



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0111586
(43) 공개일자 2022년08월09일

(51) 국제특허분류(Int. Cl.)

G06F 21/50 (2013.01) G06F 21/72 (2013.01)
G06F 21/78 (2013.01) H04L 65/40 (2022.01)
H04L 9/08 (2006.01) H04L 9/30 (2006.01)

(52) CPC특허분류

G06F 21/50 (2013.01)
G06F 21/72 (2013.01)

(21) 출원번호 10-2021-0015015

(22) 출원일자 2021년02월02일

심사청구일자 2021년02월02일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

(72) 발명자

조진성

경기도 수원시 영통구 봉영로1517번길 73, 922동 1401호(영통동, 삼성.태영 아파트)

정준영

경기도 부천시 역곡로471번가길 19-8, 402호(고강동, 월드빌리지)

(뒷면에 계속)

(74) 대리인

유미특허법인

전체 청구항 수 : 총 13 항

(54) 발명의 명칭 IoT 장치에서의 ARM PSA 기반 보안 플랫폼 장치

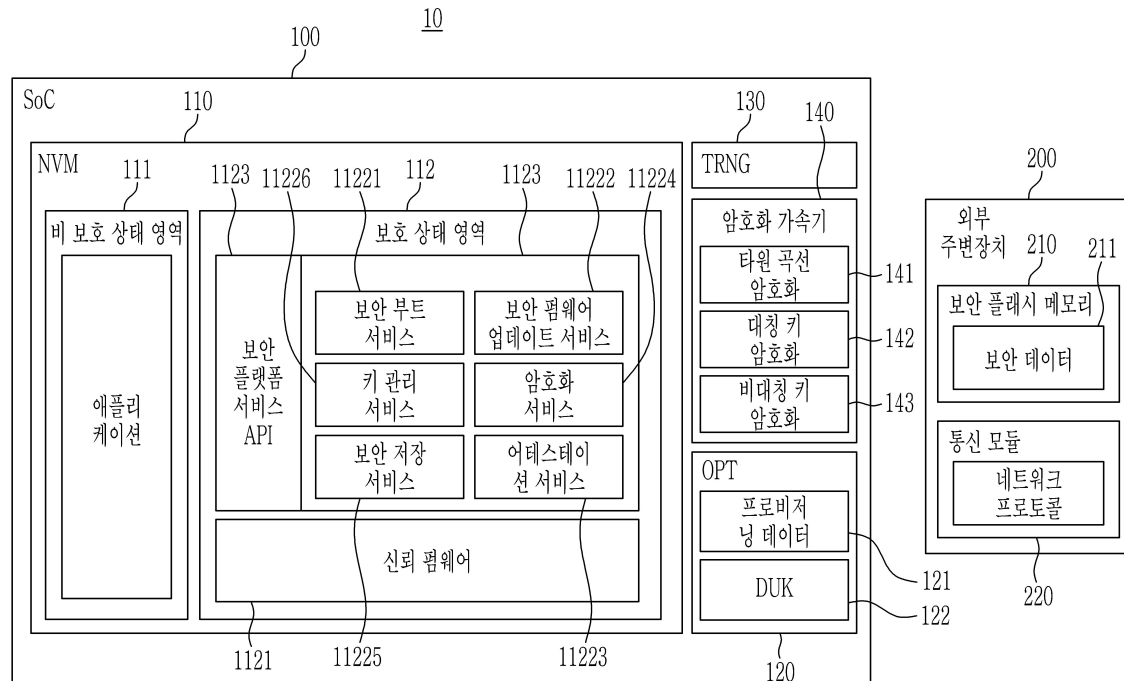
(57) 요약

IoT 장치에서의 ARM PSA 기반 보안 플랫폼 장치가 개시된다.

이 장치는 사물인터넷 장치에 탑재되는 보안 플랫폼 장치로서, 외부 주변장치 및 SoC를 포함한다. 외부 주변장치는 사물인터넷 장치에서 센싱되는 센서 데이터가 암호화되어 저장되는 보안 플래시 메모리를 포함한다. SoC는

(뒷면에 계속)

대표도



펌웨어 저장소 및 암호화 가속기를 포함한다. 펌웨어 저장소는 사물인터넷 서비스를 제공하는 애플리케이션을 저장하는 비 보안 상태 영역, 그리고 사물인터넷 장치에 대한 보안 플랫폼 서비스를 제공하는 데 사용되는 복수의 보안 플랫폼 서비스를 저장하는 보안 상태 영역을 포함한다. 암호화 가속기는 복수의 암호화 알고리즘을 포함하며, 외부 주변장치의 보안 플래시 메모리에 저장된 센서 데이터에 대한 복수의 보안 플랫폼 서비스 중 일부의 접근이 가능하도록 한다. 보안 상태 영역 내의 복수의 보안 플랫폼 서비스 중 일부는 비 보안 상태 영역에 저장된 애플리케이션에 의해 호출되어 사용 가능하다.

(52) CPC특허분류

G06F 21/78 (2013.01)

H04L 67/12 (2022.05)

H04L 9/0825 (2013.01)

H04L 9/0877 (2013.01)

H04L 9/3066 (2013.01)

공지상

경기도 성남시 분당구 분당로311번길 10-10, 201호(분당동)

(72) 발명자

김법석

경기도 수원시 팔달구 권광로 246, 105동 2502호(인계동, 래미안 노블클래스)

이 발명을 지원한 국가연구개발사업

과제고유번호	1345316564
과제번호	2017R1D1A1B04035914
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(교육부)(R&D)
연구과제명	IoT 디바이스 신뢰 플랫폼 개발 및 오픈소스 SW로의 공개
기 여 율	1/1
과제수행기관명	경희대학교(국제캠퍼스)
연구기간	2020.03.01~2021.02.28

명세서

청구범위

청구항 1

사물인터넷 장치에 탑재되는 보안 플랫폼 장치로서,

상기 사물인터넷 장치에서 센싱되는 센서 데이터가 암호화되어 저장되는 보안 플래시 메모리를 포함하는 외부 주변 장치, 그리고

펌웨어 저장소 — 상기 펌웨어 저장소는,

사물인터넷 서비스를 제공하는 애플리케이션을 저장하는 비 보안 상태 영역, 그리고

사물인터넷 장치에 대한 보안 플랫폼 서비스를 제공하는 데 사용되는 복수의 보안 플랫폼 서비스를 저장하는 보안 상태 영역

을 포함함 —, 그리고

복수의 암호화 알고리즘을 포함하며, 상기 외부 주변장치의 보안 플래시 메모리에 저장된 센서 데이터에 대한 상기 복수의 보안 플랫폼 서비스 중 일부의 접근이 가능하도록 하는 암호화 가속기

를 포함하는 SoC(System on Chip)

를 포함하며,

상기 보안 상태 영역 내의 복수의 보안 플랫폼 서비스 중 일부는 상기 비 보안 상태 영역에 저장된 애플리케이션에 의해 호출되어 사용 가능한,

보안 플랫폼 장치.

청구항 2

제1항에 있어서,

상기 복수의 보안 플랫폼 서비스는,

상기 사물인터넷 장치의 구성요소에 대한 검사를 수행하는 어테스테이션(Attestation) 서비스,

상기 암호화 가속기에 포함된 암호화 알고리즘을 사용하여 데이터에 대한 암호화 서비스를 제공하는 암호화 서비스, 그리고

상기 암호화 가속기를 통해 상기 외부 주변장치의 보안 플래시 메모리에 센서 데이터를 저장하고, 상기 보안 플래시 메모리에 저장된 센서 데이터를 읽는 기능을 제공하는 보안 저장 서비스

를 포함하는, 보안 플랫폼 장치.

청구항 3

제2항에 있어서,

상기 SoC는 상기 사물인터넷 장치의 제조 과정에서 주입된 프로비저닝 데이터 및 DUK(Device Unique Key)를 저장하고 있는 OTP(One-Time Programmable) 메모리

를 더 포함하고,

상기 복수의 보안 플랫폼 서비스는,

상기 OTP 메모리에 저장된 정보를 사용하여, 상기 보안 플래시 메모리에 저장되는 센서 데이터에 대한 암호화 및 복호화시 사용되는 유도 키(Derived Key)를 생성하거나 제거하는 키 관리 서비스

를 더 포함하는, 보안 플랫폼 장치.

청구항 4

제3항에 있어서,

상기 보안 상태 영역은,

상기 비 보안 상태 영역에 저장된 애플리케이션이 상기 보안 상태 영역 내의 복수의 보안 플랫폼 서비스 중 일부를 호출하는 데 사용되는 API(Application Program Interface)를 더 포함하며,

상기 API는 상기 복수의 보안 플랫폼 서비스 각각이 제공하는 기능을 호출하기 위한 대응하는 함수를 포함하는, 보안 플랫폼 장치.

청구항 5

제2항에 있어서,

상기 SoC는 알고리즘이 아닌 물리적 프로세스로부터 난수를 생성하는 난수 생성기(True Random Number Generator, TRNG)

를 더 포함하는, 보안 플랫폼 장치.

청구항 6

제1항에 있어서,

상기 외부 주변장치는 상기 사물인터넷이 외부의 클라우드 서버와의 보안 채널을 통한 통신이 가능하도록 하는 유무선 네트워크 통신 수단

을 더 포함하는, 보안 플랫폼 장치.

청구항 7

제1항에 있어서,

상기 암호화 가속기는,

타원 곡선을 이용한 전자 서명 알고리즘인 타원 곡선 암호화 알고리즘,

하나의 비밀 키로 데이터의 암호화와 복호화를 가능하게 하는 대칭 키 암호화 알고리즘, 그리고

공개 키와 개인 키를 사용하여 데이터의 암호화와 복호화를 가능하게 하는 비대칭 키 암호화 알고리즘

을 포함하는, 보안 플랫폼 장치.

청구항 8

제4항에 있어서,

상기 API는,

상기 사물인터넷의 구성요소의 점검을 위해 상기 어테스테이션 서비스를 호출하는 데 사용되는 함수,

상기 암호화 가속기에 포함된 암호화 알고리즘을 사용하기 위해 상기 암호화 서비스를 호출하는 데 사용되는 함수,

상기 보안 플래시 메모리에 대한 접근을 위해 상기 보안 저장 서비스를 호출하는 데 사용되는 함수, 그리고

상기 유도 키(Derived Key)를 생성하거나 삭제하기 위해 상기 키 관리 서비스를 호출하는 데 사용되는 함수

를 포함하는, 보안 플랫폼 장치.

청구항 9

제8항에 있어서,

상기 암호화 서비스를 호출하는 데 사용되는 함수는,

디지털 서명을 생성하기 위해 사용되는 함수,
 상기 암호화 가속기에 포함된 대칭 키 알고리즘을 사용하기 위해 사용되는 함수,
 상기 암호화 가속기에 포함된 비 대칭 키 알고리즘을 사용하기 위해 사용되는 함수, 그리고
 해시 값을 생성하기 위해 사용되는 함수
 를 포함하는, 보안 플랫폼 장치.

청구항 10

제8항에 있어서,
 상기 보안 저장 서비스를 호출하는 데 사용되는 함수는,
 상기 보안 플래시 메모리에 센서 데이터를 저장하기 위해 사용되는 함수, 그리고
 상기 보안 플래시 메모리에 저장된 센서 데이터를 로딩하기 위해 사용되는 함수
 를 포함하는, 보안 플랫폼 장치.

청구항 11

제8항에 있어서,
 상기 키 관리 서비스를 호출하는 데 사용되는 함수는,
 상기 OTP 메모리에 저장되어 있는 DUK를 사용하여 상기 유도 키를 생성하기 위해 사용되는 함수, 그리고
 상기 유도 키를 삭제하기 위해 사용되는 함수
 를 포함하는, 보안 플랫폼 장치.

청구항 12

제5항에 있어서,
 상기 API는,
 상기 난수 생성기를 사용하여 난수 값을 발생하기 위해 사용되는 함수
 를 포함하는, 보안 플랫폼 장치.

청구항 13

제1항 내지 제12항 중 어느 한 항에 있어서,
 상기 보안 플랫폼 장치는, ARM(Acorn RISC Machine)의 PSA(Platform Security Architecture) 기반의 플랫폼 장치인,
 보안 플랫폼 장치.

발명의 설명

기술 분야

[0001] 본 발명은 IoT 장치에서의 ARM PSA 기반 보안 플랫폼 장치에 관한 것이다.

배경 기술

[0002] 기술과 인터넷의 발전으로 다양한 임베디드 플랫폼과 센서의 개발이 진행되었고, 그에 따라 IoT(Internet of Things, 사물인터넷) 사회가 도래하였다. 이러한 IoT를 구성하는 대부분의 장치는 저사양으로 개발되기 때문에, 서버와 PC(Personal Computer) 위주의 기존 보안 솔루션을 적용하기엔 어려움이 있다.

[0003] 이를 해결하기 위해 ARM(Acorn RISC Machine)에서는 하드웨어 및 소프트웨어 리소스를 두 개의 영역(Secure

world, Non-secure world)으로 격리하여 IoT 장치의 보안성을 향상시키는 ARM 프로세서 기반의 상용 TEE(Trusted Execution Environment)인 TrustZone을 제안하였다. 이와 더불어, ARM은 최근 저사양 마이크로 컨트롤러를 위한 보안 플랫폼인 PSA(Platform Security Architecture)를 새롭게 공개하였다.

- [0004] ARM의 파트너 기업은 PSA를 통해 보안이 강화된 새로운 IoT 플랫폼 및 서비스의 개발을 할 수 있으며, 이를 통해 안전한 IoT 생태계를 구축할 수 있다.
- [0005] 그러나, PSA 적용이 가능한 IoT 서비스를 개발하기 위해 플랫폼 제조사는 ARM과 NDA(Non-Disclosure Agreements)를 맺어야 하며, PSA 적용이 가능한 하드웨어 사용이 익숙하지 못한 어플리케이션 개발자는 안전한 IoT 서비스 개발에 어려움을 느낄 수 있다.
- [0006] 따라서, 보안 강화에 대한 가능성이 있음에도 불구하고, PSA를 활용한 IoT 서비스의 연구와 개발이 상대적으로 이뤄지지 않고 있다는 문제점이 있다.

발명의 내용

해결하려는 과제

- [0007] 본 발명이 해결하고자 하는 과제는 IoT 서비스 어플리케이션 개발자의 개발 편의성을 제공하기 위한 IoT 장치에서의 ARM PSA 기반 보안 플랫폼 장치를 제공하는 것이다.

과제의 해결 수단

- [0008] 상기한 바와 같은 본 발명의 과제를 달성하고, 후술하는 본 발명의 특징적인 효과를 실현하기 위한, 본 발명의 특징적인 구성은 하기와 같다.
- [0009] 본 발명의 일 측면에 따르면, 보안 플랫폼 장치가 제공되며, 이 장치는,
- [0010] 사물인터넷 장치에 탑재되는 보안 플랫폼 장치로서, 상기 사물인터넷 장치에서 센싱되는 센서 데이터가 암호화되어 저장되는 보안 플래시 메모리를 포함하는 외부 주변 장치, 그리고 펌웨어 저장소 - 상기 펌웨어 저장소는, 사물인터넷 서비스를 제공하는 애플리케이션을 저장하는 비 보안 상태 영역, 그리고 사물인터넷 장치에 대한 보안 플랫폼 서비스를 제공하는 데 사용되는 복수의 보안 플랫폼 서비스를 저장하는 보안 상태 영역을 포함함 - , 그리고 복수의 암호화 알고리즘을 포함하며, 상기 외부 주변장치의 보안 플래시 메모리에 저장된 센서 데이터에 대한 상기 복수의 보안 플랫폼 서비스 중 일부의 접근이 가능하도록 하는 암호화 가속기를 포함하는 SoC(System on Chip)를 포함하며, 상기 보안 상태 영역 내의 복수의 보안 플랫폼 서비스 중 일부는 상기 비 보안 상태 영역에 저장된 애플리케이션에 의해 호출되어 사용 가능하다.
- [0011] 여기서, 상기 복수의 보안 플랫폼 서비스는, 상기 사물인터넷 장치의 구성요소에 대한 검사를 수행하는 어테스 테이션(Attestation) 서비스, 상기 암호화 가속기에 포함된 암호화 알고리즘을 사용하여 데이터에 대한 암호화 서비스를 제공하는 암호화 서비스, 그리고 상기 암호화 가속기를 통해 상기 외부 주변장치의 보안 플래시 메모리에 센서 데이터를 저장하고, 상기 보안 플래시 메모리에 저장된 센서 데이터를 읽는 기능을 제공하는 보안 저장 서비스를 포함한다.
- [0012] 또한, 상기 SoC는 상기 사물인터넷 장치의 제조 과정에서 주입된 프로비저닝 데이터 및 DUK(Device Unique Key)를 저장하고 있는 OTP(One-Time Programmable) 메모리를 더 포함하고, 상기 복수의 보안 플랫폼 서비스는, 상기 OTP 메모리에 저장된 정보를 사용하여, 상기 보안 플래시 메모리에 저장되는 센서 데이터에 대한 암호화 및 복호화시 사용되는 유도 키(Derived Key)를 생성하거나 제거하는 키 관리 서비스를 더 포함한다.
- [0013] 또한, 상기 보안 상태 영역은, 상기 비 보안 상태 영역에 저장된 애플리케이션이 상기 보안 상태 영역 내의 복수의 보안 플랫폼 서비스 중 일부를 호출하는 데 사용되는 API(Application Program Interface)를 더 포함하며, 상기 API는 상기 복수의 보안 플랫폼 서비스 각각이 제공하는 기능을 호출하기 위한 대응하는 함수를 포함한다.
- [0014] 또한, 상기 SoC는 알고리즘이 아닌 물리적 프로세스로부터 난수를 생성하는 난수 생성기(True Random Number Generator, TRNG)를 더 포함한다.
- [0015] 또한, 상기 외부 주변장치는 상기 사물인터넷이 외부의 클라우드 서버와의 보안 채널을 통한 통신이 가능하도록 하는 유무선 네트워크 통신 수단을 더 포함한다.

- [0016] 또한, 상기 암호화 가속기는, 타원 곡선을 이용한 전자 서명 알고리즘인 타원 곡선 암호화 알고리즘, 하나의 비밀 키로 데이터의 암호화와 복호화를 가능하게 하는 대칭 키 암호화 알고리즘, 그리고 공개 키와 개인 키를 사용하여 데이터의 암호화와 복호화를 가능하게 하는 비대칭 키 암호화 알고리즘을 포함한다.
- [0017] 상기 API는, 상기 사물인터넷의 구성요소의 점검을 위해 상기 어테스테이션 서비스를 호출하는 데 사용되는 함수, 상기 암호화 가속기에 포함된 암호화 알고리즘을 사용하기 위해 상기 암호화 서비스를 호출하는 데 사용되는 함수, 상기 보안 플래시 메모리에 대한 접근을 위해 상기 보안 저장 서비스를 호출하는 데 사용되는 함수, 그리고 상기 유도 키(Derived Key)를 생성하거나 삭제하기 위해 상기 키 관리 서비스를 호출하는 데 사용되는 함수를 포함한다.
- [0018] 또한, 상기 암호화 서비스를 호출하는 데 사용되는 함수는, 디지털 서명을 생성하기 위해 사용되는 함수, 상기 암호화 가속기에 포함된 대칭 키 알고리즘을 사용하기 위해 사용되는 함수, 상기 암호화 가속기에 포함된 비대칭 키 알고리즘을 사용하기 위해 사용되는 함수, 그리고 해시 값을 생성하기 위해 사용되는 함수를 포함한다.
- [0019] 또한, 상기 보안 저장 서비스를 호출하는 데 사용되는 함수는, 상기 보안 플래시 메모리에 센서 데이터를 저장하기 위해 사용되는 함수, 그리고 상기 보안 플래시 메모리에 저장된 센서 데이터를 로딩하기 위해 사용되는 함수를 포함한다.
- [0020] 또한, 상기 키 관리 서비스를 호출하는 데 사용되는 함수는, 상기 OTP 메모리에 저장되어 있는 DUK를 사용하여 상기 유도 키를 생성하기 위해 사용되는 함수, 그리고 상기 유도 키를 삭제하기 위해 사용되는 함수를 포함한다.
- [0021] 또한, 상기 API는, 상기 난수 생성기를 사용하여 난수 값을 발생하기 위해 사용되는 함수를 포함한다.
- [0022] 또한, 상기 보안 플랫폼 장치는, ARM(Acorn RISC Machine)의 PSA(Platform Security Architecture) 기반의 플랫폼 장치이다.

발명의 효과

- [0023] 본 발명에 따르면, 안전한 IoT 서비스의 개발을 원하는 어플리케이션 개발자들이 하드웨어의 특징 및 암호화 기술 연구에 노력을 할 필요 없이 쉽게 PSA 서비스를 이용할 수 있다.
- [0024] 또한, IoT 장치에 필수적인 보안 서비스들로 구성되어, 이를 통해 IoT 장치의 무결성과 기밀성을 보장할 수 있다.
- [0025] 또한, IoT 서비스 개발에 필요한 보안 서비스에 대한 인터페이스를 제공함으로써 IoT 서비스 어플리케이션 개발자의 개발 편의성을 제공한다.

도면의 간단한 설명

- [0026] 도 1은 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치의 개략적인 구성 블록도이다.
- 도 2는 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치의 작동 예의 흐름도이다.
- 도 3은 도 2에 도시된 센서 데이터를 복호화하고 서명을 생성하는 과정의 구체적인 흐름도이다.
- 도 4는 도 2에 도시된 센서 데이터 및 서명 검사 과정의 구체적인 흐름도이다.
- 도 5는 도 2에 도시된 검증 데이터 생성 과정의 구체적인 흐름도이다.
- 도 6은 도 2에 도시된 검증 데이터 확인 과정의 구체적인 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0027] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0028] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다

른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

- [0029] 명세서 전체에서, "및/또는"이라는 용어는 관련된 객체를 기술하기 위한 연관 관계만을 설명하고 세 가지 관계가 존재할 수 있음을 나타낸다는 것이 이해되어야 한다. 예를 들어, A 및/또는 B는 A만 존재하고, A와 B가 모두 존재하며, B만 존재하는 세 가지 경우를 나타낼 수 있다. 또한, 명세서 전체에서 문자 "/"는 일반적으로 연관된 객체 사이의 "또는" 관계를 지시한다.
- [0030] 이하, 도면을 참조하여 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치에 대해 설명한다.
- [0031] 도 1은 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치의 개략적인 구성 블록도이다.
- [0032] 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)는 SoC(System on Chip)(100) 및 외부 주변장치(200)를 포함한다. 이 때, 도 1에 도시된 ARM PSA 기반 보안 플랫폼 장치(10)는 본 발명의 일 실시예에 불과하므로 도 1을 통해 본 발명이 한정 해석되는 것은 아니며, 본 발명의 다양한 실시예들에 따라 도 1과 다르게 구성될 수도 있다. 또한, 도 1에서는 설명의 편의상 본 발명의 특징과 관련 없는 ARM PSA 기반 보안 플랫폼 장치(10)의 일반적인 구성 및 그 동작에 대한 설명은 생략하였다.
- [0033] 구체적으로, SoC(100)는 펌웨어가 저장되는 비 휘발성 메모리(Non Volatile Memory, NVM)(110), OTP(One-Time Programmable) 메모리(120), 순수 난수 생성기(True Random Number Generator, TRNG)(130) 및 암호화 가속기(Crypto Accelerator)(140)를 포함한다.
- [0034] NVM(110)은 IoT 서비스를 제공하는 애플리케이션을 저장하는 비 보안 상태 영역(Non-secure state)(111)과 보안 플랫폼 서비스를 제공하기 위해 사용되는 보안 상태 영역(Secure state)(112)을 포함한다.
- [0035] 구체적으로, 보안 상태 영역(112)은 안전한 인터럽트 및 IPC(Inter-Process Communication)를 제공하는 신뢰 펌웨어(Trusted Firmware, TF-M)(1121), 신뢰 펌웨어(1121)를 기반으로 하는 보안 플랫폼 서비스를 제공하는 보안 플랫폼 서비스 영역(1122) 및 비 보안 상태 영역(111)의 애플리케이션에서 보안 플랫폼 서비스 영역(1122) 내의 보안 플랫폼 서비스 호출이 가능하도록 하는 보안 플랫폼 서비스 API(Application Program Interface)(1123)를 포함한다.
- [0036] 보안 플랫폼 서비스 영역(1122)은 IoT 장치의 보안 처리를 위해 사용되는 다음과 같은 6개의 보안 플랫폼 서비스를 포함한다.
- [0037] 첫 번째로, 보안 부트(Secure Boot) 서비스 영역(11221)은 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)의 부팅 중에 부트 구성 요소의 무결성을 검증한다.
- [0038] 예를 들어, IoT 장치의 메인 프로세서에 리셋(Reset) 신호가 작용하면, IoT 장치가 부팅되고, 비 보안 상태 영역(111)과 보안 상태 영역(112)의 무결성이 확인된다. 이러한 보안 부트 서비스(11221)는 oneM2M의 TS-0002-Requirements를 나타내는 [표 1]에서의 SER-003, SER-013을 만족한다.

표 1

코드	요구사항
SER-002	oneM2M 시스템은 데이터의 기밀성을 보장할 수 있어야 한다.
SER-003	oneM2M 시스템은 데이터의 무결성을 보장할 수 있어야 한다.
SER-013	oneM2M 시스템은 부팅시, 런타임시 주기적으로, 그리고 M2M 장치(들)의 소프트웨어/하드웨어/펌웨어 구성요소에 대한 소프트웨어 업그레이드시, 무결성 검사 메커니즘을 제공할 수 있어야 한다.
SER-064	M2M 장치는 허용된 이해 관계자에 의해 승인되지 않는 한, M2M 장치에서 실행되는 소프트웨어/미들웨어/펌웨어의 설치 또는 수정을 방지하는 메커니즘을 제공해야 한다.
SER-065	oneM2M 시스템은 허용된 이해 관계자에 의해 승인되지 않는 M2M 장치의 소프트웨어/미들웨어/펌웨어의 설치 또는 수정을 검출할 수 있어야 한다.
SER-068	oneM2M 시스템 내에서 교환되는 정보는 정보 인증 및 정보 무결성을 보장하기 위해 암호화 기술을 사용해야 한다.
SER-069	oneM2M 시스템은 디지털 서명과 같은 적절한 방법을 사용하여 정보를 안전하게 전송할 수 있어야 한다.

[0039]

[0040]

두 번째로, 보안 펌웨어 업데이트(Secure Firmware Update) 서비스(12222)는 IoT 서비스 개발자가 개발한 현재의 비 보안 상태 영역(111)의 애플리케이션과 새로운 애플리케이션의 무결성을 검사한다. 이러한 보안 펌웨어 업데이트 서비스(12222)는 [표 1]에서의 SER-003, SER-064를 만족한다.

[0041]

세 번째로, 어테스테이션(Attestation) 서비스(12223)는 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)의 구성요소를 검사한다. 이러한 어테스테이션 서비스(12223)의 결과는 런타임 및 부팅 때 장치 검증에 사용되며, 대표적인 어테스테이션의 사용 사례는 원격 어테스테이션(Remote attestation)이다. 이러한 어테스테이션 서비스(12223)는 [표 1]에서의 SER-003, SER-013, SER-064, SER-069를 만족한다.

[0042]

네 번째로, 암호화(Cryptography) 서비스(12224)는 암호화 가속기(140)의 타원 곡선 알고리즘 및 대칭/비대칭 키 암호화 알고리즘의 사용과 TRNG(130)의 사용을 제공한다. 이러한 암호화 서비스(12224)는 [표 1]에서의 SER-002, SER-003, SER-068, SER-069를 만족한다.

[0043]

다섯 번째로, 보안 저장(Secure Storage) 서비스(12225)는 암호화 가속기(140)를 통해 외부 주변장치(200) 내의 보안 플래시(Secure Flash) 메모리(210)에 보안 데이터를 쓰고 읽는 기능을 제공한다. 이러한 보안 저장 서비스(12225)는 [표 1]에서의 SER-002, SER-003, SER-068 및 SER-069를 만족한다.

[0044]

여섯 번째로, 키 관리(Key Management) 서비스(12226)는 OTP 메모리(120) 내의 프로비전된 암호화 키(121)와 DUK(Device Unique Key)(122)에서 생성된 유도 키(Derived key)의 사용을 제공한다. 이러한 키 관리 서비스(12226)는 [표 1]에서의 SER-002, SER-003, SER-068 및 SER-069를 만족한다.

[0045]

상기에서 설명된 6개의 서비스는 이하에서 해당 서비스에 대응하는 프로그램 또는 코드를 나타낼 수 있다.

[0046]

한편, 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)는 IoT 서비스 애플리케이션 개발자에게 편의성과 빠른 개발을 제공하기 위해, 비 보안 상태 영역(111)에서 보안 상태 영역(112) 내의 보안 플랫폼 서비스(1122)의 보안 플랫폼 서비스, 즉 전술한 6개의 보안 플랫폼 서비스(122221, 122222, 122223, 12224, 12225, 12226)를 호출 할 수 있는 보안 플랫폼 서비스 API(1123)를 제공한다. 이러한 보안 플랫폼 서비스 API(1123)의 예는 다음의 [표 2]에 나타난 바와 같다.

표 2

Service	Function	Parameter(s)	Return
Attestation	int getMeasure(measureInfo_t data, measureInfo_t *result)	Measured information of device data, Result of measurement	1(Success) or 0(Failure)
Cryptography	int getRand()	-	Random integer value by TRNG
	int ecdsa(ecdsaContext *ctx, type sign_verify, char *in, size_t in_len, char *out, size_t out_len, int rng)	ECDSA context, Sign or Verify, Input data, Size of input data, Output data, Size of output data, Random integer value	1(Success) or 0(Failure)
	int aes128(int keyID, type enc_dec, char *in, size_t in_len, char *out, size_t *out_len)	ID of derived key, Input data, Size of input data, Output data, Size of output data	1(Success) or 0(Failure)
	int sha256(char *plain, size_t plain_len, char *digest, size_t *digest_len)	Plain data, Size of plain data, Digest data, Size of digest data	1(Success) or 0(Failure)
	int rsa1024(int keyID, type enc_dec, char *in, size_t in_len, char *out, size_t *out_len)	ID of derived key, Input data, Size of input data, Output data, Size of output data	1(Success) or 0(Failure)
Secure Storage	int storeData(char *cipher, int size)	Cipher data, Size of cipher data	Page ID where data are stored (pageID)
	void loadData(int pageID, int size)	Page ID where data are stored, Size of cipher data	-
Key Management	int genKey()	-	ID of the derived key (keyID)
	void delKey(int keyID)	ID of the derived key	-

[0047]

[0048]

다음, OTP 메모리(120)는 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)가 탑재되는 IoT 장치 제조 과정에서 주입된 프로비저닝 데이터(Provisioning Data)(121) 및 DUK(Device Unique Key)(122)를 저장한다.

[0049]

TRNG(130)는 알고리즘이 아닌 물리적 프로세스로부터 난수를 생성한다.

[0050]

암호화 가속기(140)는 외부 주변장치(200) 내에 있는 보안 플래시 메모리(210)에 직접 접근하여 보안 데이터의 쓰기 및 읽기가 가능하다. 구체적으로, 암호화 가속기(140)는 타원 곡선을 이용한 전자 서명 알고리즘인 타원 곡선 암호화 알고리즘(Elliptic Curve Digital Signature Algorithm, ECDSA)(141), 하나의 비밀 키로 데이터의 암호화와 복호화를 가능하게 하는 대칭 키 암호화 알고리즘(142), 예를 들어 차세대 블록 암호화 알고리즘(Advanced Encryption Standard, AES), 및 공개 키(public key)와 개인 키(private key)를 사용하여 데이터의 암호화와 복호화를 가능하게 하는 비대칭 키 암호화 알고리즘(143), 예를 들어 RSA(Rivest Shamir Adleman)를 포함한다.

[0051]

한편, 외부 주변장치(200)는 암호화된 센서 데이터인 보안 데이터(211)를 저장하는 보안 플래시 메모리(210) 및 TCP(Transmission Control Protocol), UDP(User Data Protocol), SSL(Secure Sockets Layer), 3G(Generation), 4G, 5G 등과 같은 유무선 네트워크 프로토콜을 통해 외부와 통신을 할 수 있는 통신 모듈(220)을 포함하지만, 이것으로만 제한되는 것은 아니다.

[0052]

이하, 도면을 참조하여, 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치의 작동 예에 대해 설명한다.

[0053]

도 2는 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치의 작동 예의 흐름도이다. 특히, 도 1을 참조하여 설명한 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)가 외부 주변장치(200)의 보안 플래시 메모리(210)에 저장되어 있는 센서 데이터를 외부의 클라우드 서버(도시되지 않음)로 전송하는 작동 예에 대해 설명한다.

[0054]

설명 전에, IoT 장치(도시되지 않음)의 센싱 기능에 의해 센싱된 센서 데이터가 미리 암호화되어 외부 주변장치(200)의 보안 플랫폼 메모리(210) 내에 저장되어 있는 것으로 가정하여 설명한다.

[0055]

도 2를 참조하면, 먼저, 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)는 보안 플랫폼 서비스 영역(1122) 내의 보안 플랫폼 서비스를 통해서 외부 주변장치(200)의 보안 플래시 메모리(210)에 저장된 센서 데이터(211)를 복호화하고 서명을 생성한다(S100).

[0056]

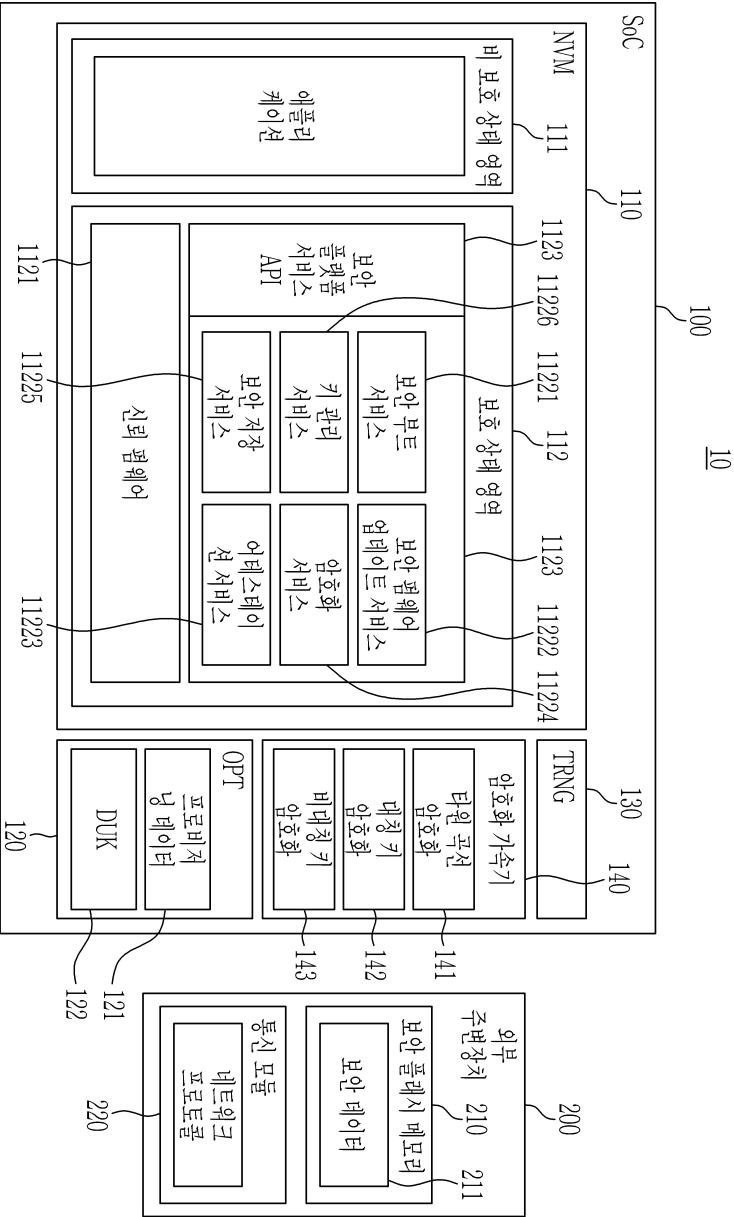
그 후, 클라우드 서버와 형성되어 있는 안전한 채널을 통해 센서 데이터 및 서명을 클라우드 서버로 전송한다(S110).

- [0057] 따라서, 클라우드 서버는 IoT 장치의 보안 플랫폼 장치(10)로부터 전송된 센서 데이터 및 서명을 검사하여 센서 데이터의 보안성을 확인한다(S120).
- [0058] 센서 데이터 및 서명 검사 결과, 이상이 없으면(S130) 클라우드 서버가 센서 데이터를 사용(저장 포함)하지만(S140), 만약 이상이 있으면(S130), IoT 장치의 해킹 여부를 판단하기 위해 장치 검증 과정을 수행한다.
- [0059] 먼저, 클라우드 서버는 IoT 장치의 보안 플랫폼 장치(10)에게 장치 검증을 요청한다(S150).
- [0060] 보안 플랫폼 장치(10)는 장치 검증을 위한 검증 데이터를 생성하고(S160), 클라우드 서버와 형성되어 있는 안전한 채널을 통해 검증 데이터를 전송한다(S170).
- [0061] 그 후, 클라우드 서버는 수신된 검증 데이터를 확인하고(S180) 확인된 검증 결과를 보안 플랫폼 장치(10)로 전송한다(S190).
- [0062] 그리고, 검증 결과가 성공인 경우(S200), 상기 단계(S110)에서 전송된 센서 데이터를 사용한다(S210).
- [0063] 그러나, 상기 단계(S200)에서 검증 결과가 실패인 경우에는 실패 처리를 수행한다(S220). 여기서, 실패 처리는 기존의 방식과 동일하게 수행될 수 있다. 예를 들어, 임계 횟수 동안의 반복된 센서 데이터의 재전송과 그에 따른 검증이 수행될 수 있으나, 이것으로만 제한되는 것은 아니다.
- [0064] 한편, 전송한 안전한 채널은 보안 플랫폼 장치(10)와 클라우드 서버 사이에 예를 들어, 데이터 전송 등의 활동에 보안 통신을 제공하는 SSL 프로토콜 접속이 이루어져 있는 전송 채널을 의미한다.
- [0065] 도 3은 도 2에 도시된 센서 데이터를 복호화하고 서명을 생성하는 과정의 구체적인 흐름도이다. 도 3에 도시된 센서 데이터를 복호화하고 서명을 생성하는 과정은 도 1을 참조하여 설명한 ARM PSA 기반 보안 플랫폼 장치(10)에 의해 수행된다.
- [0066] 도 3을 참조하면, 먼저, 보안 플랫폼 서비스 영역(1122)의 키 관리 서비스(12226)에 의해, OTP 메모리(120) 내의 DUK(120)를 사용하여 유도 키(Derived Key)가 생성된다(S01). 이 때, 보안 플랫폼 서비스 영역(1122)의 키 관리 서비스(12226)는 [표 2]에 나타난 바와 같이, 키 관리 서비스(12226)에 대응하는 함수(Function) 중에서 'genKey' 함수에 의해 호출된다.
- [0067] 다음, 보안 플랫폼 서비스 영역(1122)의 보안 저장 서비스(12225)에 의해, 암호화 가속기(140)를 통해 외부 주변장치(200)의 보안 플래시 메모리(210) 내의 센서 데이터가 로딩된다(S102). 이 때, 보안 플랫폼 서비스 영역(1122)의 보안 저장 서비스(12225)는 [표 2]에 나타난 바와 같이, 보안 저장 서비스(12225)에 대응하는 함수 중에서 'loadData' 함수에 의해 호출된다.
- [0068] 선택적으로, 상기 단계(S101)에서 생성된 유도 키가 보안 플래시 메모리(210) 내에 저장된 후, 상기 단계(S102)에서 센서 데이터와 함께 유도 키가 로딩될 수 있다.
- [0069] 계속해서, 보안 플랫폼 서비스 영역(1122)의 암호화 서비스(12224)에 의해, 유도 키를 사용하여 센서 데이터가 복호된다(S103). 이 때, 보안 플랫폼 서비스 영역(1122)의 암호화 서비스(12224)는 [표 2]에 나타난 바와 같이, 암호화 서비스(12224)에 대응하는 함수 중에서 'aes128' 함수에 의해 호출된다. 여기서, 'aes128' 함수는 미국 표준 기술 연구소(National Institute of Standards and Technology, NIST)에 의해 제정된 대칭키 방식의 암호 저장 기술 중 하나로서, 특히 키의 길이가 128 비트인 암호화 방식을 나타낸다.
- [0070] 그 후, 키 관리 서비스(12226)에 의해, 유도 키(Derived Key)가 삭제된다(S04). 이 때, 키 관리 서비스(12226)는 [표 2]에 나타난 바와 같이, 키 관리 서비스(12226)에 대응하는 함수 중에서 'delKey' 함수에 의해 호출된다.
- [0071] 마지막으로, 암호화 서비스(12224)에 의해, 본 발명의 실시예에 따른 보안 플랫폼 장치(10)의 개인 키를 사용하여 디지털 서명이 생성된다(S105). 이 때, 암호화 서비스(12224)는 [표 2]에 나타난 바와 같이, 암호화 서비스(12224)에 대응하는 함수 중에서 'ecdsa' 함수에 의해 호출된다.
- [0072] 다음, 도 4는 도 2에 도시된 센서 데이터 및 서명 검사 과정의 구체적인 흐름도이다. 도 4에 도시된 센서 데이터 및 서명 검사 과정은 클라우드 서버에 의해 수행된다.
- [0073] 도 4를 참조하면, 먼저 클라우드 서버는 본 발명의 실시예에 따른 보안 플랫폼 장치(10)에 대응하는 공용 키를 사용하여 보안 플랫폼 장치(10)로부터 전송된 디지털 서명을 복호한다(S121).

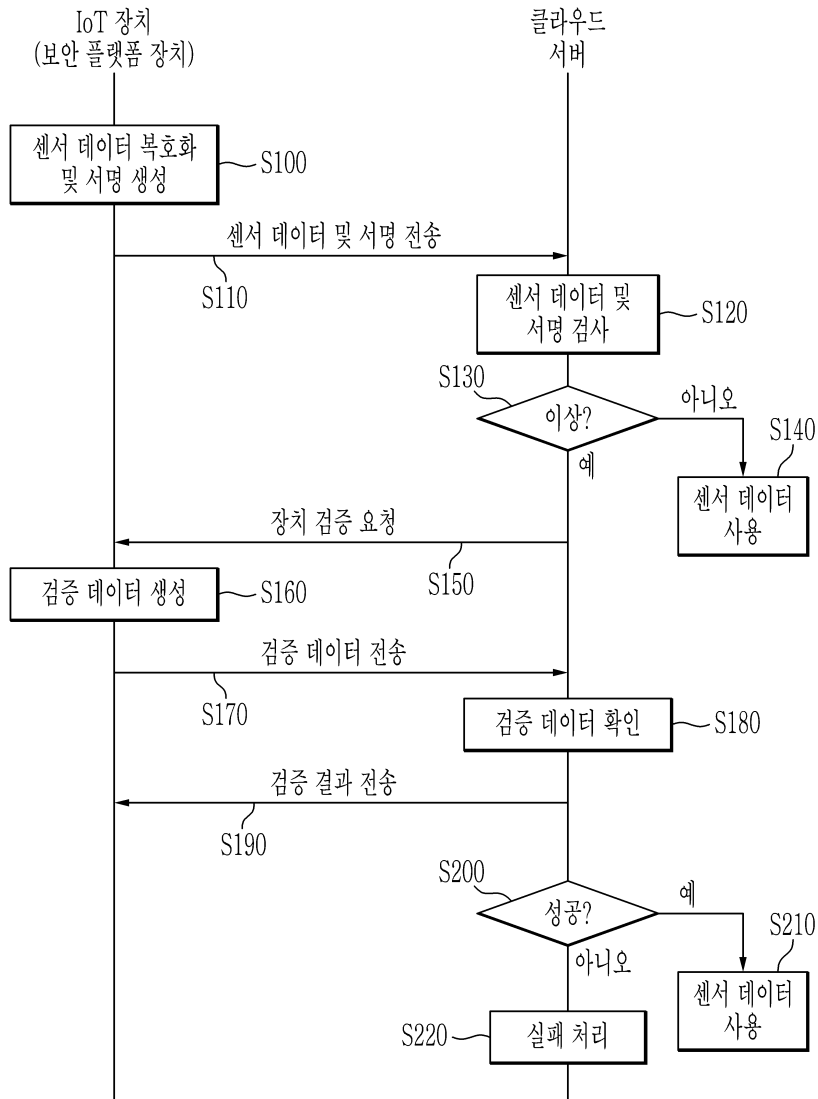
- [0074] 그 후, 센서 데이터를 검사하여(S122) 센서 데이터의 이상 유무를 판단한다(S123).
- [0075] 도 4에 도시된 클라우드 서버에서의 센서 데이터 및 서명의 검사 과정은 기존의 방식과 동일하므로 보다 구체적인 설명은 여기에서 생략한다.
- [0076] 다음, 도 5는 도 2에 도시된 검증 데이터 생성 과정의 구체적인 흐름도이다. 도 5에 도시된 검증 데이터 생성 과정은 도 1을 참조하여 설명한 ARM PSA 기반 보안 플랫폼 장치(10)에 의해 수행된다.
- [0077] 도 5를 참조하면, 먼저, 보안 플랫폼 서비스 영역(1122)의 어테스테이션 서비스(12223)에 의해, 본 발명의 실시예에 따른 보안 플랫폼 장치(10)의 구성요소를 검사한 검증 데이터를 획득한다(S161). 이 때, 보안 플랫폼 서비스 영역(1122)의 어테스테이션 서비스(12223)는 [표 2]에 나타난 바와 같이, 어테스테이션 서비스(12223)에 대응하는 함수 중에서 'getMeasure' 함수에 의해 호출된다.
- [0078] 다음, 암호화 서비스(12224)에 의해, 검증 데이터에 대해 해시 값을 생성한다(S162). 이 때, 암호화 서비스(12224)는 [표 2]에 나타난 바와 같이, 암호화 서비스(12224)에 대응하는 함수 중에서 'sha256' 함수에 의해 호출된다. 여기서, 'sha256' 함수는 임의의 길이의 데이터를 고정된 길이의 데이터로 매핑하는 해시 함수 중 하나로, 특히 64개의 암호화된 숫자로의 매핑을 수행한다.
- [0079] 그 후, 암호화 서비스(12224)에 의해, 본 발명의 실시예에 따른 보안 플랫폼 장치(10)의 개인 키를 사용하여 디지털 서명이 생성된다(S163). 이 때, 암호화 서비스(12224)는 [표 2]에 나타난 바와 같이, 암호화 서비스(12224)에 대응하는 함수 중에서 'ecdsa' 함수에 의해 호출된다.
- [0080] 다음, 도 6은 도 2에 도시된 검증 데이터 확인 과정의 구체적인 흐름도이다. 도 6에 도시된 검증 데이터 확인 과정은 클라우드 서버에 의해 수행된다.
- [0081] 도 6을 참조하면, 먼저 클라우드 서버는 본 발명의 실시예에 따른 보안 플랫폼 장치(10)에 대응하는 공용 키를 사용하여 보안 플랫폼 장치(10)로부터 전송된 검증 데이터를 복호한다(S181).
- [0082] 그 후, 복호된 검증 데이터에 대한 해시 값을 생성한 다음(S182), 검증 데이터에 대한 이상 유무를 확인한다(S183). 여기서, 검증 데이터에 대한 이상 유무는 검증 결과가 성공인지 아니면 실패인지로 나타난다.
- [0083] 도 6에 도시된 클라우드 서버에서의 검증 데이터 확인 과정은 기존의 방식과 동일하므로 보다 구체적인 설명은 여기에서 생략한다.
- [0084] 위에서는 본 발명의 실시예에 따른 ARM PSA 기반 보안 플랫폼 장치(10)가 외부 주변장치(200)의 보안 플래시 메모리(210)에 저장되어 있는 센서 데이터를 외부의 클라우드 서버로 전송하는 작동 예에 대해서만 설명하였으나, 기술한 설명에 포함된 기능들은 그 외의 다양한 형태의 서비스, 예를 들어, 센서 데이터 저장 서비스 등에도 유사하게 적용될 수 있음은 본 기술분야의 당업자라면 쉽게 이해할 것이다.
- [0085] 한편, 보안 플랫폼 서비스 영역(1122)에 포함된 보안 부트 서비스(11221)와 보안 펌웨어 업데이트 서비스(12222)는 각각 IoT 장치의 부팅과 펌웨어 업데이트 시 작동되며, 이러한 서비스들은 애플리케이션 개발자의 개입없이 자동으로 작동할 수 있다.
- [0086] 먼저, 보안 부트 서비스(11221)는 IoT 장치의 리셋 시에, 부트 ROM(Read Only Memory) 등에 미리 저장되어 있는 부트 로더의 보안 상태 및 비 보안 상태 펌웨어 무결성을 검증한다. 이러한 검증을 통해 IoT 장치의 펌웨어 교체 공격을 방지할 수 있다.
- [0087] 또한, 보안 펌웨어 업데이트 서비스(12222)는 클라우드 서버의 OTA(On The Air) 펌웨어 업데이트 시에 부트 로더의 펌웨어 버전 및 펌웨어 무결성 검수를 수행한다. 이러한 업데이트 서비스를 통해 원격 서버를 통한 펌웨어 교체 공격을 방지할 수 있고, MITM(Man-In-The-Middle) 공격을 방지할 수 있으며, 또한 펌웨어 롤백(Rollback) 공격을 방지할 수 있다.
- [0088] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있다.
- [0089] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

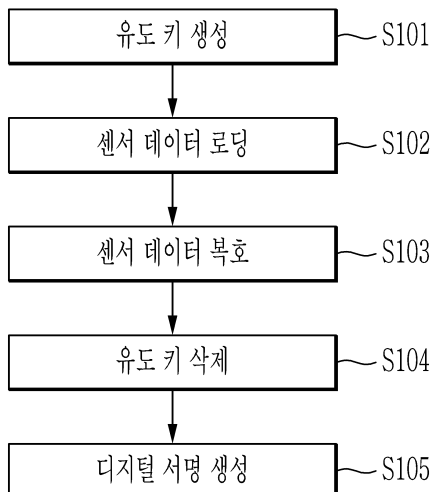
도면1



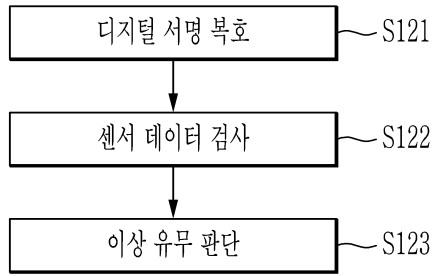
도면2



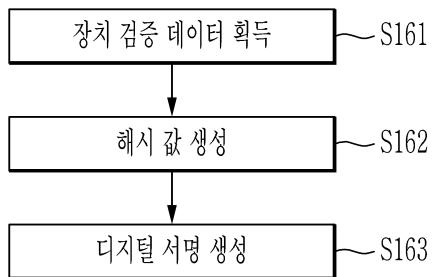
도면3



도면4



도면5



도면6

