(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 1/00 (2006.01)
G06F 12/00 (2006.01)

(45) 공고일자 2007년02월01일
(11) 등록번호 10-0676087
(24) 등록일자 2007년01월24일

(21) 출원번호 10-2005-0024353
(22) 출원일자 2005년03월24일
심사청구일자 2005년03월24일

(65) 공개번호 10-2006-0102584
(43) 공개일자 2006년09월28일

(73) 특허권자 케이비 테크놀러지 (주)
서울특별시 영등포구 여의도동 15-24 익스콘벤처타워 801호

(72) 발명자 조정일
서울 양천구 목1동 931 현대1차 103-401

전철항
경기 성남시 분당구 서현동 시범단지한신아파트 113-301

(74) 대리인 이헌수
이은철

(56) 선행기술조사문헌
1020030093079 *
* 심사관에 의하여 인용된 문헌

심사관 : 이영수

전체 청구항 수 : 총 4 항

(54) 유에스비 인터페이스를 구비한 보안 데이터 저장 장치 및방법

(57) 요약

보안 데이터를 저장하는 장치 및 그 방법이 개시된다. 본 발명에 따라, 데이터 저장 방법은 (a) USB 인터페이스를 통해 데이터를 수신하는 단계; 및 (b) 상기 수신된 데이터를, 인증을 통해서만 접근이 가능한 보안 영역에 저장하거나 또는 인증 없이도 접근이 가능한 일반 영역에 저장하는 단계를 포함하는 것을 특징으로 한다. 이에 의해, 공인 인증서, 개인별 계좌번호나 신용 카드 데이터, 중요한 아이디 및 패스 워드 데이터, 기타 사용자 인증을 요구하는 데이터를 보다 안전하게 저장할 수 있으며, RF 송수신부를 더 구비하여 전자 지갑 또는 교통 카드의 기능을 함께 수행할 수 있다.

대표도

도 2

특허청구의 범위

청구항 1.
삭제

청구항 2.
삭제

청구항 3.
삭제

청구항 4.
삭제

청구항 5.
삭제

청구항 6.

USB 인터페이스를 통해 데이터를 수신하는 USB 커넥터;

상기 수신된 데이터를 어느 영역에 저장하는가 하는 정보에 따라 상기 수신된 데이터의 저장 영역을 결정하여, 상기 수신된 데이터를 전달하는 제어부;

상기 수신된 데이터를 저장하는, 인증과정 없이 접근가능한 플래시 메모리; 및

상기 수신된 데이터를 저장하는, 인증과정을 통해 접근 가능한 보안칩을 포함하는 것을 특징으로 하는 데이터 저장 장치.

청구항 7.

제6항에 있어서,

상기 보안칩에 저장된 데이터를 RF 신호에 실어서 전송하고, 외부 RF 장치로부터의 데이터를 RF 신호를 통해 수신하는 RF 송수신부를 더 포함하는 것을 특징으로 하는 데이터 저장 장치.

청구항 8.

제6항 또는 제7항에 있어서,

상기 보안칩은 상기 수신된 데이터를 암호화하여 상기 보안칩에 포함된 메모리에 저장하거나, 상기 수신된 데이터를 암호화하여 상기 플래시 메모리로 전달하는 것을 특징으로 하는 데이터 저장 장치.

청구항 9.

제6항 또는 제7항에 있어서, 상기 보안칩은

상기 수신된 데이터의 전달을 제어하는 보안칩 제어부;

상기 수신된 데이터를 소정의 암호화 알고리즘에 따라 암호화하는 암호화 처리부; 및

상기 수신된 데이터를 그대로 저장하거나, 상기 암호화 처리부에 의해 암호화된 데이터를 저장하는 보안 데이터 저장부를 포함하는 것을 특징으로 하는 데이터 저장 장치.

청구항 10.

삭제

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 데이터 보안 기술에 관한 것으로, 보다 상세하게는 데이터를 안전하게 저장하는 장치 및 그 방법에 관한 것이다.

데이터 저장 기술의 발달로 여러 가지 종류의 휴대용 저장 장치가 사용되고 있다. 이들 휴대용 저장 장치 중에서 USB (Universal Serial Bus) 인터페이스를 구비한 플래시 메모리는 저장용량이 크면서도 휴대가 간편하고 PC와의 연결이 용이하여, 문서 데이터, 음악이나 사진 및 동영상 파일의 저장 등 여러 분야에서 널리 사용되고 있다. 그러나, 이러한 USB 플래시 메모리는 보안 기능이 매우 취약하다. 최근에는 USB 플래시 메모리의 특정 영역을 액세스하는데 패스워드를 요구하는 등의 기능을 구비한 USB 플래시 메모리도 있지만, 해커에 의한 물리적 해킹, 메모리의 덤프나 복사 등의 수단을 통해 USB 플래시 메모리에 저장된 데이터를 액세스하는 것이 가능하므로 근본적인 문제 해결 수단은 되지 못한다.

한편, 자체적인 운영체제(OS)로써 칩OS(Chip Operating System)가 탑재되고 중앙처리장치(CPU)와 보안 모듈 및 메모리를 갖춘 IC 카드가 있다. IC 카드는 암호화 기술을 채용하고 있어, 여러가지 트랜잭션을 안전하게 처리하고, 데이터를 암호화하여 저장할 수 있어 전자 지갑, 전자 통장, 개인 인증 등의 분야에서 널리 사용되고 있다. 그러나 IC 카드는 보안성이 뛰어나기는 하지만, 그 저장용량이 플래시 메모리에 비해 크지 않다. 또한, IC 카드에 데이터를 저장하거나 저장된 데이터를 읽기 위해서는 IC 카드를 읽을 수 있는 리더기가 필요하나, IC 카드 리더기는 USB 인터페이스만큼 널리 보급되어 있지 않아 사용이 불편하다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명이 이루고자 하는 기술적 과제는, USB 플래시 메모리와 IC 카드를 결합하여, 데이터를 안전하게 저장할 수 있는 보안 데이터 저장 장치 및 저장 방법을 제공하는 것이다.

본 발명이 이루고자 하는 다른 기술적 과제는, USB 플래시 메모리와 IC 카드를 결합하고, 이에 RF 송수신부를 더 구비하여 전자지갑, 전자화폐 및 교통카드 기능을 갖춘 보안 데이터 저장 장치를 제공하는 것이다.

발명의 구성

상기 기술적 과제는 본 발명에 따라, (a) USB 인터페이스를 통해 데이터를 수신하는 단계; 및 (b) 상기 수신된 데이터를, 인증을 통해서만 접근이 가능한 보안 영역에 저장하거나 또는 인증 없이도 접근이 가능한 일반 영역에 저장하는 단계를 포함하는 것을 특징으로 하는 데이터 저장 방법에 의해 달성된다.

상기 (b) 단계는, (b1) 상기 수신된 데이터를 암호화하는 단계; 및 (b2) 상기 암호화된 데이터를, 인증을 통해서만 접근이 가능한 보안 영역에 저장하거나 또는 인증 없이도 접근이 가능한 일반 영역에 저장하는 단계를 포함하는 것이 바람직하다.

또한, 상기 기술적 과제는 (a) 독출하고자 하는 데이터에 관한 정보를 입력받는 단계; (b) 상기 선택된 데이터가, 인증을 통해서만 접근이 가능한 보안 영역에 저장되어 있는지 또는 인증 없이도 접근이 가능한 일반 영역에 저장되어 있는지 판단하는 단계; 및 (c) 상기 판단 결과에 따라 보안 영역 또는 일반 영역에서 데이터를 독출하는 단계를 포함하는 것을 특징으로 하는 데이터 독출 방법에 의해서도 달성된다

상기 독출 방법은, (d) 상기 독출된 데이터가 암호화된 데이터이면 복호화를 수행하는 단계를 더 포함하는 것이 바람직하다.

한편, 본 발명의 다른 분야에 따르면, 상기 기술적 과제는 USB 인터페이스를 통해 데이터를 수신하는 USB 커넥터; 상기 수신된 데이터를 어느 영역에 저장하는가 하는 정보에 따라 상기 수신된 데이터의 저장 영역을 결정하여, 상기 수신된 데이터를 전달하는 제어부; 상기 수신된 데이터를 저장하는, 인증과정 없이 접근가능한 플래시 메모리; 및 상기 수신된 데이터를 저장하는, 인증과정을 통해 접근 가능한 보안칩을 포함하는 것을 특징으로 하는 데이터 저장 장치에 의해서도 달성된다.

상기 데이터 저장 장치는, 상기 보안칩에 저장된 데이터를 RF 신호에 실어서 전송하고, 외부 RF 장치로부터의 데이터를 RF 신호를 통해 수신하는 RF 송수신부를 더 포함하는 것이 바람직하다.

또한, 상기 보안칩은 상기 수신된 데이터의 전달을 제어하는 보안칩 제어부; 상기 수신된 데이터를 소정의 암호화 알고리즘에 따라 암호화하는 암호화 처리부; 및 상기 수신된 데이터를 그대로 저장하거나, 상기 암호화 처리부에 의해 암호화된 데이터를 저장하는 보안 데이터 저장부를 포함하는 것이 바람직하다.

이하 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대해 상세히 설명한다.

도 1은 USB 인터페이스를 갖는 플래시 저장장치의 구성도이다.

USB 인터페이스를 갖는 플래시 저장장치는 USB 커넥터(110), 제어부(120) 및 플래시 메모리(130)를 포함한다. USB 커넥터(110)는 호스트와 데이터를 주고 받기 위한 물리적 인터페이스를 제공한다. 즉, USB로 정의된 버스에 접속하여, 호스트로 데이터를 전송하고 호스트로부터 데이터를 수신한다. 제어부(120)는 사용자에게 보여지는 파일 시스템을 플래시 메모리(130)의 물리적 주소와 명령에 대응되도록 변환하여, 플래시 메모리(130)가 데이터를 저장하도록 한다. 플래시 메모리(130)에 저장된 데이터를 액세스하는 경우에는 플래시 메모리의 물리적 주소를 논리적 파일 시스템으로 변환하여 사용자가 인식할 수 있는 형태로 보여준다. 플래시 메모리(130)는 비휘발성 메모리로써 전원이 공급되지 않아도 저장된 데이터는 삭제되지 않는다.

도 2는 본 발명의 바람직한 실시예에 따른 보안 데이터 저장 장치의 구성과, 데이터의 저장 경로를 도시한 도면이다.

보안 데이터 저장 장치는 USB 커넥터(210), 제어부(220), 플래시 메모리(230) 및 보안칩(240)을 포함하고, 바람직하게는 RF 송수신부(250)를 더 포함한다. USB 커넥터(210)는 호스트와 데이터를 주고받기 위한 물리적 인터페이스를 제공한다. 즉, USB로 정의된 버스에 접속하여, 호스트로 데이터를 전송하고 호스트로부터 데이터를 수신한다. 이 때 본 발명에 의한 데이터 저장 방법에 따르면, 호스트로부터 USB 커넥터(210)를 통해 수신한 데이터를 제어부(220)를 경유하여, 플래시 메모리(230)에 저장하거나 보안칩(240)에 포함된 메모리에 저장할 수도 있다. 보안칩(240)은 수신된 데이터에 대해 암호화를 수행하지 않고 그대로 저장하거나, 수신된 데이터에 대해 암호화를 수행하여 저장할 수 있다. 또는, 보안칩(240)에 내장된 암호화 알고리즘에 따라, 수신된 데이터를 암호화하여 플래시 메모리(230)에 저장할 수도 있다.

데이터의 전송 경로를 표시하면 일반적인 데이터 저장은 저장 경로 1(260)을 따라 이루어지며, 보안칩(240)에로의 저장은 저장 경로 2(270)를 따라 이루어지며, 보안칩(240)에서 데이터의 암호화를 수행하여 플래시 메모리(230)로 저장하는 것은 저장 경로 3(280)을 따라 이루어진다. 보다 상세한 동작 설명은 후술한다.

제어부(220)는 USB 커넥터(210)로부터 수신한 데이터를 플래시 메모리(230)로 전달하거나 보안칩(240)으로 전달하고, 보안칩(240)에서 암호화한 데이터를 다시 받아 플래시 메모리(230)로 전달한다. 이를 위해, 제어부(220)는 사용자에게 보여지는 파일 시스템을 플래시 메모리(230)의 물리적 주소와 명령에 대응되도록 변환하여, 플래시 메모리(230)가 데이터를 저장하도록 한다. 플래시 메모리(230)에 저장된 데이터를 액세스하는 경우에도 물리적 주소를 논리적 파일 시스템으로 변환하여 사용자가 인식할 수 있는 형태로 보여준다.

RF 송수신부(250)는 RF 통신을 통해 타 장치와 데이터를 주고받는다. 예를 들어, 비접촉식으로 교통카드나 전자화폐 기능을 수행하기 위해 보안칩(240)에 기록되어 있는 교통카드나 전자화폐 관련 데이터를 RF 리더 등을 통해 전달한다. 이 경우에 보안칩(240)은 RF 송수신부(250)로부터 전원을 인가 받아 동작한다.

이제 호스트로부터의 데이터를 저장하는 것을, 데이터의 전송 경로에 따라 상세히 설명한다. 저장 경로 1(260)에 따라 데이터를 저장하는 것은 일반적인 USB 플래시 메모리에 데이터를 저장하는 과정과 동일하게 이루어진다. 이러한 과정은 도 1을 참조하여 전술한 바와 같다.

저장 경로 2(270)에 따라 데이터를 저장하는 것은, 데이터 저장을 수행하는 애플리케이션 프로그램이 호스트에서 실행되면, 보안칩(240)으로 인증을 요청하고, 보안칩(240)에서의 사용자 인증이 성공하면, 호스트의 애플리케이션 프로그램이 저장하고자 하는 데이터를 전송한다. 보안칩(240)은 수신된 데이터를 그대로 저장하거나, 암호화하여 저장한다. 한편, 암호화 과정에 시간이 많이 소요되므로 수신된 데이터의 일부에 대해서만 암호화를 수행하여 저장할 수도 있다. 일부 데이터는 예를 들어, 수신된 데이터의 4 바이트의 헤더가 될 수 있다.

저장 경로 3(280)에 따라 데이터를 저장하는 과정을 설명하면 다음과 같다. 데이터 저장을 수행하는 애플리케이션 프로그램이 호스트에서 실행되면, 보안칩(240)으로 인증을 요청하고, 보안칩(240)에서의 사용자 인증이 성공하면, 호스트의 애플리케이션 프로그램이 저장하고자 하는 데이터를 전송한다. 보안칩(240)은 수신된 데이터를 암호화하여 제어부(220)를 거쳐 플래시 메모리(230)로 전송한다. 이 경우에도 마찬가지로 수신된 데이터의 일부에 대해서만 암호화를 수행하여 저장할 수도 있다. 한편, 데이터의 암호화를 보안칩(240)에서 수행하지 않고 호스트에 내장된 암호화 프로그램에 따라 미리 데이터를 암호화하여 전송하여, 수신된 암호화된 데이터를 플래시 메모리(230)에 저장할 수 있다. 암호화 프로그램은 애플리케이션 내에 포함될 수도 있다.

상술한 예에서 데이터의 암호화와 복호화의 예를 보다 상세하게 설명하면, 암호화의 수행은 보안칩의 비밀키에 의해 수행되고, 복호화는 호스트가 가지고 있는 공개키에 의해 수행될 수 있다. 사용될 수 있는 암호화 알고리즘에는 DES(Data Encryption Standard), RSA(Rivest-Shamir-Adleman) 알고리즘뿐만 아니라 일반적인 암호화 알고리즘이 모두 포함된다.

도 3은 도 2의 보안 데이터 저장 장치의 상세 구성도이다.

USB 커넥터(210)는 호스트, 예를 들어 PC의 USB 포트와 연결되어 데이터 통신을 수행한다. USB 제어부(220)는 USB 커넥터(210)와 연결되어 USB 커넥터(210)로부터 수신되는 정보를 분석하여, 플래시 메모리(230)를 액세스하기 위한 메모리 선택신호, 어드레스 및 제어 신호를 생성한다. 또한 데이터를 보안칩(240)의 보안 데이터 저장부(330)에 저장하는 경우에는, 보안칩 제어부(310)와 데이터 통신을 수행한다. 플래시 메모리(230)는 암호화가 필요없는 일반 데이터를 저장하거나, 보안칩(240)의 암호화 처리부(320)에 의해 암호화된 보안 데이터를 저장한다.

보안칩(240)은, 보다 상세하게는 보안칩 제어부(310), 암호화 처리부(320), 보안 데이터 저장부(330) 및 RF 인터페이스부(340)를 포함한다. 보안칩 제어부(310)는 사용자의 보안 데이터 저장 명령에 따라, USB 제어부(220)로부터 수신된 데이터를 암호화 과정없이 보안 데이터 저장부(330)에 저장하도록 제어하거나, 암호화 신호를 암호화 처리부(320)에 전달하여 데이터를 암호화하도록 한다. 또한, 보안 데이터 저장부(330)에 저장된 데이터를 RF 인터페이스부(340)를 통해 RF 송수신부(250)로 전달하도록 한다.

암호화 처리부(320)는 소정의 암호화 알고리즘에 따라, 수신된 데이터를 암호화하거나, 암호화된 데이터를 복호화하여 출력한다. 보안 데이터 저장부(330)는 암호화되지 않은 데이터를 USB 제어부(220)와 보안칩 제어부(310)를 통해 전달받아 저장하거나, 암호화 처리부(320)에 의해 암호화된 데이터를 보안칩 제어부(310)를 통해 전달받아 저장한다. 보안 데이터 저장부(330)에 저장되는 데이터의 일예로는 공인 인증서나 계좌 정보,신용 카드 정보 등을 들 수 있다. RF 인터페이스부(340)는 교통 카드나 전자 지갑 등의 기능을 위해서, 외부의 RF 리더로부터 명령에 따라, 보안 데이터 저장부(330)에 저장된 데이터를 RF 송수신부(250)를 통해 전송한다.

도 4는 본 발명의 바람직한 실시예에 따른 데이터 저장 방법의 흐름도이다.

호스트의 애플리케이션 프로그램이 수행되면 사용자 인터페이스가 제공되고, 이를 통해 사용자로부터 저장하고자 하는 데이터와 이를 암호화하여 저장할 것인가의 여부 및 어느 영역에 저장할 것인가 하는 암호화 여부 정보를 입력받는다(S410). 데이터를 암호화하여 저장할 것인가의 여부를 판단하여(S420), 저장하고자 하는 데이터가 중요한 데이터로써 암호화를 수행하여 저장하고자 하는 명령을 입력받으면 보안 알고리즘을 수행하여, 저장하고자 하는 데이터를 암호화한다(S430). 암호화를 수행하고자 하지 않는 경우에는 암호화 과정은 생략된다. 다음으로 이렇게 암호화된 데이터 또는 일반 데이터를 보안 영역에 저장할 것인가의 여부 정보를 판단하여(S440), 그 결과에 따라 데이터를 보안 영역에 저장하거나(S450), 일반 영역에 저장한다(S460). 보안 영역은 보안칩 내부의 메모리가 되며, 일반 영역은 플래시 메모리가 된다.

도 5는 본 발명의 바람직한 실시예에 따른 데이터 독출 방법의 흐름도이다.

애플리케이션 프로그램이 실행되면 이에 따른 사용자 인터페이스를 통해, 독출할 데이터를 선택받는다(S510). 예를 들어, 독출할 파일 이름 등의 정보가 될 수 있다. 그리고, 독출한 데이터가 저장되어 있는 저장영역을 확인한다(S520), 독출할 데이터가 보안 영역에 저장되어 있으면 인증을 수행하고(S530), 인증에 성공하면 보안 영역에 저장되어 있는 데이터를 읽는다(S540). 한편, 독출할 데이터가 일반 영역에 저장되어 있는 데이터이면 일반 영역에서 데이터를 읽는다(S550). 읽어낸 보안 영역 또는 일반 영역에 저장되어 있는 데이터가 암호화되어 있는 데이터인지 판단하여(S560), 암호화되어 있는 데이터이면 복호화를 수행한다(S570). 한편, S530 단계에서 인증을 수행하는데 있어서, 일정 횟수 이상 예를 들어 3회 이상 인증에 실패하면 더 이상 데이터를 읽을 수 없도록 락을 걸 수 있다.

한편, 전술한 보안 데이터 저장 방법은 컴퓨터 프로그램으로 작성 가능하다. 상기 프로그램을 구성하는 코드들 및 코드 세그먼트들은 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 상기 프로그램은 컴퓨터가 읽을 수 있는 정보저장매체(computer readable media)에 저장되고, 컴퓨터에 의하여 읽혀지고 실행됨으로써 보안 데이터 저장 방법을 구현한다. 상기 정보저장매체는 자기 기록매체, 광 기록매체, 및 캐리어 웨이브 매체를 포함한다.

이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

발명의 효과

전술한 바와 같이 본 발명에 따르면, 공인 인증서, 개인별 계좌 번호나 신용 카드 데이터, 중요한 아이디 및 패스 워드 데이터, 기타 사용자 인증을 요구하는 데이터를 보다 안전하게 저장할 수 있으며, RF 송수신부를 더 구비하여 전자 지갑 또는 교통 카드의 기능을 함께 수행할 수 있다.

도면의 간단한 설명

도 1은 USB 인터페이스를 갖는 플래시 저장장치의 구성도,

도 2는 본 발명의 바람직한 실시예에 따른 보안 데이터 저장 장치의 구성과, 데이터의 저장 경로를 도시한 도면,

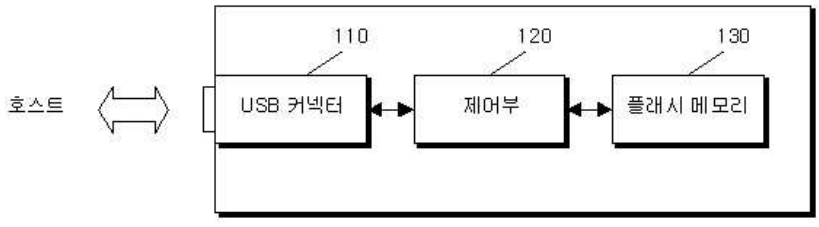
도 3은 도 2의 보안 데이터 저장 장치의 상세 구성도,

도 4는 본 발명의 바람직한 실시예에 따른 데이터 저장 방법의 흐름도,

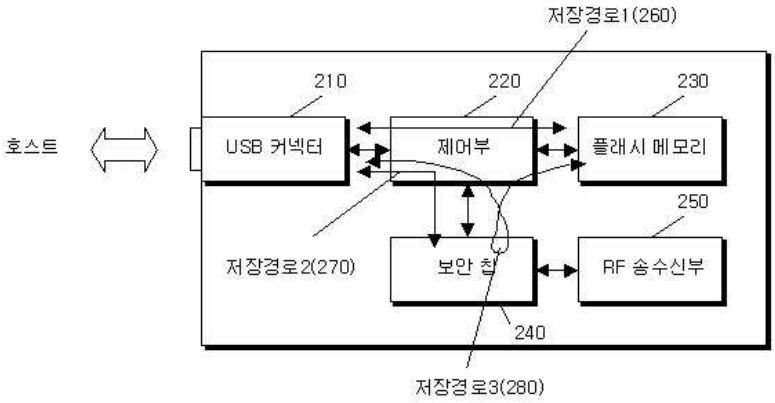
도 5는 본 발명의 바람직한 실시예에 따른 데이터 독출 방법의 흐름도이다.

도면

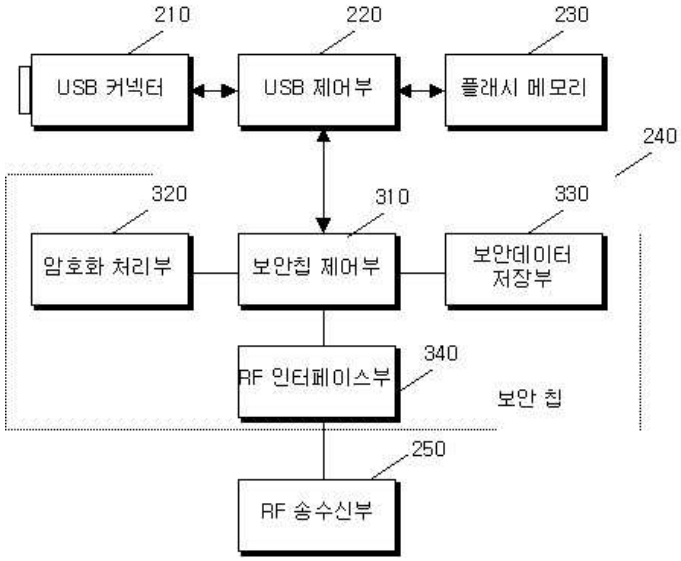
도면1



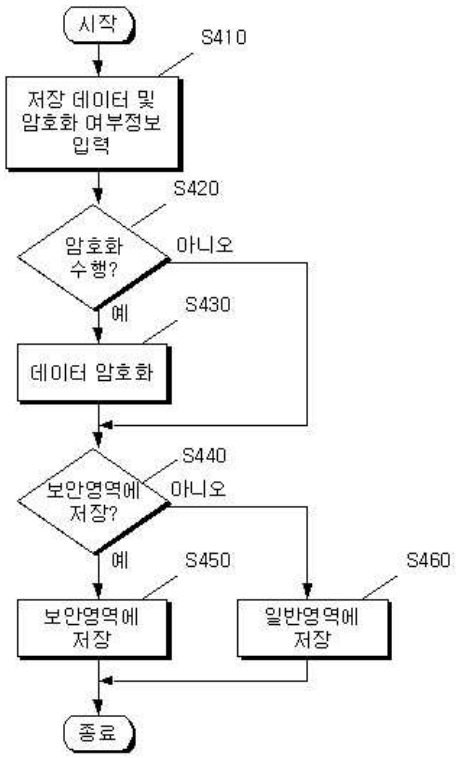
도면2


저장경로1(260)
210
220
230
호스트
USB 커넥터
제어부
플래시 메모리
250
저장경로2(270)
보안 칩
RF 송수신부
240
저장경로3(280)

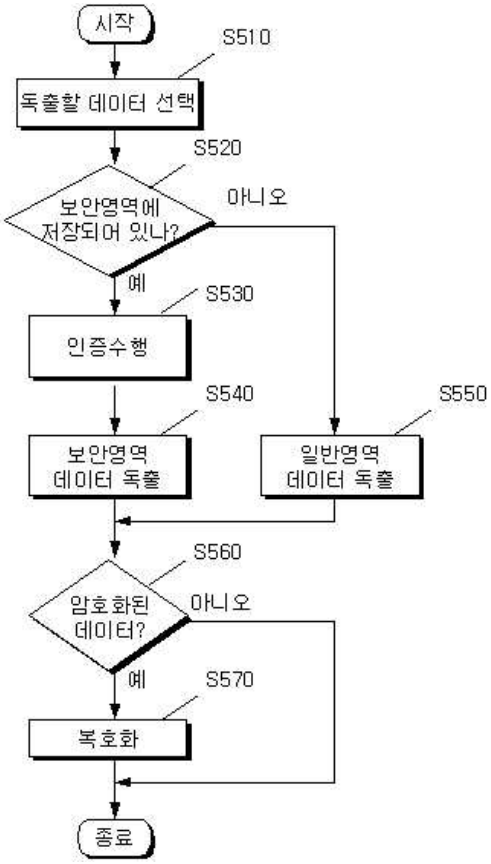
도면3


210
220
230
USB 커넥터
USB 제어부
플래시 메모리
240
320
310
330
암호화 처리부
보안칩 제어부
보안데이터 저장부
340
RF 인터페이스부
보안 칩
250
RF 송수신부

도면4


시작
S410
저장 데이터 및 암호화 여부정보 입력
S420
암호화 수행?
아니오
예
S430
데이터 암호화
S440
보안영역에 저장?
아니오
예
S450
S460
보안영역에 저장
일반영역에 저장
종료

도면5


시작
S510
독출할 데이터 선택
S520
보안영역에 저장되어 있나?
아니오
예
S530
인증수행
S540
S550
보안영역 데이터 독출
일반영역 데이터 독출
S560
암호화된 데이터?
아니오
예
S570
복호화
종료