 이에 한정하는 것은 아니다.

[0108] 전자 장치(200)는 보안 정보 입력 동작을 감지하는 경우, 512 과정에서, 보안 정보 입력 동작에 대응하는 인터럽트(Interrupt)를 발생시켜 보안 영역(Secure World) 내 보안 정보 입력 모듈로 전달할 수 있다.

[0109] 인터럽트를 보안 영역(Secure World) 내 보안 정보 입력 모듈에 전달함에 있어서, 간접적으로 일반 영역(Normal World) 내 보안 정보 인식 드라이버를 이용하여 전달할 수 있고, 직접적으로 보안 영역(Secure World) 내 보안 정보 입력 모듈로 전달할 수도 있다.

[0110] 전자 장치(200)는, 514 과정에서, 일반 영역(Normal World) 또는 보안 영역(Secure World)을 통해 전달된 인터럽트에 대응하여 보안 영역(Secure World) 내 보안 정보 입력 모듈을 통해 사용자의 보안 정보(Security information)에 관한 원본 데이터(Raw data)를 읽을 수 있다.

[0111] 보안 정보 입력 모듈은 보안 영역(Secure World) 내 위치하므로 사용자의 보안 정보에 관한 원본 데이터(Raw data)를 입력 초기부터 외부의 악성 해킹 툴로부터 보호할 수 있다.

[0112] 전자 장치(200)는, 516 과정에서, 보안 정보에 관한 원본 데이터를 보안 정보 처리 모듈로 전달할 수 있다. 한편, 보안 정보 처리 모듈은 보안 정보 입력 모듈과 함께 보안 영역(Secure World) 내 존재할 수도 있고, 일반 영역(Normal World) 내 존재할 수도 있다.

[0113] 이렇게 전달된 보안 정보에 관한 원본 데이터(Raw data)는 보안 정보의 형판(Template)을 생성하고, 암호화(Encrypt)하는데 이용될 수 있으며, 궁극적으로는 제어 모듈의 보안 정보 인식 서비스를 통해 입력된 보안 정보를 기반으로 사용자를 식별할 수 있다.

[0114] 도 6은 다양한 실시 예에 따른, 보안 정보 처리 모듈의 블록도를 도시한다.

[0115] 도 6은 다양한 실시 예에 따른, 보안 영역의 보안 정보 처리 모듈 600은, 보안 데이터 생성부 610, 데이터 매칭부 620, 및 보안 처리부 630로 이루어질 수 있다.

[0116] 보안 데이터 생성부 610는, 센서 모듈로부터 획득한 보안 정보에 관한 원본(Raw) 데이터를 기초로 인식 객체의 고유 특징 정보를 산출할 수 있다.

[0117] 보안 데이터 생성부 610는, 산출된 고유 특징 정보를 보안 형판(Security template)으로 변환하여 보안 데이터를 생성할 수 있다. 상기 형판은 센서 모듈을 통해 취득된 보안 이미지 정보를 부호화 한 것일 수 있다.

[0118] 일 실시 예에 따르면, 보안 데이터 생성부 610는, 센싱 데이터로부터 보안 이미지(예; 지문 이미지, 홍채 이미지, 얼굴 이미지 등)를 획득할 수 있다. 예를 들면, 보안 이미지는 빛의 반사를 이용하는 광학식 또는 압력, 열, 초음파 등을 이용하는 비광학식으로 획득할 수 있다. 보안 데이터 생성부 310는, 보안 이미지를 기반으로 개인 고유의 특징 정보를 추출할 수 있다. 예를 들면, 지문 인식을 위한 특징 정보는 지문 인식일 경우, 선의 끝 점(ridge end)이나 분기점(bifurcation point), 중심점(core point), 삼각주(delta point) 등의 특징점(minutiae) 일 수 있다. 특징 정보는 등록된 보안 데이터와 매칭되는 정도를 확인하기 위해 기 설정된 포맷(또는 프레임) 형식으로 산출 될 수 있다. 예를 들면, 기 설정된 포맷의 정보 형식은 형판(Template) 형태일 수 있다.

[0119] 보안 데이터 생성부 610는, 보안 정보 등록 요청이 검출되면, 생성된 보안 데이터를 등록 정보로서 메모리에 저장할 수 있다. 여기서, 보안 정보 등록 요청은, 일반 영역으로부터 전달된 보안 신호를 통해 요청될 수 있다.

[0120] 데이터 매칭부 620는 보안 인증 요청이 검출되면, 인증을 위해 입력된 보안 인증 데이터가 기 등록된 보안 데이터와 매칭되는지 판단할 수 있다. 여기서, 보안 인증 요청은, 일반 영역으로부터 전달된 보안 신호를 통해 요청될 수 있다.

[0121] 일 실시예에서, 데이터 매칭부 620는, 보안 인증을 위해 입력된 원본(Raw) 데이터로부터 산출된 특징 정보를 기 등록된 적어도 하나의 보안 등록 데이터와 비교하고, 매칭값을 산출할 수 있다. 매칭값은 보안 인증 데이터가 보안 등록 데이터와 매칭되는 정보를 나타낸 값일 수 있다.

[0122] 예를 들면, 매칭값은 데이터 매칭 시 각각의 보안 데이터에 포함된 특징점들 중에서, 서로 대응되는(또는 서로 일치하는) 것으로 판단되는 특징점들의 개수를 나타낸 값으로 산출될 수 있다. 또는, 매칭값은 각각의 보안 데이터에 포함된 특징점들간의 거리, 방향 또는 특징점들의 배치 형태의 유사성 등을 고려하여 통계적 데이터 또는 확률적 함수에 따라 산출될 수 있다.

[0123] 데이터 매칭부 620는 특정 정보의 매칭값을 기준으로 보안 인증 성공 여부를 판단할 수 있다. 예를 들면, 데이

터 매칭부 620는 매칭값이 설정된 임계값을 초과하는 경우, 보안 인증이 성공된 것으로 판단하고, 매칭값이 설정된 임계값 이하인 경우, 보안 인증이 실패한 것으로 판단할 수 있다.

[0124] 데이터 매칭부 620는, 인증 성공 여부에 대한 결과 정보(예; 진위형 타입의 신호)를 일반 영역 내의 보안 정보 인식 서비스로 전달하도록 제어할 수 있다.

[0125] 보안 처리부 630는 보안 데이터를 암호화 및 복호화하도록 제어할 수 있다. 보안 처리부 630는 장치의 고유 식별 정보를 기반으로 유니크 키를 생성할 수 있다 예를 들면, 유니크 키는 보안 모드 시 접근 가능한 값일 수 있다.

[0126] 일 실시 예에서, 보안 처리부 630는 보안 정보 등록 시, 유니크 키를 이용하여 보안 데이터를 암호화하고, 암호화된 보안 데이터를 메모리의 보안 영역에 저장하도록 제어할 수 있다. 보안 처리부 630는 보안 정보 인증 시, 암호화된 보안 데이터를 메모리의 보안 영역으로부터 획득하고, 유니크 키를 이용하여 복호화할 수 있다. 보안 처리부 630는 복호화된 보안 데이터를 상기 데이터 매칭부로 전달할 수 있다. 이 경우, 유니크 키를 생성하기 위한 함수는 가상 보안 코어 시스템으로 동작 시 생성될 수 있는 값이며, 일반 보안 코어 시스템으로 동작 시 접근이 제한될 수 있다.

[0127] 일 실시 예에서, 보안 처리부 630는, 유니크 키를 이용해 보안 데이터를 암호화하고, 암호화된 보안 데이터를 일반 영역의 보안 정보 인식 서비스로 전달하도록 제어할 수 있다. 보안 처리부 630는 보안 인증 시, 일반 영역의 보안 정보 인식 서비스로부터 암호화된 보안 데이터를 전달받고, 암호화된 보안 데이터를 보안 모드에서 생성된 유니크 키를 이용하여 복호화할 수 있다. 보안 처리부는 복호화된 보안 데이터를 상기 데이터 매칭부로 전달할 수 있다.

[0128] 한 실시 예에서, 보안 처리부 630는 변형 함수를 통해 보안 데이터를 변형하여 모조 데이터(pseudo data)를 생성할 수 있다. 변형 함수는 일방 함수(one way), 데이터 배열 함수 등을 포함할 수 있으며, 보안 모드 시 또는 별도의 보안 하드웨어에서 획득 가능한 값을 이용한 함수를 이용할 수 있다. 변형 함수는 보안 데이터의 메타데이터로 저장될 수 있다.

[0129] 보안 처리부 630는 생성된 모조 데이터를 데이터 매칭부 620 및 데이터 생성부 610로 전달할 수 있다. 예를 들면, 데이터 생성부 610는 모조 데이터를 등록 정보로서 저장할 수 있다. 데이터 매칭부 620는 등록된 모조 데이터와, 새로 생성된 모조 데이터를 비교함으로써, 보안 인증 성공 여부를 판단할 수 있다.

[0130] 보안 처리부 630는 모조 데이터를 생성하기 위한 변형 함수를 가변적으로 운용할 수 있다. 예를 들면, 보안 인증 정보가 의도하지 않게 외부로 노출될 경우, 보안 처리부 630는 변형 함수를 변경하고, 변경된 변형 함수를 통해 모조 데이터를 새롭게 생성할 수 있다. 외부 노출 시 보안 데이터의 메타 데이터 역시 갱신되므로, 보안 처리부 630는 기존의 보안 데이터를 새로 갱신하거나 폐기하도록 처리할 수 있다.

[0131] 다양한 실시 예에 따르면, 하나의 프로세서를 통해 일반 영역 및 보안 영역으로 동작되는 전자 장치에 있어서, 보안 인증을 위한 센서 모듈 및 일반 영역에서 센서 모듈로부터 생체 정보 입력 이벤트를 검출하고, 상기 일반 영역에서 보안 정보 입력 이벤트를 보안 영역으로 전달하고, 상기 보안 영역에서 보안 정보 입력 이벤트에 응답하여 센서 모듈로부터 센싱 데이터를 획득하고, 상기 보안 영역에서 획득된 센싱 데이터를 처리하여 보안 정보 등록 결과 및 보안 인증 결과에 관한 정보를 일반 영역으로 전달하도록 제어하는 프로세서를 포함할 수 있다.

[0132] 상기 프로세서는, 보안 영역에서, 센싱 데이터로부터 특징 정보를 산출하고, 특징 정보를 기반으로 보안 데이터를 생성하고, 상기 보안 데이터를 고유의 식별 정보를 기반으로 생성된 유니크 키를 이용하여 암호화하고, 암호화된 보안 데이터를 등록하도록 제어할 수 있다.

[0133] 상기 프로세서는, 상기 암호화된 보안 데이터를 일반 영역으로 전달하고, 일반 영역에서 암호화된 보안 데이터를 저장할 수 있다.

[0134] 상기 프로세서는, 보안 영역 또는 일반 영역으로 할당된 메모리로부터 암호화된 등록 데이터를 획득하고, 암호화된 등록 데이터를 고유의 식별 정보를 기반으로 생성된 유니크 키를 이용하여 복호화하고, 복호화된 등록 데이터와 생성된 보안 데이터를 비교하여 보안 인증을 수행하고, 상기 비교 결과, 데이터의 매칭값이 설정된 임계값을 초과하는 경우, 보안 인증 성공으로 판단하고, 매칭 값이 설정된 임계값 이하인 경우, 보안 인증 실패로 판단할 수 있다.

[0135] 상기 프로세서는, 등록 또는 인증 결과에 대응하는 진위형 타입의 신호로 전달할 수 있다.

[0136] 도 7는 다양한 실시 예에 따른, 전자 장치의 보안 정보 등록 방법을 도시한다.

[0137] 도 7를 참조하면, 보안 정보 등록(예; 등록 모드)을 위해 동작 710에서 프로세서는 일반 영역에서 센서 모듈로부터 전달되는 인터럽트 신호를 기반으로 보안 정보 입력 이벤트를 검출할 수 있다. 프로세서는 상기 일반 영역에서 보안 정보 등록을 위한 기능 요청이 발생되면, 센서 모듈을 활성화시키고, 센서 모듈을 통해 인식 객체를 센싱할 수 있다. 예를 들면, 전자 장치는 지문 센서를 이용하여 사용자가 손가락을 센서와 접촉하는 동작을 인식할 수 있다. 전자 장치는 홍채 센서를 이용하여 사용자의 눈이 센서에 접근하는 동작을 인식할 수 있다. 전자 장치는 정맥 센서를 이용하여 사용자의 손이 센서에 접근하는 동작을 인식할 수 있다. 전자 장치는 음성 센서를 이용하여 사용자가 음성을 입력하는 동작을 인식할 수 있다. 전자 장치는 안면 센서를 이용하여 사용자의 얼굴이 센서에 접근하는 동작을 인식할 수 있다.

[0138] 동작 720에서, 프로세서는, 보안 정보 입력 이벤트가 검출되면, 가상 보안 코어 시스템을 호출하기 위해 이벤트 검출 신호를 보안 영역으로 전달할 수 있다. 이때, 이벤트 검출 신호는 보안 인터럽트 신호일 수 있다.

[0139] 동작 730에서, 프로세서는 보안 영역에서, 센서 모듈로부터 센싱 데이터를 획득할 수 있다. 센싱 데이터는 보안 정보의 원본 데이터(Raw data)일 수 있다. 예를 들면, 센싱 데이터는, 사용자의 지문, 손 무늬, 망막 패턴, 홍채 패턴, 혈관 패턴, 귀 모양, 얼굴 모양, 사용자의 음성 및 필체 정보 중 적어도 하나를 포함할 수 있다.

[0140] 동작 740에서 프로세서는 보안 영역에서, 센싱 데이터를 기반으로 인식 객체의 고유 특징 정보를 산출할 수 있다. 예를 들면, 프로세서는, 센싱 데이터로부터 센싱 이미지를 획득하고, 센싱 이미지로부터 특징 정보를 추출할 수 있다.

[0141] 동작 750에서, 프로세서는 보안 영역에서, 특징 정보를 형판(template)으로 변환하여 보안 데이터를 생성할 수 있다.

[0142] 동작 760에서, 프로세서는 보안 영역에서, 보안 데이터를 암호화할 수 있다. 예를 들면, 프로세서는 보안 영역에서 장치의 고유 식별 정보를 기반으로 유니크 키를 생성할 수 있다. 유니크 키는 보안 모드 시 접근 가능한 값일 수 있다. 예를 들면, 프로세서는, 유니크 키 생성을 위한 함수 정보를 보안 영역으로 할당된 메모리에 저장하고, 보안 모드 시 함수 정보를 통해 유니크 키를 생성할 수 있다. 한편, 동작 760은 생략될 수 있으나, 이에 한정하는 것은 아니다.

[0143] 동작 765에서 프로세서는 보안 영역에서, 암호화된 보안 데이터를 일반 영역으로 전달할 수 있다. 예를 들면, 프로세서는 일반영역에서, 암호화된 보안 데이터를 일반 영역으로 할당된 메모리(예; REE file system)에 저장할 수 있다.

[0144] 동작 770에서 프로세서는 보안 영역에서, 보안 데이터 또는 암호화된 보안 데이터를 보안 인증을 위한 등록 정보로 저장 및 등록할 수 있다.

[0145] 일 실시 예에서, 프로세서는 보안 데이터를 보안 모드 시 접근 가능한 보안 영역에 저장 및 등록할 수 있다.

[0146] 일 실시 예에서, 프로세서는, 암호화 시 이용된 유니크 키 또는 유니크 키 생성을 위한 함수 정보를 보안 모드 시 접근 가능한 보안 영역에 저장하고, 암호화된 보안 데이터는 일반 영역으로 전달할 수 있다. 프로세서는 일반 영역에서, 보안 영역으로부터 전달받은 암호화된 보안 데이터를 접근 제한이 없는 일반 영역에 저장 및 등록할 수 있다.

[0147] 동작 780에서 프로세서는 보안 영역에서, 보안 정보 등록 결과를 일반 영역으로 전달할 수 있다.

[0148] 동작 790에서, 프로세서는 일반 영역에서, 가상의 일반 코어를 통해 보안 정보의 등록이 완료되었음을 알리는 정보를 사용자 인터페이스 또는 전자 장치의 구성요소를 통해 사용자에게 제공할 수 있다.

[0149] 한편, 프로세서는, 원본(Raw) 데이터의 품질 저하 등의 원인으로 보안 정보 등록이 실패할 경우, 재등록 절차를 수행하도록 처리할 수 있다. 이를 위해, 프로세서는 일반 영역에서, 등록 실패에 대한 피드백(예; 시각적, 청각적, 후각적, 촉각적 효과 등) 및 새로운 센싱 데이터의 획득 중 적어도 하나를 사용자 인터페이스를 통해 제공되도록 제어할 수 있다.

[0150] 도 8는 다양한 실시 예에 따른, 전자 장치의 보안 정보 인증 방법을 도시한다.

[0151] 도 8를 참조하면, 보안 정보 인증(예; 인증 모드)을 위해 동작 810에서 프로세서는, 일반 영역에서 센서 모듈로부터 전달되는 인터럽트 신호를 기반으로 보안 정보 인증 이벤트를 검출할 수 있다. 프로세서는 일반 영역에서,

보안 정보 인증을 위한 기능 요청이 발생되면, 센서 모듈을 활성화시키고, 센서 모듈을 통해 인식 객체를 센싱할 수 있다.

[0152] 동작 820에서 프로세서는 일반 영역에서, 보안 정보 입력 이벤트가 검출되면, 이벤트 검출 신호를 보안 영역으로 전달할 수 있다. 이때, 이벤트 검출 신호는 보안 인터럽트 신호일 수 있다.

[0153] 동작 830에서, 프로세서는 보안 영역에서, 센서 모듈로부터 센싱 데이터를 획득할 수 있다. 동작 840에서, 프로세서는 보안 영역에서, 센싱 데이터를 기반으로 인식 객체의 고유 특징 정보를 산출하고, 보안 정보 인증을 위한 보안 인증 데이터를 생성할 수 있다. 여기서, 보안 인증 데이터는 기 설정된 포맷 예를 들면, 템플릿 형태일 수 있다.

[0154] 동작 850에서 프로세서는 보안 영역에서, 일반 영역으로부터 암호화된 보안 등록 데이터를 전달받거나, 보안 영역으로 할당된 메모리로부터 암호화된 보안 등록 데이터를 획득할 수 있다.

[0155] 동작 860에서 프로세서는 보안 영역에서, 저장된 보안 등록 데이터(예; 암호화된 생체 데이터)를 복호화할 수 있다. 예를 들면, 프로세서는 보안 영역에서, 암호화된 보안 데이터가 획득되면, 암호화된 보안 데이터를 유니크 키를 이용하여 복호화할 수 있다. 프로세서는, 유니크 키 생성을 위한 함수 정보를 접근 제한이 있는 보안 영역으로 할당된 메모리로부터 획득하고, 획득된 함수 정보를 통해 유니크 키를 생성할 수 있다.

[0156] 동작 870에서 프로세서는 보안 영역에서, 보안 인증 데이터 및 보안 등록 데이터로부터 산출된 특징 정보를 비교하여 매칭값을 산출할 수 있다.

[0157] 동작 880에서 프로세서는 보안 영역에서, 특징 정보의 매칭값을 기준으로 보안 인증 성공 여부를 판단할 수 있다. 예를 들면, 프로세서는, 매칭값이 설정된 임계값을 초과하는 경우, 보안 인증 성공으로 판단할 수 있고, 매칭값이 설정된 임계값 이하인 경우, 보안 인증 실패로 판단할 수 있다.

[0158] 동작 885에서 프로세서는 보안 영역에서, 보안 정보 인증 결과를 일반 영역으로 전달할 수 있다. 동작 890에서 프로세서는 일반 영역에서, 보안 정보 인증 결과를 사용자 인터페이스 또는 전자 장치의 구성요소를 통해 사용자에게 제공할 수 있다.

[0159] 한편, 프로세서는, 원본(Raw) 데이터의 품질 저하 등의 원인으로 보안 정보 인증이 실패할 경우, 재 인증 절차를 수행하도록 처리할 수 있다. 이를 위해, 프로세서는 일반 영역에서, 인증 실패에 대한 피드백(예; 시각적, 청각적, 촉각적, 후각적 효과 등) 및 새로운 센싱 데이터의 획득 중 적어도 하나를 사용자 인터페이스를 통해 제공되도록 제어할 수 있다.

[0160] 다양한 실시예들에 따르면, 본 개시에 따른 장치(예: 모듈들 또는 그 기능들) 또는 방법(예: 동작들)의 적어도 일부는, 예컨대, 프로그래밍 모듈의 형태로 컴퓨터로 읽을 수 있는 저장매체(computer-readable storage media)에 저장된 명령어로 구현될 수 있다. 상기 명령어는, 하나 이상의 프로세서 (예: 상기 프로세서, 210)에 의해 실행될 경우, 상기 하나 이상의 프로세서가 상기 명령어에 해당하는 기능을 수행할 수 있다. 컴퓨터로 읽을 수 있는 저장매체는, 예를 들면, 상기 메모리(230)가 될 수 있다. 상기 프로그래밍 모듈의 적어도 일부는, 예를 들면, 상기 프로세서(210)에 의해 구현(implement)(예: 실행)될 수 있다. 상기 프로그래밍 모듈의 적어도 일부는 하나 이상의 기능을 수행하기 위한, 예를 들면, 모듈, 프로그램, 루틴, 명령어 세트 (sets of instructions) 또는 프로세스 등을 포함할 수 있다.

[0161] 상기 컴퓨터로 판독 가능한 기록 매체에는 하드디스크, 플로피디스크 및 자기 테이프와 같은 마그네틱 매체(Magnetic Media)와, CD-ROM(Compact Disc Read Only Memory), DVD(Digital Versatile Disc)와 같은 광기록 매체(Optical Media)와, 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media)와, 그리고 ROM(Read Only Memory), RAM(Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령(예: 프로그래밍 모듈)을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함될 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 본 개시의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지다.

[0162] 본 개시에 따른 모듈 또는 프로그래밍 모듈은 전술한 구성요소들 중 적어도 하나 이상을 포함하거나, 일부가 생략되거나, 또는 추가적인 다른 구성요소를 더 포함할 수 있다. 본 개시에 따른 모듈, 프로그래밍 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.

[0163] 본 명세서와 도면에 개시된 실시 예들은 본 명세서에 개시된 다양한 실시예들의 내용을 쉽게 설명하고, 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 명세서에 개시된 다양한 실시예들의 범위를 한정하고자 하는 것은 아니다. 따라서 본 명세서에 개시된 다양한 실시예들의 범위는 여기에 개시된 실시 예들 이외에도 본 명세서에 개시된 다양한 실시예들의 기술적 사상을 바탕으로 도출되는 모든 변경 또는 변형된 형태가 본 명세서에 개시된 다양한 실시예들의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0164] 300: 센서 모듈 310: 일반 영역

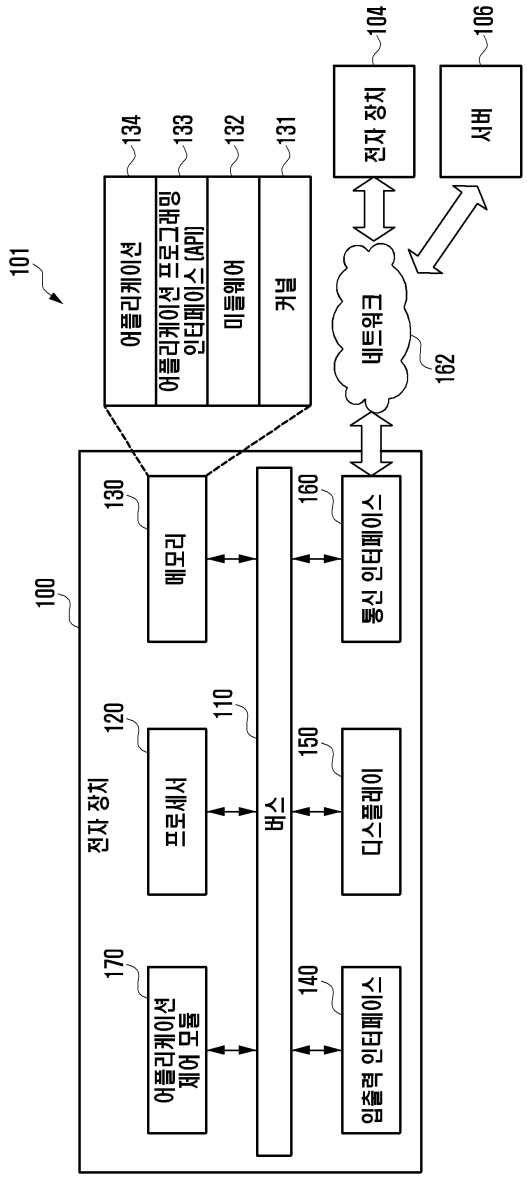
312: 보안 정보 인식 드라이버 314: 제어 모듈

316: 보안 정보 인식 App 320: 보안 영역

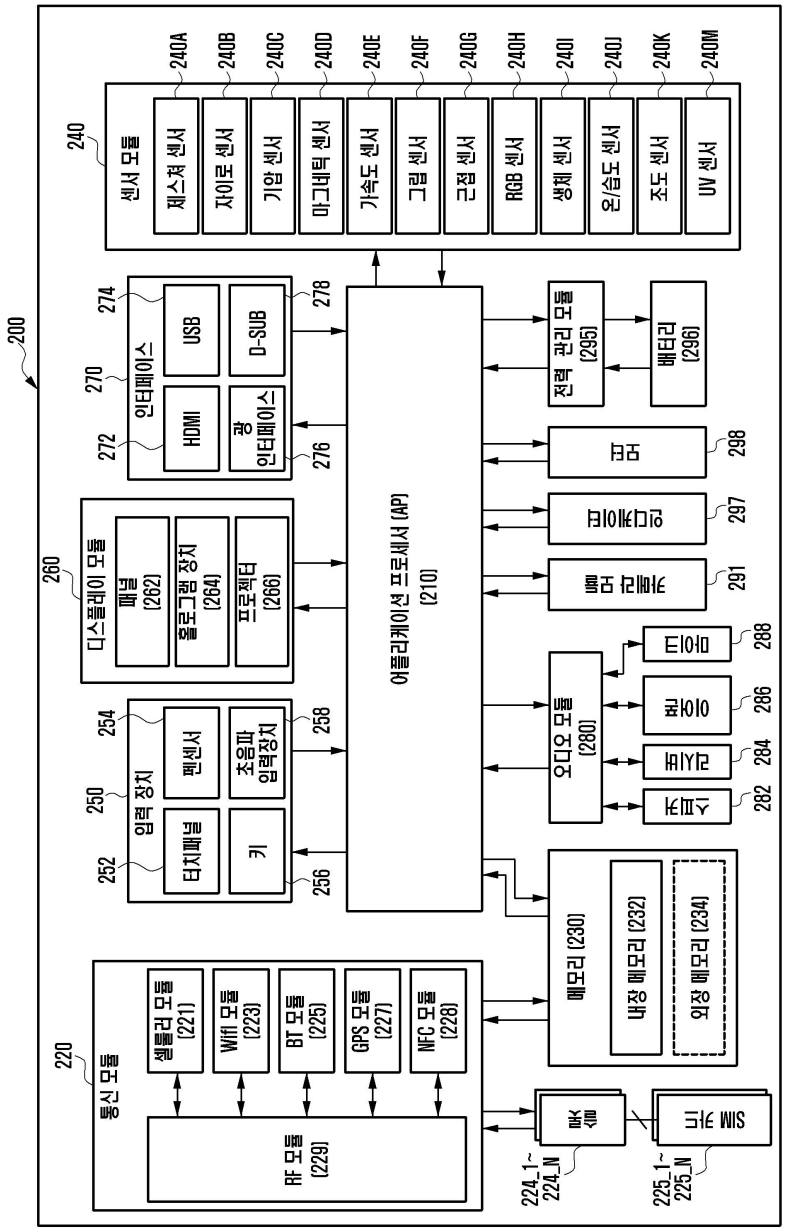
322: 보안 정보 입력 모듈 324: 보안 정보 처리 모듈

도면

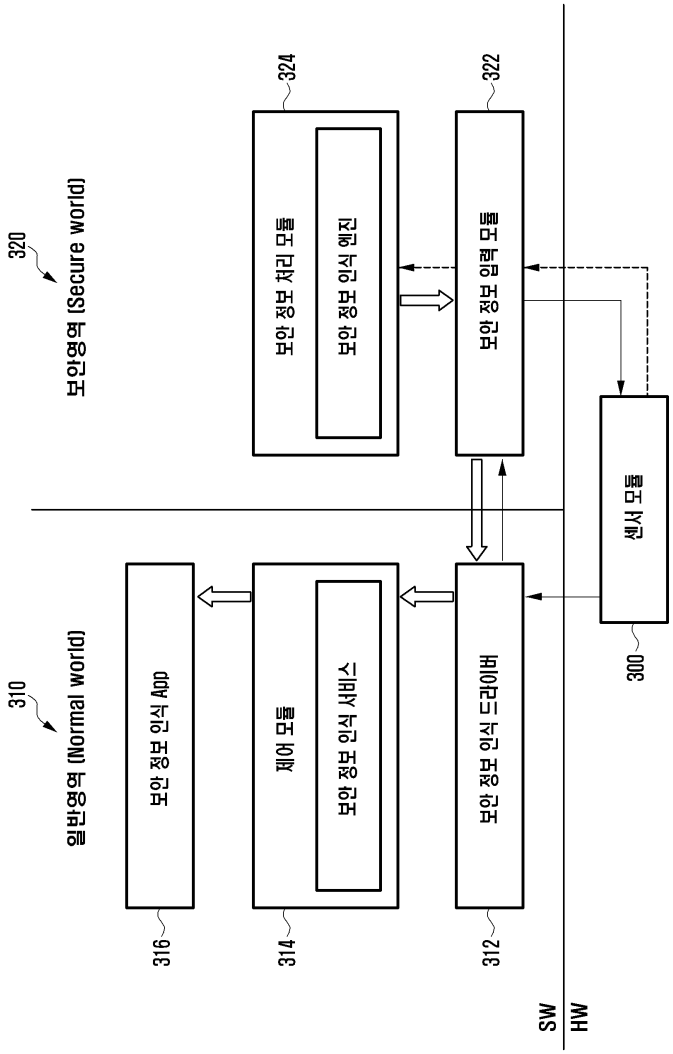
도면1



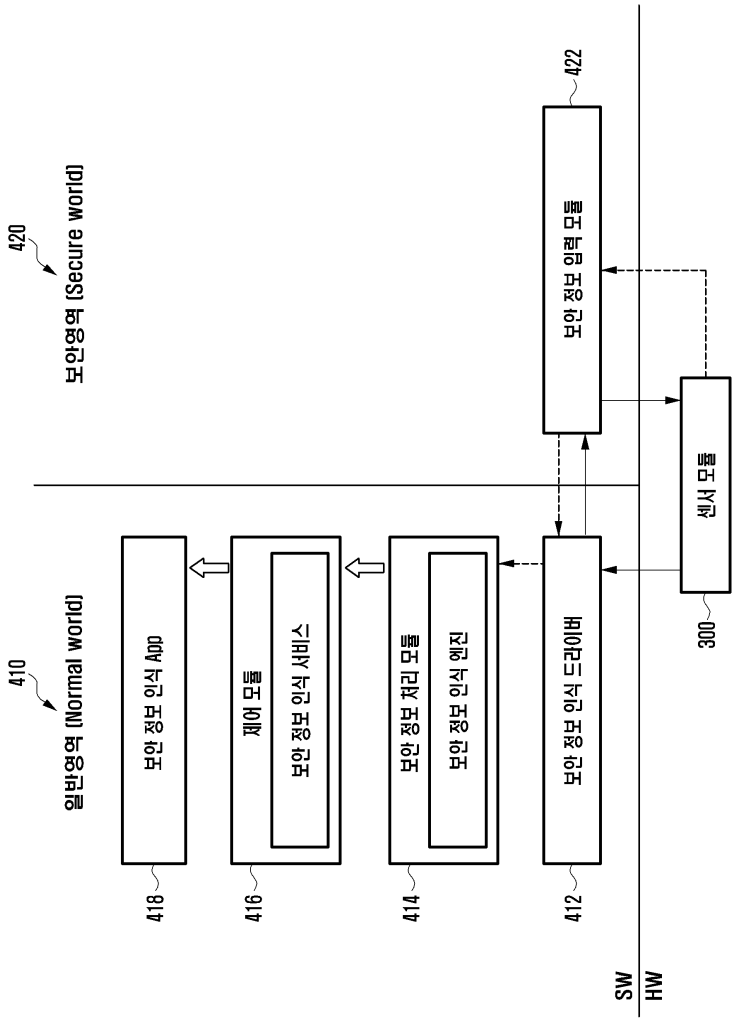
도면2


200
220
통신 모듈
셀룰러 모듈 (221)
Wifi 모듈 (223)
BT 모듈 (225)
GPS 모듈 (227)
NFC 모듈 (228)
RF 모듈 (229)
224_1~224_N
안테나
225_1~225_N
SIM 카드
메모리 (230)
내장 메모리 (232)
외장 메모리 (234)
240
센서 모듈
240A 제스쳐 센서
240B 자이로 센서
240C 기압 센서
240D 마그네틱 센서
240E 가속도 센서
240F 그립 센서
240G 근접 센서
240H RGB 센서
240I 생체 센서
240J 온/습도 센서
240K 조도 센서
240M UV 센서
260
디스플레이 모듈
패널 (262)
홀로그램 장치 (264)
프로젝터 (266)
270
인터페이스
272 HDMI
274 USB
276 광 인터페이스
278 D-SUB
250
입력 장치
252 터치패널
254 펜센서
256 키
258 초음파 입력장치
어플리케이션 프로세서 (AP) (210)
오디오 모듈 (280)
282 스피커
284 리시버
286 마이크
288 이어폰
전력 관리 모듈 (295)
배터리 (296)
297 인디케이터
291 가입자 식별
298 모터

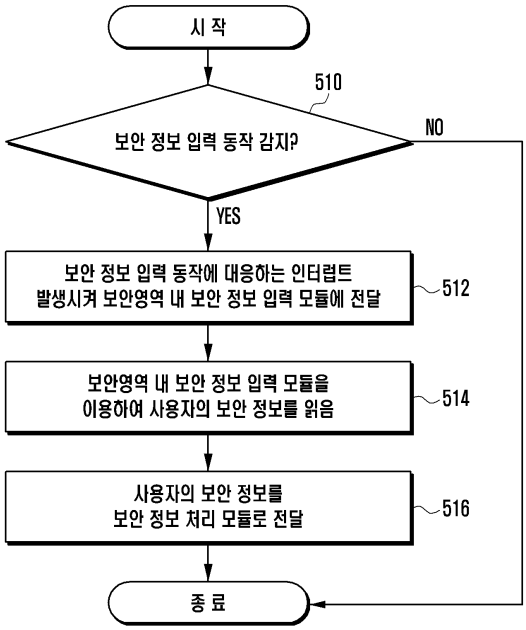
도면3


320
보안영역 (Secure world)
324
보안 정보 처리 모듈
보안 정보 인식 엔진
322
보안 정보 입력 모듈
센서 모듈
300
310
일반영역 (Normal world)
보안 정보 인식 App
316
제어 모듈
보안 정보 인식 서비스
314
보안 정보 인식 드라이버
312
SW
HW

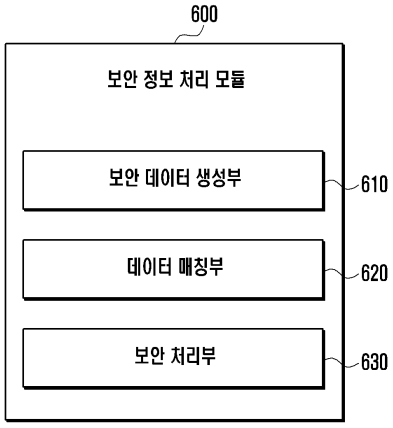
도면4


420
보안영역 (Secure world)
410
일반영역 (Normal world)
422
보안 정보 입력 모듈
센서 모듈
300
보안 정보 인식 드라이버
412
보안 정보 처리 모듈
보안 정보 인식 엔진
414
제어 모듈
보안 정보 인식 서비스
416
보안 정보 인식 App
418
SW
HW

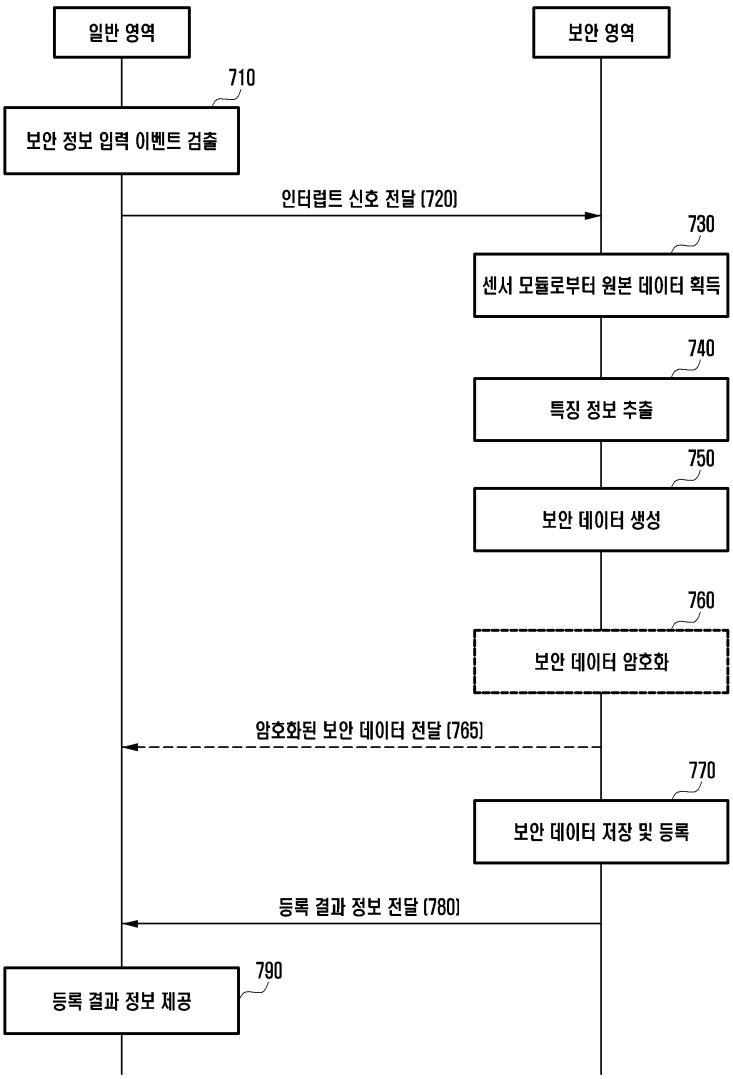
도면5


시 작
510
보안 정보 입력 동작 감지?
NO
YES
보안 정보 입력 동작에 대응하는 인터럽트 발생시켜 보안영역 내 보안 정보 입력 모듈에 전달
512
보안영역 내 보안 정보 입력 모듈을 이용하여 사용자의 보안 정보를 읽음
514
사용자의 보안 정보를 보안 정보 처리 모듈로 전달
516
종 료

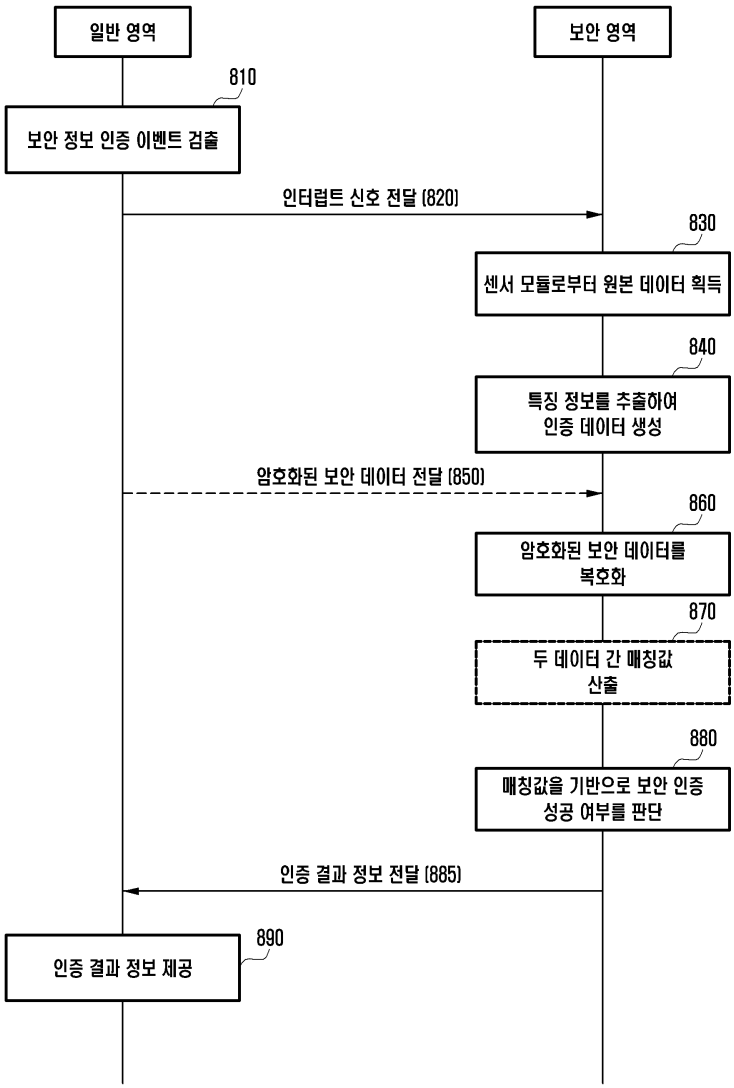
도면6


600
보안 정보 처리 모듈
보안 데이터 생성부
610
데이터 매칭부
620
보안 처리부
630

도면7


일반 영역
보안 영역
710
보안 정보 입력 이벤트 검출
인터럽트 신호 전달 (720)
730
센서 모듈로부터 원본 데이터 획득
740
특징 정보 추출
750
보안 데이터 생성
760
보안 데이터 암호화
암호화된 보안 데이터 전달 (765)
770
보안 데이터 저장 및 등록
등록 결과 정보 전달 (780)
790
등록 결과 정보 제공

도면8


일반 영역
보안 영역
810
보안 정보 인증 이벤트 검출
인터럽트 신호 전달 (820)
830
센서 모듈로부터 원본 데이터 획득
840
특징 정보를 추출하여
인증 데이터 생성
암호화된 보안 데이터 전달 (850)
860
암호화된 보안 데이터를
복호화
870
두 데이터 간 매칭값
산출
880
매칭값을 기반으로 보안 인증
성공 여부를 판단
인증 결과 정보 전달 (885)
890
인증 결과 정보 제공