(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0036779
(43) 공개일자 2019년04월05일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/24* (2006.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 63/306 (2013.01)
H04L 41/082 (2013.01)
(21) 출원번호 10-2017-0126088
(22) 출원일자 2017년09월28일
심사청구일자 2017년09월28일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
조진성
경기도 수원시 영통구 봉영로 1620, 101동 1801호 (영통동, 대우 월드마크 영통)
김병선
경기도 용인시 기흥구 덕영대로 1732 경희대학교 (서천동)
(뒷면에 계속)
(74) 대리인
특허법인도담

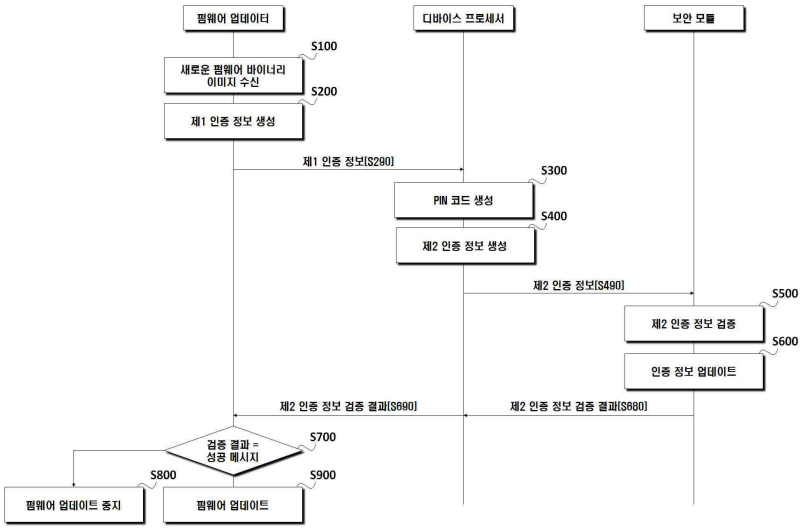
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **보안 펌웨어 업데이트 방법 및 시스템**

(57) 요 약

본 발명은 보안 펌웨어 업데이트 방법에 대한 것으로, 펌웨어 업데이터가 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서로 전송하는 단계, 상기 디바이스 프로세서가 제1 인증 정보를 이용하여 PIN 코드를 생성하고, 상기 제1 인증 정보에 상기 PIN 코드를 포함시켜 제2 인증 정보를 생성하는 단계, 상기 제2 인증 정보를 보안 모듈로 전송하는 단계, 상기 보안 모듈은 상기 디바이스 프로세서로부터 수신한 상기 제2 인증 정보를 검증한 후, 검증이 완료되면 상기 보안 모듈에 기 저장된 현재 인증 정보를 상기 제2 인증 정보로 업데이트 하는 단계, 상기 업데이트가 완료되면, 상기 제2 인증 정보의 검증 결과를 펌웨어 업데이터로 전송하는 단계, 상기 펌웨어 업데이터는 상기 검증 결과에 따라 펌웨어 업데이트를 결정하는 단계를 포함하는 것을 특징으로 한다.

대 표 도



(52) CPC특허분류
H04L 63/083 (2013.01)
H04L 63/12 (2013.01)
H04L 9/0643 (2013.01)

(72) 발명자
이기영
경기도 성남시 중원구 도촌남로 22, 113동 404호 (도촌동, 휴먼시아섬마을1단지아파트)
이기웅
경기도 군포시 수리산로 203번길 14 (산본동)
조성희
경기도 용인시 수지구 성복2로 86, 203동 1104호 (성복동, 성동마을LG빌리지2차아파트)
윤중철
경기도 화성시 삼성전자로 1-1 DSR Security 제품개발팀 (반월동)
정준영
경기도 부천시 역곡로471번가길 19-8, A동 401호 (고강동, 월드빌리지)

명 세 서

청구범위

청구항 1

보안 펌웨어 업데이트 방법에 있어서,

펌웨어 업데이터가 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서로 전송하는 단계;

상기 디바이스 프로세서가 제1 인증 정보를 이용하여 PIN 코드를 생성하고, 상기 제1 인증 정보에 상기 PIN 코드를 포함시켜 제2 인증 정보를 생성하는 단계;

상기 제2 인증 정보를 보안 모듈로 전송하는 단계;

상기 보안 모듈은 상기 디바이스 프로세서로부터 수신한 상기 제2 인증 정보를 검증한 후, 검증이 완료되면 상기 보안 모듈에 기 저장된 현재 인증 정보를 상기 제2 인증 정보로 업데이트 하는 단계;

상기 업데이트가 완료되면, 상기 제2 인증 정보의 검증 결과를 펌웨어 업데이터로 전송하는 단계;

상기 펌웨어 업데이터는 상기 검증 결과에 따라 펌웨어 업데이트를 결정하는 단계를 포함하는 보안 펌웨어 업데이트 방법.

청구항 2

제1항에 있어서,

상기 제1 인증 정보는 기 설정된 패스워드, 새로운 펌웨어 이미지 해시, 및 새로운 펌웨어 버전 식별 정보를 포함하는 것을 특징으로 하는 보안 펌웨어 업데이트 방법.

청구항 3

제2항에 있어서,

상기 새로운 펌웨어 이미지 해시는 새로운 펌웨어 바이너리 이미지에 SHA 함수를 적용함으로써 생성되는 것을 특징으로 하는 보안 펌웨어 업데이트 방법.

청구항 4

제2항에 있어서,

상기 패스워드는 IoT 디바이스가 제조될 때 설정되는 고유 값인 것을 특징으로 하는 보안 펌웨어 업데이트 방법.

청구항 5

제1항에 있어서,

상기 PIN 코드는 현재 펌웨어의 제1 PIN 코드와 상기 현재 인증 정보의 업데이트를 위한 제2 PIN 코드를 포함하는 보안 펌웨어 업데이트 방법.

청구항 6

제5항에 있어서,

상기 제1 PIN 코드는 상기 디바이스 프로세서에 기 저장된 알고리즘에 따라 현재 펌웨어의 이미지 해시 값을 통해 생성되는 단계;

상기 제2 PIN 코드는 상기 디바이스 프로세서에 기 저장된 알고리즘에 따라 새로운 펌웨어의 이미지 해시 값을 통해 생성되는 단계를 더 포함하는 보안 펌웨어 업데이트 방법.

청구항 7

제5항에 있어서,

상기 보안 모듈이 상기 디바이스 프로세서로부터 수신한 제2 인증 정보의 검증 단계는

상기 보안 모듈의 패스워드와 상기 제2 인증 정보의 패스워드를 비교하는 단계;

상기 보안 모듈의 PIN 코드와 상기 제2 인증 정보의 상기 제1 PIN 코드를 비교하는 단계;

상기 보안 모듈에 포함된 펌웨어 버전과 상기 제2 인증 정보에 포함된 펌웨어 버전을 비교하는 단계;

상기 제2 인증 정보의 검증 결과를 생성하는 단계를 포함하는 보안 펌웨어 업데이트 방법.

청구항 8

제7항에 있어서,

상기 제2 인증 정보의 검증 결과를 생성하는 단계는

상기 제2 인증 정보가 적합하다고 검증되면 성공 메시지를 생성하는 단계;

상기 제2 인증 정보가 적합하지 않다고 검증되면 에러 메시지를 생성하는 단계를 더 포함하는 보안 펌웨어 업데이트 방법.

청구항 9

제1항에 있어서,

상기 펌웨어 업데이터가 펌웨어 업데이트를 결정하는 단계는

성공 메시지를 수신하면 펌웨어의 업데이트를 진행하는 단계를 더 포함하는 보안 펌웨어 업데이트 방법.

청구항 10

제1항에 있어서,

상기 펌웨어 업데이터가 펌웨어 업데이트를 결정하는 단계는

에러 메시지를 수신하면 펌웨어의 업데이트를 중단하는 단계를 더 포함하는 보안 펌웨어 업데이트 방법.

청구항 11

제1항에 있어서,

상기 디바이스 프로세서는 상기 제2 인증 정보를 Command APDU 프로토콜의 데이터 필드에 포함하여 상기 보안 모듈로 전송하는 것을 특징으로 하는 보안 펌웨어 업데이트 방법.

청구항 12

보안 펌웨어 업데이트 시스템에 있어서,

새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서로 전송하고, 펌웨어를 업데이트하는 펌웨어 업데이터;

PIN 코드를 생성하고, 상기 제1 인증 정보에 상기 PIN 코드를 포함시켜 제2 인증 정보를 생성하며, 상기 제2 인증 정보를 보안 모듈로 전송하는 디바이스 프로세서;

상기 디바이스 프로세서로부터 수신한 상기 제2 인증 정보를 검증한 후, 검증이 완료되면 기 저장된 현재 인증 정보를 상기 제2 인증 정보로 업데이트하고, 상기 업데이트가 완료되면 상기 제2 인증 정보의 검증 결과를 상기 펌웨어 업데이터로 전송하는 보안 모듈을 포함하는 보안 펌웨어 업데이트 시스템.

청구항 13

보안 펌웨어 업데이트를 수행하기 위한 펌웨어 업데이터에 있어서,

새로운 펌웨어 바이너리 이미지, 기 설정된 패스워드 및 새로운 펌웨어 버전 식별 정보를 수신하고, 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서로 전송하는 통신부;

새로운 펌웨어의 제1 인증 정보를 생성하는 펌웨어 패키지 생성부;

상기 디바이스 프로세서가 송신한 검증 결과에 따라 펌웨어 업데이트를 결정하는 펌웨어 업데이트부를 포함하고

상기 제1 인증 정보는 상기 기 설정된 패스워드, 상기 새로운 펌웨어 버전 식별 정보, 새로운 펌웨어 바이너리 이미지에 SHA 함수를 적용함으로써 생성된 새로운 펌웨어 이미지 해시를 포함하는 펌웨어 업데이터.

청구항 14

보안 모듈을 이용한 보안 펌웨어 업데이트 시스템의 디바이스 프로세서에 있어서,

펌웨어 업데이터가 송신한 제1 인증 정보를 이용하여 PIN 코드를 생성하고, 상기 PIN 코드를 제1 인증 정보에 포함시켜 제2 인증 정보를 생성하는 인증 정보 관리부;

상기 제2 인증 정보를 보안 모듈로 전송하고, 상기 보안 모듈이 송신한 제2 인증 정보의 검증 결과를 펌웨어 업데이터에 송신하는 통신부를 포함하는 디바이스 프로세서.

청구항 15

제14항에 있어서,

상기 PIN 코드는 현재 펌웨어의 제1 PIN 코드와 상기 보안 모듈의 현재 인증 정보 업데이트를 위한 제2 PIN 코드를 포함하는 디바이스 프로세서.

청구항 16

제14항에 있어서,

상기 보안 모듈은 상기 제2 인증 정보를 검증하고, 검증이 완료되면 검증 결과를 디바이스 프로세서에 송신하는 디바이스 프로세서.

청구항 17

제14항에 있어서,

상기 보안 모듈의 패스워드와 상기 제2 인증 정보의 패스워드를 비교하고,

상기 보안 모듈의 PIN 코드와 상기 제2 인증 정보의 제1 PIN 코드를 비교하고,

상기 보안 모듈의 펌웨어 버전과 상기 제2 인증 정보의 펌웨어 버전을 비교하여 상기 제2 인증 정보의 검증 결과를 생성하는 디바이스 프로세서.

청구항 18

제17항에 있어서,

상기 제2 인증 정보가 적합하다고 검증되면 성공 메시지를 생성하고,

상기 제2 인증 정보가 적합하지 않다고 검증되면 에러 메시지를 생성하는 디바이스 프로세서.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안 펌웨어 업데이트 방법 및 시스템에 관한 것으로, 보다 구체적으로 보안 모듈과 디바이스 프로세서, 펌웨어 업데이터를 포함하는 보안 펌웨어 업데이트 방법 및 시스템에 관한 것이다.

배 경 기 술

[0003] IoT(Internet Of Things)는 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술로 최근 가전, 자동차, 스마트시티 등과 같은 서비스 분야에 폭넓게 활용되고 있어 실생활에서 쉽게 접할 수 있게 보급 속도가 증가하고 있는 추세이다. 그러나 IoT가 보편화됨에 따라 다양한 부작용이 발생할 수 있다. IoT는 센서 기술, 통신 기술, 칩 기술, 운영체제 기술, 임베디드 시스템 기술, 플랫폼 기술, 빅데이터 기술, 텍스트 마이닝 기술, 오픈 API 기술 등 다양한 요소기술이 통합되어 사용되기 때문에 기술 혹은 구현하는 방법의 문제에 따라 보안 취약점이 존재할 수 있다. 또한 IoT기기의 기반인 운영체제가 올바른 보안을 갖추지 못하거나 적절한 업데이트가 이루어지지 않을 경우 해킹을 당할 위험이 존재한다. 실제로 IoT 환경의 보안적인 취약점을 악용하여 사생활을 침해한 사례도 있다. 예를 들어 CCTV의 영상을 불특정 다수에게 유포하고, 아파트 도어록 해킹 후 출입문을 열거나, 자동차의 문 잠금을 해제한 뒤 절도하는 등의 다양한 피해가 발생하고 있다.

[0004] 시장에 존재하는 다양한 보안 솔루션은 대부분 고성능 PC의 환경을 대상으로 구성되었고 IoT 디바이스의 연결성이 점점 정교하고 복잡해지고 있기때문에 보안 솔루션을 그대로 IoT 디바이스에 적용하는 것에는 어려움이 있다. 실제로 많은 기업들이 적절한 보안 대책을 갖추지 않고 있으며 IoT 디바이스의 보안 위험성에 대해 인지하지 못하고 있다.

[0005] IoT 환경에서 주로 발생하는 공격 중 펌웨어 롤백이나 펌웨어 중간자 공격은 펌웨어를 업데이트 할 때 새로운 버전의 펌웨어가 아닌 악의적인 펌웨어로 교체하는 것으로 디바이스의 시스템 제어권을 탈취당해, 디바이스 내의 데이터와 개인 정보가 유출되며 또한 추가적인 공격에 노출될 수 있다. 또한 이러한 공격에 유출되게 되면 디바이스가 공격자의 의도대로 조작될 수 있어 사용자의 생활을 위협할 수 있다.

[0006] 그러나 위에서 상술한 바와 같이 IoT의 보안이 취약함에도 불구하고 IoT 디바이스의 펌웨어 업데이트의 수준은 아주 열악하다. IoT 디바이스 내부에 저장된 펌웨어 이미지는 서비스 형태에 따라 바이너리 코드 및 크기가 상이하기 때문에 롬 바이오스에 어플리케이션 검증 과정을 추가하는 것은 불가능하여 공격자들이 펌웨어 이미지를 교체하는 것이 용이하다. 일반적으로 사용되는 IoT 디바이스의 펌웨어 업데이트는 디바이스가 새로운 펌웨어 바이너리 코드를 수신하면, 부트 로더가 현재 펌웨어 바이너리 코드를 삭제하고 새로운 펌웨어의 바이너리 코드를 삽입하여 펌웨어를 실행하는 방식으로 수행된다. 따라서 IoT 디바이스는 펌웨어 업데이트를 시도하는 주체에 대해 파악할 수 없으며 새로운 펌웨어 바이너리 코드가 정상적인 지 판단할 수 없기 때문에, 공격자가 IoT 디바이스에 불법 펌웨어를 업데이트하여 시스템 제어권을 획득하기는 용이하다.

[0007] 이를 방지하기 위해 상호 인증을 통한 공개 키 기반 구조, 암호 키 등을 이용한 상호 인증, 대기 시간 점검, 비공개 채널으로 키를 주고 받고 공개 채널으로 암호문을 보내는 양자 암호 등의 방법이 사용되고 있다. 대표적으

로 공개 키 기반 구조는 요청자에게 제공되고 타인과 공유할 수 없는 개인키와 모든 사람이 접근할 수 있는 공개키를 이용한다. 보다 구체적으로 A가 B에게 메시지를 송신할 때, A는 B의 공개키를 사용하여 메시지를 암호화하고 A의 개인키를 이용하여 디지털 인증서를 암호화하여 함께 송신한다. B가 메시지를 수신하게 되면 B의 개인키를 통해 복호화하여 메시지를 확인하고, 함께 수신한 디지털 인증서를 통해 A에게 온 메시지라는 것을 확인한다.

[0008] 상술한 바와 같이 IoT 디바이스에서 발생하는 다양한 보안상의 취약점을 대비하기 위한 종래의 기술로는 대한민국 공개특허공보 제10-2012-0092222호 “보안 부팅 방법 및 보안 부트 이미지 생성 방법” 이 있으며, 이는 초기 부트 로더가 공개키를 이용하여 제1 부트 로더에 포함된 제1 디지털 서명을 검증하고 유효한 경우, 제1 부트 로더가 고유 키를 이용하여 제2 부트 로더에 포함된 제1 메시지 인증 코드를 검증하고 유효한 경우, 제2 부트 로더를 실행하는 것을 특징으로 한다.

[0009] 또한, 대한민국 공개특허공보 10-2014-0073397호는 “보안 부팅을 수행하는 칩 시스템과 이를 이용하는 화상형성장치 및 그 부팅 방법” 이라는 명칭으로 복수의 암호화 키 중에서 암호화 키 설정 값에 대응되는 암호화 키를 이용하여 외부 비휘발성 메모리에 저장된 암호화된 데이터를 복호화하고, 복호화된 데이터를 메모리에 저장하고 이를 이용하여 부팅을 수행하는 기술을 개시한 바 있다.

[0010] 상기와 같은 종래 특허의 기존 소프트웨어 기반의 보안 솔루션은 저사양 IoT 디바이스에 적용하는데 제약이 있다. 이를 해결하기 위한 방안으로 소프트웨어와 하드웨어 기반의 융합 보안 솔루션을 접목시킴으로써 저사양 IoT 디바이스의 보안적인 한계를 극복할 필요가 있다.

선행기술문헌

특허문헌

[0012] (특허문헌 0001) 대한민국 공개특허공보 제10-2012-0092222호(2012년 08월 21일)

(특허문헌 0002) 대한민국 공개특허공보 제10-2014-0073397호(2014년 06월 16일)

발명의 내용

해결하려는 과제

[0013] 본 발명은 전술한 문제를 해결하기 위한 것으로, IoT 디바이스가 펌웨어 업데이트를 수행하고자 할 때 공격자가 불법 펌웨어를 이용하여 펌웨어 업데이트를 수행하는 것을 효과적으로 차단할 수 있는 방법 및 시스템을 제공하는 것을 일 목적으로 한다.

[0014] 또한, 본 발명은 별도의 보안 모듈을 이용하여 불법 펌웨어를 검증함으로써 보안성을 더욱 향상시킬 수 있는 보안 펌웨어 업데이트 방법 및 시스템을 제공하는 것을 다른 목적으로 한다.

[0015] 또한, 본 발명은 불법 펌웨어를 검증하여 IoT 디바이스의 업데이트를 차단함으로써 사용자의 데이터 및 사생활을 보호하는 것을 다른 목적으로 한다.

과제의 해결 수단

[0017] 이러한 목적을 달성하기 위한 본 발명은 보안 펌웨어 업데이트 방법에 있어서, 펌웨어 업데이터가 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서로 전송하는 단계, 상기 디바이스 프로세서가 제1 인증 정보를 이용하여 PIN 코드를 생성하고, 상기 제1 인증 정보에 상기 PIN 코드를 포함시켜 제2 인증 정보를 생성하는 단계, 상기 제2 인증 정보를 보안 모듈로 전송하는 단계, 상기 보안 모듈은 상기 디바이스 프로세서로부터 수신한 상기 제2 인증 정보를 검증한 후, 검증이 완료되면 상기 보안 모듈에 기 저장된 현재 인증 정보를 상기 제2 인증 정보로 업데이트 하는 단계, 상기 업데이트가 완료되면, 상기 제2 인증 정보의 검증 결과를 펌웨어 업데이터로 전송하는 단계, 상기 펌웨어 업데이터는 상기 검증 결과에 따라 펌웨어 업데이트를 결정하는 단계를 포함하는 것을 일 특징으로 한다.

[0018] 또한 상기 제1 인증 정보는 기 설정된 패스워드, 새로운 펌웨어 이미지 해시, 및 새로운 펌웨어 버전 식별 정보를 포함하는 것을 일 특징으로 한다.

[0019] 나아가 상기 새로운 펌웨어 이미지 해시는 새로운 펌웨어 바이너리 이미지에 SHA 함수를 적용함으로써 생성되는 것을 일 특징으로 한다.

[0020] 또한 상기 패스워드는 IoT 디바이스가 제조될 때 설정되는 고유 값인 것을 일 특징으로 한다.

[0021] 나아가 상기 PIN 코드는 현재 펌웨어의 제1 PIN 코드와 상기 현재 인증 정보의 업데이트를 위한 제2 PIN 코드를 포함하는 것을 일 특징으로 한다.

[0022] 또한 상기 제1 PIN 코드는 상기 디바이스 프로세서에 기 저장된 알고리즘에 따라 현재 펌웨어의 이미지 해시 값을 통해 생성되는 단계, 상기 제2 PIN 코드는 상기 디바이스 프로세서에 기 저장된 알고리즘에 따라 새로운 펌웨어의 이미지 해시 값을 통해 생성되는 단계를 더 포함하는 것을 일 특징으로 한다.

[0023] 나아가 상기 보안 모듈이 상기 디바이스 프로세서로부터 수신한 제2 인증 정보의 검증 단계는 상기 보안 모듈의 패스워드와 상기 제2 인증 정보의 패스워드를 비교하는 단계, 상기 보안 모듈의 PIN 코드와 상기 제2 인증 정보의 상기 제1 PIN 코드를 비교하는 단계, 상기 보안 모듈에 포함된 펌웨어 버전과 상기 제2 인증 정보에 포함된 펌웨어 버전을 비교하는 단계, 상기 제2 인증 정보의 검증 결과를 생성하는 단계를 포함하는 것을 일 특징으로 한다.

[0024] 또한 상기 제2 인증 정보의 검증 결과를 생성하는 단계는 상기 제2 인증 정보가 적합하다고 검증되면 성공 메시지를 생성하는 단계, 상기 제2 인증 정보가 적합하지 않다고 검증되면 에러 메시지를 생성하는 단계를 더 포함하는 것을 일 특징으로 한다.

[0025] 나아가 상기 펌웨어 업데이터가 펌웨어 업데이트를 결정하는 단계는 성공 메시지를 수신하면 펌웨어의 업데이트를 진행하는 단계를 더 포함하는 것을 일 특징으로 한다.

[0026] 또한 상기 펌웨어 업데이터가 펌웨어 업데이트를 결정하는 단계는 에러 메시지를 수신하면 펌웨어의 업데이트를 중단하는 단계를 더 포함하는 것을 일 특징으로 한다.

[0027] 나아가 상기 디바이스 프로세서는 상기 제2 인증 정보를 Command APDU 프로토콜의 데이터 필드에 포함하여 상기 보안 모듈로 전송하는 것을 일 특징으로 한다.

[0028] 또한 본 발명은 보안 펌웨어 업데이트 시스템에 있어서, 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서로 전송하고, 펌웨어를 업데이트하는 펌웨어 업데이터, PIN 코드를 생성하고, 상기 제1 인증 정보에 상기 PIN 코드를 포함시켜 제2 인증 정보를 생성하며, 상기 제2 인증 정보를 보안 모듈로 전송하는 디바이스 프로세서, 상기 디바이스 프로세서로부터 수신한 상기 제2 인증 정보를 검증한 후, 검증이 완료되면 기 저장된 현재 인증 정보를 상기 제2 인증 정보로 업데이트하고, 상기 업데이트가 완료되면 상기 제2 인증 정보의 검증 결과를 상기 펌웨어 업데이터로 전송하는 보안 모듈을 포함하는 것을 일 특징으로 한다.

[0029] 나아가 본 발명은 보안 펌웨어 업데이트를 수행하기 위한 펌웨어 업데이터에 있어서, 새로운 펌웨어 바이너리 이미지, 기 설정된 패스워드 및 새로운 펌웨어 버전 식별 정보를 수신하고, 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서로 전송하는 통신부, 새로운 펌웨어의 제1 인증 정보를 생성하는 펌웨어 패키지 생성부, 상기 디바이스 프로세서가 송신한 검증 결과에 따라 펌웨어 업데이트를 결정하는 펌웨어 업데이트부를 포함하고 상기 제1 인증 정보는 상기 기 설정된 패스워드, 상기 새로운 펌웨어 버전 식별 정보, 새로운 펌웨어 바이너리 이미지에 SHA 함수를 적용함으로써 생성된 새로운 펌웨어 이미지 해시를 포함하는 것을 일 특징으로 한다.

[0030] 또한 본 발명은 보안 모듈을 이용한 보안 펌웨어 업데이트 시스템의 디바이스 프로세서에 있어서, 펌웨어 업데이터가 송신한 제1 인증 정보를 이용하여 PIN 코드를 생성하고, 상기 PIN 코드를 제1 인증 정보에 포함시켜 제2 인증 정보를 생성하는 인증 정보 관리부, 상기 제2 인증 정보를 보안 모듈로 전송하고, 상기 보안 모듈이 송신한 제2 인증 정보의 검증 결과를 펌웨어 업데이터에 송신하는 통신부를 포함하는 것을 일 특징으로 한다.

[0031] 나아가 상기 PIN 코드는 현재 펌웨어의 제1 PIN 코드와 상기 보안 모듈의 현재 인증 정보 업데이트를 위한 제2 PIN 코드를 포함하는 것을 일 특징으로 한다.

[0032] 또한 상기 보안 모듈은 상기 제2 인증 정보를 검증하고, 검증이 완료되면 검증 결과를 디바이스 프로세서에 송신하는 것을 일 특징으로 한다.

[0033] 나아가 상기 보안 모듈의 패스워드와 상기 제2 인증 정보의 패스워드를 비교하고, 상기 보안 모듈의 PIN 코드와 상기 제2 인증 정보의 제1 PIN 코드를 비교하고, 상기 보안 모듈의 펌웨어 버전과 상기 제2 인증 정보의 펌웨어 버전을 비교하여 상기 제2 인증 정보의 검증 결과를 생성하는 것을 일 특징으로 한다.

[0034] 또한 상기 제2 인증 정보가 적합하다고 검증되면 성공 메시지를 생성하고, 상기 제2 인증 정보가 적합하지 않다고 검증되면 에러 메시지를 생성하는 것을 일 특징으로 한다.

발명의 효과

[0036] 전술한 바와 같은 본 발명에 의하면, IoT 디바이스가 펌웨어 업데이트를 수행하고자 할 때 공격자가 불법 펌웨어를 이용하여 펌웨어 업데이트를 수행하는 것을 차단할 수 있다.

[0037] 또한, 본 발명은 별도의 보안 모듈을 이용하여 불법 펌웨어를 검증함으로써, 보안성을 더욱 향상시킬 수 있다.

[0038] 또한, 본 발명은 불법 펌웨어를 검증하여 IoT 디바이스의 업데이트를 차단함으로써 사용자의 데이터 및 사생활을 보호할 수 있다.

도면의 간단한 설명

[0040] 도1은 본 발명의 일 실시 예에 의한 보안 펌웨어 업데이트 시스템의 구성을 도시한 도면이다.

도2는 본 발명의 일 실시 예에 의한 보안 펌웨어 업데이트 방법을 설명하기 위한 도면이다.

도3은 본 발명의 일 실시 예에 의한 인증 정보 검증 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0041] 전술한 목적, 특징 및 장점은 첨부된 도면을 참조하여 상세하게 후술되며, 이에 따라 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 상세한 설명을 생략한다.

[0042] 도면에서 동일한 참조부호는 동일 또는 유사한 구성요소를 가리키는 것으로 사용되며, 명세서 및 특허청구의 범위에 기재된 모든 조합은 임의의 방식으로 조합될 수 있다. 그리고 다른 식으로 규정하지 않는 한, 단수에 대한 언급은 하나 이상을 포함할 수 있고, 단수 표현에 대한 언급은 또한 복수 표현을 포함할 수 있음이 이해되어야 한다.

[0043] 본 명세서에서 사용되는 용어는 단지 특정 예시적 실시 예들을 설명할 목적을 가지고 있으며 한정할 의도로 사용되는 것이 아니다. 본 명세서에서 사용된 바와 같은 단수적 표현들은 또한, 해당 문장에서 명확하게 달리 표시하지 않는 한, 복수의 의미를 포함하도록 의도될 수 있다. 용어 "및/또는," "그리고/또는"은 그 관련되어 나열되는 항목들의 모든 조합들 및 어느 하나를 포함한다. 용어 "포함한다", "포함하는", "포함하고 있는", "구비하는", "갖는", "가지고 있는" 등은 내포적 의미를 갖는바, 이에 따라 이러한 용어들은 그 기재된 특징, 정수, 단계, 동작, 요소, 및/또는 컴포넌트를 특정하며, 하나 이상의 다른 특징, 정수, 단계, 동작, 요소, 컴포넌트, 및/또는 이들의 그룹의 존재 혹은 추가를 배제하지 않는다. 본 명세서에서 설명되는 방법의 단계들, 프로세스들, 동작들은, 구체적으로 그 수행 순서가 확정되는 경우가 아니라면, 이들의 수행을 논의된 혹은 예시된 그러한 특정 순서로 반드시 해야 하는 것으로 해석돼서는 안 된다. 추가적인 혹은 대안적인 단계들이 사용될 수 있음을 또한 이해해야 한다.

[0044] 또한, 각각의 구성요소는 각각 하드웨어 프로세서로 구현될 수 있고, 위 구성요소들이 통합되어 하나의 하드웨어 프로세서로 구현될 수 있으며, 또는 위 구성요소들이 서로 조합되어 복수 개의 하드웨어 프로세서로 구현될 수도 있다.

[0045] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시 예를 상세히 설명하기로 한다.

[0047] 도1은 본 발명의 일 실시 예에 의한 보안 펌웨어 업데이트 시스템의 구성을 도시한 도면이다. 도1을 참조하면,

본 발명의 일 실시예에 의한 보안 펌웨어 업데이트 시스템은 펌웨어 업데이터(100)와 디바이스 프로세서(200), 그리고 보안 모듈(300)을 포함한다.

[0048] 펌웨어 업데이터(100)는 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서(200)로 전송하고, 펌웨어를 업데이트하는 장치로, 펌웨어 패키지 생성부(120), 펌웨어 업데이트부(140), 그리고 통신부(160)를 포함할 수 있다.

[0049] 펌웨어 패키지 생성부(120)는 보안 모듈(300)에 저장된 데이터를 업데이트하기 위해 펌웨어 패키지를 생성할 수 있다. 여기서 펌웨어 패키지는 제1 인증 정보와 새로운 펌웨어를 포함할 수 있다.

[0050] 보다 구체적으로 제1 인증 정보는 통신부(160)를 통해 수신한 보안 모듈(300)의 인증 정보 업데이트를 요청하기 위한 기 설정된 패스워드와 새로운 펌웨어 버전 식별 정보, 그리고 새로운 펌웨어 바이너리 이미지에 SHA 함수를 적용함으로써 생성된 새로운 펌웨어 이미지 해시를 포함할 수 있다. 일반적으로 펌웨어 패키지의 인증 정보에는 PIN 코드가 포함되어 있으나, 본 발명에서 PIN 코드 생성 알고리즘을 펌웨어 업데이터(100)가 아닌 디바이스 프로세서(200)가 보유하고 있기 때문에 제1 인증 정보에는 PIN 코드의 데이터가 존재하지 않을 수 있다.

[0051] 보다 구체적으로 제1 인증 정보의 패스워드는 IoT 디바이스가 제조될 때 설정되는 패스워드로, 모든 디바이스가 상이한 값을 보유할 수 있다. 그리고 새로운 펌웨어의 버전 식별 정보는 디바이스 프로세서(200)의 플래시 메모리의 서비스 어플리케이션에 대한 정보를 포함한다.

[0052] 또한 새로운 펌웨어 이미지 해시는 새로운 펌웨어 바이너리 이미지에 SHA 함수를 적용함으로써 생성될 수 있다. SHA 함수는 임의의 길이로 구성된 데이터를 고정된 길이의 해시 값으로 출력하는 함수이다. SHA 함수를 통해 데이터의 오류나 변조를 탐지할 수 있도록 하는 무결성을 제공할 수 있으며 SHA 함수로는 SHA-1, SHA-256, SHA-384, SHA-512 등이 있으며, SHA-1은 공격에 대한 취약점이 발견되었기 때문에 SHA-256 이상의 SHA 함수를 사용하는 것이 보다 바람직하다. 다만, 본 발명은 이러한 예시에 의해 한정되지 아니하며, 상술한 함수의 종류 외의 다른 종류의 SHA 함수도 적용 가능하다.

[0053] 펌웨어 업데이트부(140)는 디바이스 프로세서(200)가 송신한 검증 결과에 따라 펌웨어 업데이트를 결정할 수 있다. 검증 결과는 성공 메시지와 에러 메시지로 구분될 수 있다. 펌웨어 업데이터의 통신부(160)가 성공 메시지를 수신했을 경우 펌웨어 업데이트부(140)는 펌웨어 업데이트를 수행하고, 에러 메시지를 수신했을 경우 펌웨어 업데이트부(140)는 인증 정보가 적합하지 않다고 판단하여 펌웨어 업데이트를 중단할 수 있다.

[0054] 통신부(160)는 새로운 펌웨어 바이너리 이미지, 기 설정된 패스워드 및 새로운 펌웨어 버전 식별 정보를 수신하고, 펌웨어 패키지 생성부(120)가 생성한 새로운 펌웨어의 제1 인증 정보를 디바이스 프로세서(200)로 전송할 수 있다.

[0056] 디바이스 프로세서(200)는 PIN 코드를 생성하고, 제1 인증 정보에 PIN 코드를 포함시켜 제2 인증 정보를 생성하며, 제2 인증 정보를 보안 모듈(300)로 전송하는 장치로, 어플리케이션부(240)와 인증 정보 관리부(220)를 포함할 수 있다.

[0057] 어플리케이션부(240)는 펌웨어 업데이터(100)가 송신한 제1 인증 정보를 UART Interrupt Receiver 기능을 이용하여 수신할 수 있다. 보다 구체적으로, UART Interrupt Receiver 기능은 병렬 데이터의 형태를 직렬 방식으로 전환하여 데이터를 송수신하는 것이다. 기본적으로 8 bit의 데이터 영역과 데이터 영역의 시작과 끝을 알리는 2~3 bit의 동기화 비트, 그리고 에러 보정 방법으로 사용되는 패리티 비트의 구조를 통해 데이터를 송신할 수 있다. 패리티 비트는 데이터 영역에 해당하는 5~9 bit의 값을 모두 더하여 홀수인지 짝수인지의 여부를 판단하여 패리티 비트의 데이터 공간에 기록하여 송신할 수 있다. 데이터를 수신한 수신자는 동일한 작업을 수행하여 수신된 패리티 비트와 일치하는 지를 비교하여 데이터 영역에 에러가 발생하였는 지를 판단할 수 있다.

[0058] 어플리케이션부(240)는 인증 정보의 검증 요청 및 현재 인증 정보의 업데이트 요청을 위해 보안 모듈(300)과 통신할 수 있으며 인증 정보의 검증 결과 제공을 위해 펌웨어 업데이터(100)와 통신할 수 있다. 보다 구체적으로 인증 정보의 검증을 위해 인증 정보를 보안 모듈(300)로 전송하고, 보안 모듈(300)이 인증 정보의 검증을 완료하면, 보안 모듈(300)로부터 검증 결과를 수신하고, 수신한 검증 결과를 펌웨어 업데이터(100)에 전송할 수 있다.

[0059] 인증 정보 관리부(220)는 펌웨어 업데이터(100)가 전송한 제1 인증 정보를 이용하여 PIN 코드를 생성하고, PIN 코드를 제1 인증 정보에 포함시켜 제2 인증 정보를 생성할 수 있으며, 보다 구체적으로 PIN 코드 생성부(223)와

제2 인증 정보 생성부(225), 그리고 APDU 생성부(미도시)를 포함할 수 있다.

[0060] PIN 코드 생성부(223)는 현재 펌웨어의 제1 PIN 코드와 보안 모듈의 현재 인증 정보 업데이트를 목적으로 하는 제2 PIN 코드를 생성할 수 있다. PIN 코드는 애플릿이 구동될 때마다 사용자를 인증하는 데에 사용되는 8 bit의 숫자 암호로, AES 함수를 통해 내부적으로 암호화되어 보관될 수 있다.

[0061] AES 함수는 암호화 및 복호화 과정에서 동일한 키를 사용하는 대칭 키 알고리즘으로, 해당 키가 제3자에게 노출되지 않도록 관리해야 한다. AES 함수는 AES_SETKEY 명령에 의해 AES 키 길이 및 암호화 모드를 정의할 수 있다.

[0062] PIN 코드는 비공개로 관리되는 Key Generation Algorithm을 통해 생성될 수 있으며, 현재 펌웨어의 PIN 코드는 현재 펌웨어의 이미지 해시를, 보안 모듈의 현재 인증 정보 업데이트를 목적으로 하는 PIN 코드는 새로운 펌웨어의 이미지 해시를 통해 생성될 수 있다.

[0063] 제2 인증 정보 생성부(225)는 PIN 코드 생성부(223)에서 생성된 PIN 코드를 제1 인증 정보에 추가할 수 있다.

[0064] 어플리케이션부(240)는 제2 인증 정보를 보안 모듈로 전송하고, 보안 모듈이 송신한 제2 인증 정보의 검증 결과를 펌웨어 업데이터(100)에 송신할 수 있다. 디바이스 프로세서(200)가 보안 모듈(300)과 통신하기 위해서는 APDU 생성부가 생성한 APDU 프로토콜을 사용할 수 있다. APDU 프로토콜은 Command APDU와 Response APDU로 나눌 수 있다. Command APDU는 요청할 명령을 나타내는 4 byte 헤더부와 필요한 경우 사용하는 데이터 필드 등을 포함하는 옵션부로 구성될 수 있으며, Response APDU는 데이터 필드, 서로를 연결하여 결과 메시지를 나타내는 상태 코드인 SW1과 SW2로 구성될 수 있다.

[0065] 디바이스 프로세서(200)가 생성한 제2 인증 정보를 Command APDU의 구조로 보안 모듈(300)에 송신하고자 할 때, 제2 인증 정보를 데이터 필드에 저장하고, 요청 타입을 헤더부에 저장할 수 있다. 보다 구체적으로, Command APDU는 명령 클래스 CLA, 명령 코드인 INS, 명령 코드의 파라미터 P1과 P2, 데이터 필드의 길이, 데이터 필드, 받을 응답 길이 Le로 구성될 수 있다. 예를 들어 PIN 코드의 Command APDU는 CLA:80, INS:20, P1:00, P2:00, Le:04, 데이터 필드:PIN 코드, Le:N/A로 구성될 수 있다. Command APDU의 생성이 완료되면 어플리케이션부(240)는 보안 모듈(300)에 Command APDU를 송신할 수 있다.

[0067] 보안 모듈(300)은 디바이스 인증을 기본으로 수행하며 저장된 개인 정보 및 데이터를 보호하기 위한 암호화 키를 생성하고, 생성된 키를 보안 모듈 내부에 저장하여 소프트웨어 기반의 불법 프로그램으로부터 IoT 디바이스를 보호할 수 있다. 또한, 보안 모듈의 내부에는 JavaCard OS 등과 같은 별도의 운영체제가 포함되어 있어 기존 시스템과 통합하기 쉽고, 시스템의 요구사항에 맞춰 칩 내부에 개별적인 보안 솔루션을 프로그래밍 할 수 있다는 장점이 있다.

[0068] 보안 모듈(300)은 디바이스 프로세서(200)로부터 수신한 제2 인증 정보에서 패스워드, 버전 정보, PIN 코드를 추출하고, 기 저장된 현재 인증 정보의 패스워드, 버전 정보, PIN 코드와 비교하여 검증한 후, 검증이 완료되면 기 저장된 현재 인증 정보를 제2 인증 정보로 업데이트하고, 업데이트가 완료되면 제2 인증 정보의 검증 결과를 펌웨어 업데이터(100)로 전송하는 장치로, 보안 애플릿부(320)와 데이터부(340)를 포함할 수 있다.

[0069] 보안 애플릿은 JavaCard OS에서 동작하는 응용 프로그램이다. 보안 모듈(300)은 다양한 보안 애플릿을 사용할 수 있으며, APDU 명령을 통해 실행 및 응답을 보낼 수 있다.

[0070] 보안 애플릿부(320)는 보안 펌웨어 업데이트를 수행하기 위한 기술을 포함하고 있으며, 제2 인증 정보를 검증하고, 검증이 완료되면 데이터부(360)의 현재 인증 정보를 제2 인증 정보로 업데이트할 지를 결정하고, 검증 결과를 디바이스 프로세서(200)에 송신할 수 있으며, 보다 구체적으로 검증부(330)와 통신부(340)를 포함할 수 있다.

[0071] 검증부(330)는 디바이스 프로세서(200)로부터 수신된 Command APDU에서 제2 인증 정보를 추출한 후 데이터부(360)에 저장된 현재 인증 정보와 비교하여 검증을 수행함으로써 새로운 펌웨어가 적합한 지의 여부를 판단할 수 있다. 보다 구체적으로 패스워드 검증부(332)와 버전 정보 검증부(334)와 PIN 코드 검증부(336), 그리고 업데이트부(338)를 포함할 수 있다.

[0072] 패스워드 검증부(332)는 데이터부(360)에 저장된 현재 인증 정보의 패스워드와 제2 인증 정보의 패스워드를 비교할 수 있다. 현재 인증 정보의 패스워드와 제2 인증 정보의 패스워드가 일치할 경우에는 버전 정보 검증부

(334)가 버전 정보를 검증하는 단계로 넘어가며, 일치하지 않으면 데이터 필드:N/A, SW1:6A, SW2:10의 Response APDU 구조를 갖는 에러 메시지를 생성하여 디바이스 프로세서(200)로 송신할 수 있다. 따라서 패스워드를 검증하는 과정에서 공격자는 IoT 디바이스의 고유한 패스워드를 알 수 없기 때문에 불법 펌웨어를 이용하여 펌웨어를 업데이트할 수 없도록 하는 효과가 있다.

[0073] 버전 정보 검증부(334)는 데이터부(360)에 저장된 현재 인증 정보의 버전 정보와 제2 인증 정보의 버전 정보 즉, 현재 펌웨어의 버전과 새로운 펌웨어의 버전을 비교할 수 있다. 보다 구체적으로 현재 인증 정보에 포함된 버전 정보보다 제2 인증 정보에 포함된 새로운 펌웨어의 버전 정보가 상위 버전인 지를 확인할 수 있다. 펌웨어의 버전은 비공개로 관리되기 때문에 공격자가 현재 펌웨어보다 상위 버전의 펌웨어를 생성할 수 없다. 따라서 공격자가 이전 펌웨어 중 취약성이 있는 펌웨어를 변조하여 IoT 디바이스의 펌웨어의 업데이트를 시도할 경우에, 보안 모듈(300)이 새로운 펌웨어 버전 정보가 현재 펌웨어의 버전 정보와 일치하거나 그 이하의 버전 정보라고 판단하게 되어 펌웨어의 업데이트를 진행할 수 없도록 하는 효과가 있다.

[0074] 보다 구체적으로 현재 인증 정보의 버전 정보가 제2 인증 정보의 버전 정보보다 상위 버전일 경우 PIN 코드 검증부(336)가 PIN 코드를 검증하는 단계로 넘어가며, 현재 인증 정보의 버전 정보가 제2 인증 정보의 버전 정보와 일치하거나 그보다 낮은 하위 버전일 경우 데이터 필드: N/A, SW1:6A, SW2:30의 Response APDU 구조를 갖는 에러 메시지를 생성하여 디바이스 프로세서(200)로 송신할 수 있다. 따라서, 공격자가 이전 펌웨어 중 취약성이 있는 펌웨어를 변조하여 IoT 디바이스의 펌웨어의 업데이트를 시도할 경우에 보안 모듈(300)이 새로운 펌웨어 버전 정보가 현재 펌웨어의 버전 정보와 일치하거나 그 이하의 버전 정보라고 판단하면 펌웨어의 업데이트를 진행할 수 없도록 하는 효과가 있다.

[0075] PIN 코드 검증부(336)는 데이터부(360)에 저장된 현재 인증 정보의 PIN 코드와 제2 인증 정보의 제1 PIN 코드를 비교할 수 있다.

[0076] 업데이트부(338)는 패스워드와 버전 정보, 그리고 PIN 코드가 모두 적합하다고 판단하면 데이터부(360)의 현재 인증 정보를 제2 인증 정보로 업데이트할 수 있다. 또한 디바이스의 펌웨어 업데이트를 위하여 검증 성공 메시지를 생성하여 디바이스 프로세서(200)에게 송신할 수 있다. 이 때, 검증 성공 메시지는 데이터 필드: N/A, SW1:90, SW2:00의 Response APDU 구조로 생성될 수 있다.

[0077] 데이터부(360)는 패스워드, 현재 펌웨어의 인증 정보 등을 저장한다. 데이터부(360)는 각종 중요 데이터를 안전하게 보관하기 위한 용도로 사용되며, 데이터부(360)에 저장된 데이터는 보안 모듈(300)의 전원이 차단되어도 손실되지 않는다. 본 발명에서 데이터부(360)에는 패스워드, 현재 펌웨어의 인증 정보 등이 저장될 수 있다. 또한, 보안 모듈(300)의 운영 체제(JavaCard OS), Stack, APDU 버퍼 등은 기타 영역으로 분류될 수 있다.

[0078] 통신부(340)는 디바이스 프로세서(200)로부터 제2 인증 정보를 수신하고, 검증부가 수행한 제2 인증 정보의 검증 결과, 즉 성공 메시지 또는 에러 메시지를 디바이스 프로세서(200)로 전송할 수 있다.

[0080] 이하에서는 도2 내지 도3을 참조하여 본 발명의 일 실시 예에 의한 보안 펌웨어 업데이트 방법을 설명한다. 보안 펌웨어 업데이트 방법에 관한 설명에서 전술한 보안 펌웨어 업데이트 시스템과 중복되는 세부 실시 예는 생략될 수 있다.

[0081] 도2를 참조하면 먼저 펌웨어 업데이터(100)는 제조사로부터 새로운 펌웨어 바이너리 이미지를 수신할 수 있다. 도2에는 도시되지 않았으나 펌웨어 업데이터(100)는 제조사로부터 새로운 펌웨어 바이너리 이미지 뿐 아니라 IoT 디바이스의 패스워드와 새로운 펌웨어의 버전 정보도 함께 수신할 수 있다(S100).

[0082] 펌웨어 업데이터(100)는 새로운 펌웨어 바이너리 이미지에 SHA 함수를 적용하여 새로운 펌웨어 이미지 해시를 생성할 수 있다.

[0083] 새로운 펌웨어 이미지 해시를 생성하면, 펌웨어 업데이터(100)는 패스워드, 새로운 펌웨어 이미지 해시, 새로운 펌웨어의 버전 정보를 포함하는 제1 인증 정보를 생성할 수 있다(S200).

[0084] 제1 인증 정보가 생성되면, 펌웨어 업데이터(100)는 제1 인증 정보를 디바이스 프로세서(200)에 전송할 수 있다.(S290) 디바이스 프로세서(200)는 제1 인증 정보의 새로운 펌웨어 이미지 해시 값에 기 저장된 PIN 코드 생성 알고리즘을 적용하여 PIN 코드를 생성할 수 있다.(S300)

[0085] PIN 코드가 생성되면, 디바이스 프로세서(200)는 제1 인증 정보의 비어 있는 PIN 코드의 데이터 공간에 생성한

PIN 코드를 포함시켜 제2 인증 정보를 생성할 수 있다.(S400)

[0086] 다음으로, 디바이스 프로세서(200)는 생성된 제2 인증 정보를 이용하여 새로운 펌웨어 검증 요청을 위해 보안 모듈(300)에 제2 인증 정보를 전송할 수 있다.(S490)

[0087] 디바이스 프로세서(200)가 제2 인증 정보를 보안 모듈(300)로 전송하면, 보안 모듈(300)은 제2 인증 정보의 패스워드, 버전 정보, PIN 코드를 추출할 수 있다. 그리고 보안 모듈(300)에 저장된 현재 인증 정보와 비교하여 검증을 수행할 수 있다.(S500)

[0088] 단계 500에서 보안 모듈(300)은 도3에 도시된 바와 같이 현재 인증 정보의 패스워드와 제2 인증 정보의 패스워드가 일치하는지 판단하고(S510), 단계 510에서의 판단 결과 현재 인증 정보의 패스워드와 제2 인증 정보의 패스워드가 일치하면 PIN 코드 검증 단계로 넘어가고, 일치하지 않으면 현재 인증 정보를 제2 인증 정보로 업데이트 하지 않고(S560) 패스워드 에러 메시지를 생성할 수 있다.(S570)

[0089] 단계 520에서 보안 모듈(300)은 현재 인증 정보의 PIN 코드와 제2 인증 정보의 제1 PIN 코드가 일치하는 지 판단하고, 단계 520의 판단 결과 현재 인증 정보의 PIN 코드와 제2 인증 정보의 PIN 코드가 일치하면 버전 정보 검증 단계로 넘어가고, 일치하지 않으면 현재 인증 정보를 제2 인증 정보로 업데이트 하지 않고(S560) PIN 코드 에러 메시지를 생성할 수 있다.(S570)

[0090] 단계 530에서 보안 모듈(300)은 현재 인증 정보의 버전 정보와 제2 인증 정보의 버전 정보를 비교할 수 있다. 제2 인증 정보의 버전 정보가 현재 인증 정보의 버전 정보보다 상위 버전일 경우 제2 인증 정보가 적합하다는 검증이 완료될 수 있다. 만약 제2 인증 정보의 버전 정보가 현재 인증 정보의 버전 정보와 일치하거나 또는 그 하위 버전일 경우 보안 모듈(300)은 현재 인증 정보를 제2 인증 정보로 업데이트 하지 않고(S560) 버전 정보 에러 메시지를 생성할 수 있다.(S570)

[0091] 단계 510 내지 단계 530에서 제2 인증 정보가 적합하다는 검증이 완료되면 보안 모듈(300)은 현재 인증 정보를 제2 인증 정보로 업데이트할 수 있다.(S600)

[0092] 현재 인증 정보를 제2 인증 정보로 업데이트를 하면, 보안 모듈(300)은 성공 메시지를 생성할 수 있다.(S650)

[0093] 제2 인증 정보 검증을 완료하고 검증 결과를 생성하면, 보안 모듈(300)은 제2 인증 정보의 검증 결과를 디바이스 프로세서(200)에 전송할 수 있다.(S680)

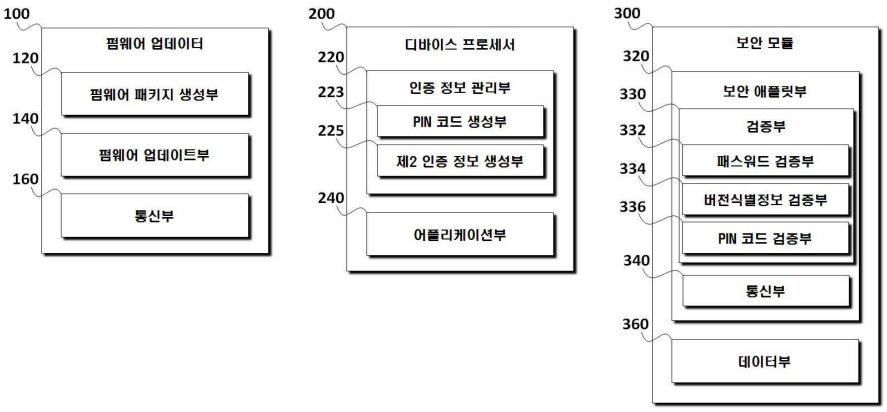
[0094] 디바이스 프로세서(200)는 보안 모듈(300)로부터 수신한 제2 인증 정보 검증 결과를 펌웨어 업데이터(100)에 전송할 수 있다.(S690)

[0095] 펌웨어 업데이터(100)는 디바이스 프로세서(200)로부터 수신한 제2 인증 정보 검증 결과에서 성공 메시지 또는 에러 메시지를 추출할 수 있다. 추출한 제2 인증 정보 검증 결과가 성공 메시지일 경우 펌웨어 업데이터(100)는 현재 펌웨어를 새로운 펌웨어로 업데이트할 수 있다.(S900) 또한, 추출한 제2 인증 정보 검증 결과가 에러 메시지일 경우 펌웨어 업데이터(100)는 펌웨어 업데이트를 중지하고 현재 펌웨어를 유지할 수 있다.(S800)

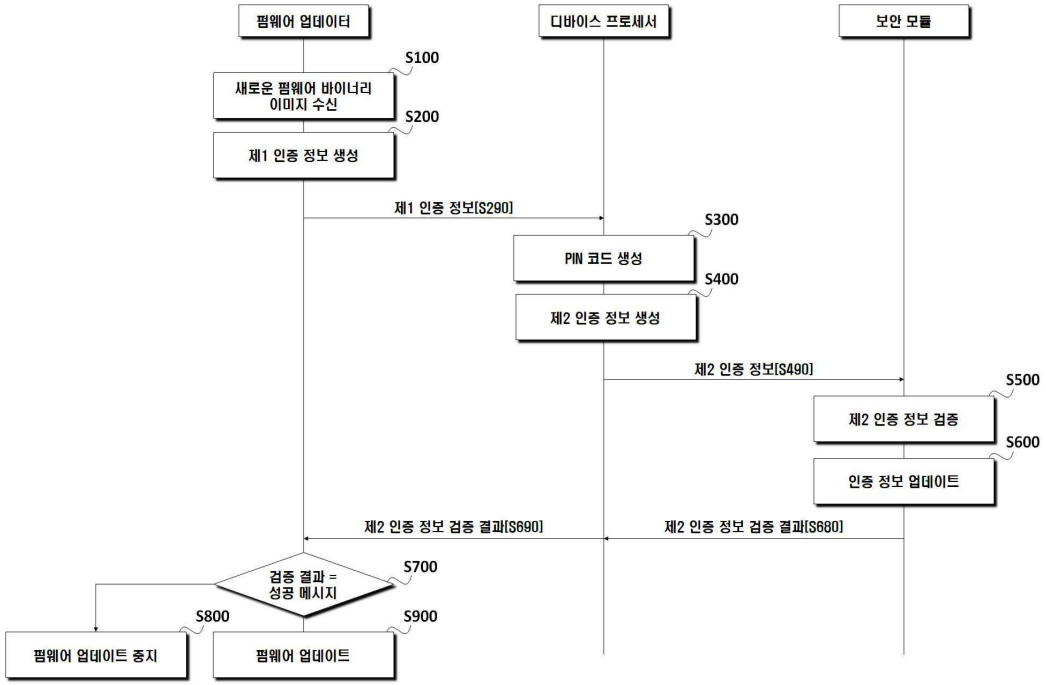
[0096] 본 명세서와 도면에 개시된 본 발명의 실시 예들은 본 발명의 기술 내용을 쉽게 설명하고 본 발명의 이해를 돕기 위해 특정 예를 제시한 것뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다.

도면

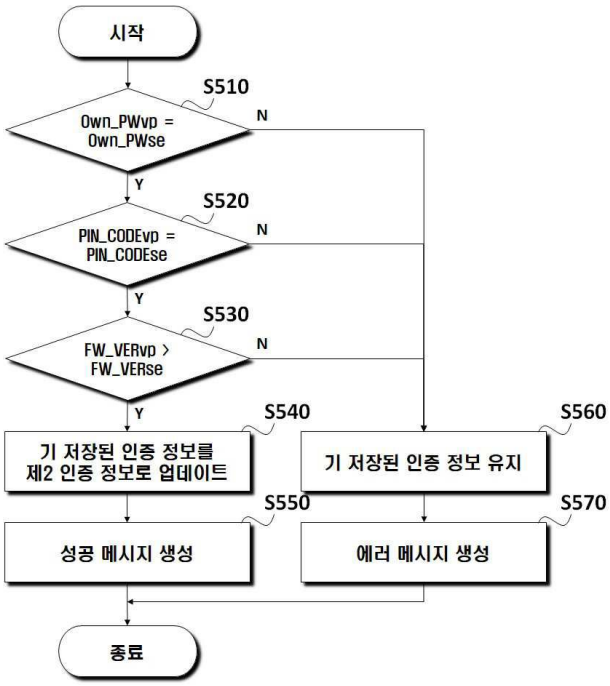
도면1


100
펌웨어 업데이터
120
펌웨어 패키지 생성부
140
펌웨어 업데이트부
160
통신부
200
디바이스 프로세서
220
인증 정보 관리부
223
PIN 코드 생성부
225
제2 인증 정보 생성부
240
어플리케이션부
300
보안 모듈
320
보안 애플릿부
330
검증부
332
패스워드 검증부
334
버전식별정보 검증부
336
PIN 코드 검증부
340
통신부
360
데이터부

도면2


펌웨어 업데이터
디바이스 프로세서
보안 모듈
S100
새로운 펌웨어 바이너리 이미지 수신
S200
제1 인증 정보 생성
제1 인증 정보[S290]
S300
PIN 코드 생성
S400
제2 인증 정보 생성
제2 인증 정보[S490]
S500
제2 인증 정보 검증
S600
인증 정보 업데이트
제2 인증 정보 검증 결과[S690]
제2 인증 정보 검증 결과[S680]
검증 결과 = 성공 메시지
S700
S800
펌웨어 업데이트 중지
S900
펌웨어 업데이트

도면3


시작
S510
Own_PWvp =
Own_PWse
N
Y
S520
PIN_CODEvp =
PIN_CODEse
N
Y
S530
FW_VERvp >
FW_VERse
N
Y
S540
기 저장된 인증 정보를
제2 인증 정보로 업데이트
S560
기 저장된 인증 정보 유지
S550
성공 메시지 생성
S570
에러 메시지 생성
종료