(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년10월22일
(11) 등록번호 10-1562651
(24) 등록일자 2015년10월16일

(51) 국제특허분류(Int. Cl.)
G06F 21/78 (2013.01) *G06F 1/00* (2006.01)
G06F 21/31 (2013.01) *G06F 21/60* (2013.01)
(21) 출원번호 10-2013-0167671
(22) 출원일자 2013년12월30일
심사청구일자 2013년12월30일
(65) 공개번호 10-2015-0078373
(43) 공개일자 2015년07월08일
(56) 선행기술조사문헌
JP2011034577 A*
KR1020090050266 A*
KR1020050103448 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
대전대학교 산학협력단
대전광역시 동구 대학로 62 (용운동, 대전대학교)
(72) 발명자
김유성
인천 계양구 아나지로 332, 101동 804호 (작전동, 우림카이저팰리스1단지)
박기웅
대전 유성구 상대남로 26, 914동 102호 (상대동, 트리풀시티아파트)
(74) 대리인
심충섭

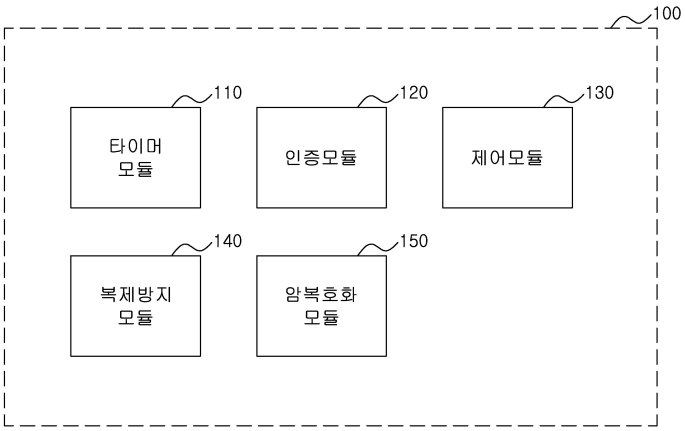
전체 청구항 수 : 총 12 항 심사관 : 구본재

(54) 발명의 명칭 **이동식 저장매체 보안시스템 및 그 제공방법**

(57) 요 약

이동식 저장매체 보안시스템 및 그 제공방법이 개시된다. 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템은, 이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하기 위한 타이머 모듈, 상기 이동식 저장매체에 설정된 인증정보를 이용하여 사용자를 인증하기 위한 인증모듈, 및 상기 타이머 모듈에 의해 카운트되는 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 상기 인증모듈에 의해 상기 사용자가 인증되지 않을 경우, 상기 이동에 저장된 소정의 데이터를 삭제하기 위한 제어모듈을 포함한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하기 위한 타이머 모듈;

상기 이동식 저장매체에 설정된 인증정보를 이용하여 사용자를 인증하기 위한 인증모듈; 및

상기 타이머 모듈에 의해 카운트되는 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 상기 인증모듈에 의해 상기 사용자가 인증되지 않을 경우, 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하되,

상기 데이터를 포함하며 상기 이동식 저장매체에 설정된 소정의 보안영역에 저장된 정보를 삭제하는 제어모듈을 포함하는 이동식 저장매체 보안시스템.

청구항 2

제1항에 있어서, 상기 이동식 저장매체 보안시스템은,

상기 인증모듈에 의해 인증이 성공하기 전까지는 상기 데이터를 복제하지 못하도록 제어하는 복제방지 모듈을 더 포함하는 이동식 저장매체 보안시스템.

청구항 3

삭제

청구항 4

제1항에 있어서, 상기 제어모듈은,

상기 보안영역에 더미 데이터를 기록하는 프로세스를 복수 회 반복하여 상기 보안영역에 저장된 정보를 삭제하는 것을 특징으로 하는 이동식 저장매체 보안시스템

청구항 5

이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하기 위한 타이머 모듈;

상기 이동식 저장매체에 설정된 인증정보를 이용하여 사용자를 인증하기 위한 인증모듈; 및

상기 타이머 모듈에 의해 카운트되는 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 상기 인증모듈에 의해 상기 사용자가 인증되지 않을 경우, 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하기 위한 제어모듈을 포함하며,

상기 타이머 모듈은,

상기 인증모듈에 의해 인증이 되기 전에 상기 이동식 저장매체가 상기 호스트에서 분리되는 경우, 분리된 시점에 상응하는 상기 경과시간을 저장하며,

상기 이동식 저장매체가 재연결된 경우 상기 경과시간부터 카운트를 연속하여 수행하는 것을 특징으로 하는 이동식 저장매체 보안시스템.

청구항 6

제1항에 있어서, 상기 이동식 저장매체 보안시스템은,

상기 데이터를 암호화하거나 복호화하기 위한 암복호화 모듈을 더 포함하는 이동식 저장매체 보안시스템.

청구항 7

이동식 저장매체에 있어서,

소프트웨어가 저장되는 저장장치; 및

호스트와 연결되는 인터페이스를 포함하며,

상기 인터페이스를 통해 상기 이동식 저장매체가 호스트에 연결되면 상기 소프트웨어가 상기 호스트에서 실행되고,

상기 소프트웨어에 의해 구동되는 상기 호스트에 의해,

상기 이동식 저장매체가 상기 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하고,

카운트 되는 상기 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 사용자가 인증되지 않을 경우, 상기 이동식 저장매체에 저장된 소정의 데이터가 삭제되되,

상기 데이터를 포함하며 상기 이동식 저장매체에 설정된 소정의 보안영역에 저장된 정보가 삭제되는 것을 특징으로 하는 이동식 저장매체.

청구항 8

이동식 저장매체 보안시스템이 이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하는 단계;

상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 설정된 인증정보를 이용하여 사용자를 인증하는 단계; 및

카운트 되는 상기 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 상기 사용자가 인증되지 않을 경우, 상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하는 단계를 포함하며,

상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하는 단계는,

상기 이동식 저장매체 보안시스템이 상기 데이터를 포함하며 상기 이동식 저장매체에 설정된 소정의 보안영역에 저장된 정보를 삭제하는 단계를 포함하는 이동식 저장매체 보안시스템 제공방법.

청구항 9

제8항에 있어서, 상기 이동식 저장매체 보안시스템 제공방법은,

상기 이동식 저장매체 보안시스템이 상기 사용자의 인증이 성공하기 전까지는 상기 데이터를 복제하지 못하도록 제어하는 단계를 더 포함하는 이동식 저장매체 보안시스템 제공방법.

청구항 10

삭제

청구항 11

제8항에 있어서, 상기 이동식 저장매체 보안시스템이 상기 데이터를 포함하며 상기 이동식 저장매체에 설정된 소정의 보안영역에 저장된 정보를 삭제하는 단계는,

상기 이동식 저장매체 보안시스템이 상기 보안영역에 더미 데이터를 기록하는 프로세스를 복수 회 반복하여 상기 보안영역에 저장된 정보를 삭제하는 단계를 포함하는 이동식 저장매체 보안시스템 제공방법.

청구항 12

이동식 저장매체 보안시스템 제공방법에 있어서,

이동식 저장매체 보안시스템이 이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하는 단계;

상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 설정된 인증정보를 이용하여 사용자를 인증하는 단계; 및

카운트 되는 상기 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 상기 사용자가 인증되지 않을 경우, 상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하는 단계를 포함하며,

상기 이동식 저장매체 보안시스템 제공방법은,

상기 사용자가 인증되기 전에 상기 이동식 저장매체가 상기 호스트에서 분리되는 경우, 상기 이동식 저장매체 보안시스템이 분리된 시점에 상응하는 상기 경과시간을 저장하는 단계; 및

상기 이동식 저장매체가 재연결되는 경우, 상기 이동식 저장매체 보안시스템이 상기 경과시간부터 카운트를 연속하여 수행하는 단계를 더 포함하는 이동식 저장매체 보안시스템 제공방법.

청구항 13

제8항에 있어서, 상기 이동식 저장매체 보안시스템 제공방법은,

상기 이동식 저장매체 보안시스템이 상기 데이터를 암호화하거나 복호화하는 단계를 더 포함하는 이동식 저장매체 보안시스템 제공방법.

청구항 14

제8항 내지 제9항 또는 제11항 내지 제13항 중 어느 한 항에 기재된 방법을 수행하기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 이동식 저장매체 보안시스템 및 그 제공방법에 관한 것으로, 보다 상세하게는 이동식 저장매체(예컨대, USB 메모리 등)가 호스트(예컨대, 컴퓨터 등)에 연결되면 미리 설정된 시간 내에 사용자 인증이 수행될 수 있도록 하고, 상기 설정된 시간 내에 사용자 인증이 수행되지 않는 경우 상기 이동식 저장매체에 저장된 데이터를 삭제하도록 하여 사용자가 상기 이동식 저장매체를 분실하거나 도난당하는 경우에도 부당 사용자가 상기 이동식 저장매체에 저장된 데이터를 사용할 수 없도록 하는 시스템 및 그 제공방법에 관한 것이다.

배 경 기 술

[0002] 휴대가 용이하고 설치 및 사용이 간편한 이동식 저장매체(예컨대, USB 메모리 등)가 널리 사용되고 있다. 이러한 이동식 저장매체는 별도의 전원이나 별도의 하드웨어 드라이브를 구비하지 않고서도 간편하게 구동이 가능하여 많은 사용자들에 의해 사용이 확산 되고 있다.

[0003] 그러나 이러한 이동식 저장매체의 사용이 확산 되면서, 사용자들이 상기 이동식 저장매체에 중요한 데이터를 저

장하고 다니는 경우가 많아지는데, 이동성이 높은 이동식 저장매체의 특성상 분실이나 도난의 위험이 커 이동식 저장매체에 대한 보안문제가 크게 부각되고 있다.

[0004] 이러한 이동식 저장매체의 보안을 위한 기술적 사상이 한국공개특허(공개번호 특2003-0084037, "유에스비 메모리 장치의 보안 방법 및 이를 이용한 컴퓨터의 사용제한 방법", 이하 '종래기술')에 개시되어 있다.

[0005] 상기 종래기술은 USB 메모리 장치에 소정의 보안 프로그램과 상기 보안 프로그램에 대응하는 패스워드를 설정하여 저장하고, 상기 USB 메모리 장치가 컴퓨터에 연결되면 컴퓨터에서 상기 보안 프로그램을 로딩하여 상기 USB 메모리 장치에 대한 보안 기능에 의해 패스워드를 요구하고, 패스워드가 일치하지 않으면 상기 USB 메모리 장치에 대한 억세스를 제한하도록 하는 기술구성을 포함하고 있다.

[0006] 상기 종래기술은 보안 프로그램에 의해 미리 설정된 패스워드를 통해 정당한 사용자를 인증하도록 하고 있는데, 인증이 실패하는 경우에도 단순히 상기 USB 메모리 장치에 대한 억세스를 제한하는데 그쳐 악의적인 사용자에 의해 상기 USB 메모리 장치에 저장된 데이터를 사용하기 위한 다양한 시도가 가능해지는 문제점이 있다.

[0007] 따라서 상기 패스워드와 같은 소정의 인증정보를 이용해 이동식 저장매체의 정당한 사용자를 인증할 수 있게 하면서도, 일정 시간 내에 인증이 성공하지 못하면 상기 이동식 저장매체에 저장된 데이터를 삭제하도록 하여 악의적인 사용자가 상기 이동식 저장매체에 저장된 데이터를 사용하기 위한 시도를 원천적으로 억제할 수 있는 기술적 사상이 요구된다.

발명의 내용

해결하려는 과제

[0008] 따라서 본 발명이 이루고자 하는 기술적인 과제는 이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하고, 상기 경과시간이 미리 설정된 타임아웃시간에 도달하기 전에 사용자의 인증을 수행하지 못하면 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제할 수 있도록 하는 기술적 사상을 제공하는 것이다.

[0009] 또한, 상기 데이터를 삭제하는 경우 상기 데이터의 복구가 불가능하도록 하여, 악의적인 사용자가 추후 상기 데이터를 복구하여 상기 데이터를 사용할 수 있는 위험을 제거할 수 있는 기술적 사상을 제공하는 것이다.

[0010] 또한, 상기 사용자의 인증이 수행되지 않은 채(즉, 상기 경과시간이 카운트 되는 도중에) 상기 이동식 저장매체가 상기 호스트로부터 분리되면, 상기 이동식 저장매체가 상기 호스트에 재연결되는 경우 상기 이동식 저장매체가 상기 호스트로부터 분리된 시점에 상응하는 경과시간부터 연속해서 카운트 될 수 있도록 하여 악의적인 사용자가 반복적으로 인증을 시도하는 것을 방지할 수 있는 기술적 사상을 제공하는 것이다.

과제의 해결 수단

[0011] 상기 기술적 과제를 해결하기 위한 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템은, 이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하기 위한 타이머 모듈, 상기 이동식 저장매체에 설정된 인증정보를 이용하여 사용자를 인증하기 위한 인증모듈, 및 상기 타이머 모듈에 의해 카운트되는 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 상기 인증모듈에 의해 상기 사용자가 인증되지 않을 경우, 상기 이동에 저장된 소정의 데이터를 삭제하기 위한 제어모듈을 포함할 수 있다.

[0012] 또한, 상기 이동식 저장매체 보안시스템은, 상기 인증모듈에 의해 인증이 성공하기 전까지는 상기 데이터를 복제하지 못하도록 제어하는 복제방지 모듈을 더 포함할 수 있다.

[0013] 또한, 상기 제어모듈은, 상기 데이터를 포함하며 상기 이동식 저장매체에 설정된 소정의 보안영역에 저장된 정보를 삭제하는 것을 특징으로 할 수 있다.

[0014] 또한, 상기 제어모듈은, 상기 보안영역에 더미 데이터를 기록하는 프로세스를 복수 회 반복하여 상기 보안영역에 저장된 정보를 삭제하는 것을 특징으로 할 수 있다.

[0015] 또한, 상기 타이머 모듈은, 상기 인증모듈에 의해 인증이 되기 전에 상기 이동식 저장매체가 상기 호스트에서 분리되는 경우, 분리된 시점에 상응하는 상기 경과시간을 저장하며, 상기 이동식 저장매체가 재연결된 경우 상

기 경과시간부터 카운트를 연속하여 수행하는 것을 특징으로 할 수 있다.

[0016] 또한, 상기 이동식 저장매체 보안시스템은, 상기 데이터를 암호화하거나 복호화하기 위한 암복호화 모듈을 더 포함할 수 있다.

[0017] 상기 기술적 과제를 해결하기 위한 본 발명의 실시 예에 따른 이동식 저장매체는, 소프트웨어가 저장되는 저장장치, 및 호스트와 연결되는 인터페이스를 포함하며, 상기 인터페이스를 통해 상기 이동식 저장매체가 호스트에 연결되면 상기 소프트웨어가 상기 호스트에서 실행되고, 상기 소프트웨어에 의해 구동되는 상기 호스트에 의해, 상기 이동식 저장매체가 상기 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하고, 카운트 되는 상기 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 사용자가 인증되지 않을 경우, 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하는 것을 특징으로 할 수 있다.

[0018] 상기 기술적 과제를 해결하기 위한 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템 제공방법은, 이동식 저장매체 보안시스템이 이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하는 단계, 상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 설정된 인증정보를 이용하여 사용자를 인증하는 단계, 및 카운트 되는 상기 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 상기 사용자가 인증되지 않을 경우, 상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하는 단계를 포함할 수 있다.

[0019] 또한, 상기 이동식 저장매체 보안시스템 제공방법은, 상기 이동식 저장매체 보안시스템이 상기 사용자의 인증이 성공하기 전까지는 상기 데이터를 복제하지 못하도록 제어하는 단계를 더 포함할 수 있다.

[0020] 또한, 상기 이동식 저장매체 보안시스템이 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제하는 단계는, 상기 이동식 저장매체 보안시스템이 상기 데이터를 포함하며 상기 이동식 저장매체에 설정된 소정의 보안영역에 저장된 정보를 삭제하는 단계를 포함할 수 있다.

[0021] 또한, 상기 이동식 저장매체 보안시스템이 상기 데이터를 포함하며 상기 이동식 저장매체에 설정된 소정의 보안영역에 저장된 정보를 삭제하는 단계는, 상기 이동식 저장매체 보안시스템이 상기 보안영역에 더미 데이터를 기록하는 프로세스를 복수 회 반복하여 상기 보안영역에 저장된 정보를 삭제하는 단계를 포함할 수 있다.

[0022] 또한, 상기 이동식 저장매체 보안시스템 제공방법은, 상기 사용자가 인증되기 전에 상기 이동식 저장매체가 상기 호스트에서 분리되는 경우, 상기 이동식 저장매체 보안시스템이 분리된 시점에 상응하는 상기 경과시간을 저장하는 단계, 및 상기 이동식 저장매체가 재연결되는 경우, 상기 이동식 저장매체 보안시스템이 상기 경과시간부터 카운트를 연속하여 수행하는 단계를 더 포함할 수 있다.

[0023] 또한, 상기 이동식 저장매체 보안시스템 제공방법은, 상기 이동식 저장매체 보안시스템이 상기 데이터를 암호화하거나 복호화하는 단계를 더 포함할 수 있다.

[0024] 상기 이동식 저장매체 보안시스템 제공방법은 프로그램을 기록한 컴퓨터 판독 가능한 기록매체에 기록될 수 있다.

발명의 효과

[0025] 본 발명의 기술적 사상에 의하면, 이동식 저장매체가 호스트에 연결되면 소정의 기준시점으로부터의 경과시간을 카운트하고, 상기 경과시간이 미리 설정된 타임아웃시간에 도달하기 전에 사용자의 인증을 수행하지 못하면 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제할 수 있도록 하여, 정확한 인증정보를 알고 있는 정당한 사용자 외에는 상기 데이터를 사용할 수 없어 보안이 향상될 수 있는 효과가 있다.

[0026] 또한, 상기 데이터를 삭제하는 경우 상기 데이터의 복구가 불가능하도록 하여, 악의적인 사용자가 추후 상기 데이터를 복구하여 상기 데이터를 사용할 수 있는 위험을 제거할 수 있는 효과가 있다.

[0027] 또한, 상기 사용자의 인증이 수행되지 않은 채(즉, 상기 경과시간이 카운트 되는 도중에) 상기 이동식 저장매체가 상기 호스트로부터 분리되면, 상기 이동식 저장매체가 상기 호스트에 재연결되는 경우 상기 이동식 저장매체가 상기 호스트로부터 분리된 시점에 상응하는 경과시간부터 연속해서 카운트 될 수 있도록 하여 악의적인 사용자가 반복적으로 인증을 시도하는 것을 방지할 수 있어 보안성이 높아질 수 있는 효과가 있다.

도면의 간단한 설명

[0028] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 간단한 설명이 제공된다.

도 1은 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템의 개략적인 구성을 나타낸다.

도 2는 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템의 보안영역 또는 보안 데이터 설정의 일 예를 나타낸다.

도 3은 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템이 보안영역에 저장된 데이터를 삭제하는 방법의 일 예를 나타낸다.

도 4는 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템이 경과시간의 카운트를 수행하는 일 예를 나타낸다.

도 5는 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템 제공방법의 개략적인 흐름을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시 예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

[0030] 또한, 본 명세서에 있어서는 어느 하나의 구성요소가 다른 구성요소로 데이터를 '전송'하는 경우에는 상기 구성요소는 상기 다른 구성요소로 직접 상기 데이터를 전송할 수도 있고, 적어도 하나의 또 다른 구성요소를 통하여 상기 데이터를 상기 다른 구성요소로 전송할 수도 있는 것을 의미한다.

[0031] 반대로 어느 하나의 구성요소가 다른 구성요소로 데이터를 '직접 전송'하는 경우에는 상기 구성요소에서 다른 구성요소를 통하지 않고 상기 다른 구성요소로 상기 데이터가 전송되는 것을 의미한다.

[0032] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

[0033] 도 1은 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템의 개략적인 구성을 나타낸다.

[0034] 도 1을 참조하면, 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템(100)은 타이머 모듈(110), 인증모듈(120), 및 제어모듈(130)을 포함한다. 구현 예에 따라 상기 이동식 저장매체 보안시스템(100)은 복제방지 모듈(140), 및/또는 암복호화 모듈(150)을 더 포함할 수 있다.

[0035] 상기 이동식 저장매체 보안시스템(100)은 소정의 이동식 저장매체(예컨대, USB 메모리 등)에 설치되는 소프트웨어가 상기 이동식 저장매체가 연결되는 호스트의 하드웨어와 유기적으로 결합되어 구현될 수 있다.

[0036] 예컨대, 상기 이동식 저장매체 보안시스템(100)은, 상기 이동식 저장매체 보안시스템(100)을 구현하기 위한 소프트웨어가 상기 이동식 저장매체에 설치되고, 상기 이동식 저장매체가 소정의 호스트(예컨대, 컴퓨터, 랩탑 등의 데이터 프로세싱 장치)에 연결되는 경우 상기 소프트웨어가 실행되어 상기 호스트의 하드웨어와 유기적으로 결합됨으로써 구현될 수 있다. 즉, 상기 소프트웨어는 상기 이동식 저장매체가 상기 호스트에 연결되는 경우 자동으로 실행될 수 있도록 구현될 수 있다. 또한 상기 소프트웨어는 상기 이동식 저장매체의 시스템 영역에 설치되어 사용자가 임의로 삭제하거나 변경할 수 없도록 구현될 수 있다.

[0037] 또한, 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어의 리소스(resource)의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것은 아님은 본 발명의 기술분야의 평균적 전문가에게는 용이하게 추론될 수 있다.

[0038] 상기 타이머 모듈(110)은 상기 이동식 저장매체가 상기 호스트에 연결되면, 소정의 기준시점으로부터의 경과시간을 카운트할 수 있다. 상기 소정의 기준시점은 예컨대, 상기 이동식 저장매체가 상기 호스트에 연결된 시점 또는 상기 이동식 저장매체가 상기 호스트에 연결된 후 소정의 시점(예컨대, 상기 호스트에 의해 상기 이동식 저장매체가 인식된 시점, 또는 상기 소프트웨어가 상기 호스트에 로딩된 시점)을 의미할 수 있다.

[0039] 상기 인증모듈(120)은 상기 이동식 저장매체가 상기 호스트에 연결되면 사용자를 인증할 수 있다. 이를 위하여,

상기 이동식 저장매체에는 상기 사용자에 상응하는 소정의 인증정보(예컨대, 사용자 ID 및/또는 비밀번호)가 미리 설정되어 있을 수 있으며, 상기 인증모듈(120)은 상기 인증정보를 이용하여 상기 사용자를 인증할 수 있다.

[0040] 본 발명의 기술적 사상에 의하면, 상기 인증모듈(120)에 의해 수행되는 사용자의 인증은 상기 타이머 모듈(110)에 의해 카운트 되는 경과시간이 모두 경과 하기 전 즉, 미리 설정된 타임아웃시간에 도달하기 전에 수행되도록 구현될 수 있다.

[0041] 본 발명의 실시 예에 의하면, 상기 제어모듈(130)은 상기 타이머 모듈(110)에 의해 상기 경과시간이 카운트 되어 상기 타임아웃시간이 도래하기 전에 상기 인증모듈(120)에 의해 사용자의 인증이 수행되지 않을 경우, 상기 이동식 저장매체에 저장된 소정의 데이터를 삭제할 수 있다.

[0042] 상기 데이터는 상기 이동식 저장매체의 시스템 영역을 제외한 나머지 영역(즉, 사용자 영역)에 저장된 전체 데이터를 의미할 수도 있고, 상기 사용자 영역 중 미리 설정된 보안영역에 저장된 데이터 및/또는 상기 전체 데이터 중 보안 데이터로 설정된 데이터를 의미할 수도 있다. 물론, 구현 예에 따라서는 상기 시스템 영역 중에 일부가 상기 보안영역으로 설정될 수도 있다. 이러한 경우에는 상기 소프트웨어는 상기 보안영역 이외의 시스템 영역에 저장되는 것이 바람직하다.

[0043] 이하에서는 본 발명의 실시 예에 따른 보안영역은 상기 사용자 영역 중 적어도 일부로 설정되는 일 예를 설명하며, 이러한 일 예가 도 2에 도시된다.

[0044] 도 2는 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템의 보안영역 또는 보안 데이터 설정의 일 예를 나타낸다.

[0045] 도 2a를 참조하면, 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템(100)은 상기 이동식 저장매체의 저장영역 중 적어도 일부를 보안영역(10)으로 설정할 수 있다. 예를 들어, 도시된 바와 같이 상기 이동식 저장매체에서 상기 시스템 영역을 제외한 나머지 영역(즉, 사용자 영역(20)) 중 일부가 상기 보안영역(10)으로 설정될 수 있다. 이러한 경우 상기 제어모듈(130)은 상기 타이머 모듈(110)에 의해 카운트 되는 상기 경과시간이 상기 타임아웃시간에 도달하기 전에 상기 인증모듈(120)에 의해 사용자의 인증이 수행되지 않으면, 상기 보안영역(10)에 저장된 데이터를 삭제할 수 있다.

[0046] 또는, 상기 보안영역(10)은 상기 사용자 영역(20) 전체로 설정될 수도 있다. 이러한 경우에는 전술한 바와 같이 상기 타임아웃시간이 되기 전에 사용자의 인증이 수행되지 않는 경우 상기 시스템 영역을 제외한 상기 이동식 저장매체에 저장된 모든 데이터가 상기 제어모듈(130)에 의해 삭제될 수 있다.

[0047] 구현 예에 따라, 도 2b에 도시된 바와 같이 상기 이동식 저장매체 보안시스템(100)은 상기 이동식 저장매체의 저장영역을 구분하는 것이 아니라 상기 이동식 저장매체에 저장된 전체 데이터(21) 중 적어도 일부의 데이터를 보안 데이터(11)로 설정할 수도 있다. 이러한 경우, 상기 제어모듈(130)은 상기 타임아웃시간 전까지 상기 인증모듈(120)에 의해 상기 사용자의 인증이 수행되지 않으면 미리 설정된 상기 보안 데이터(11)를 삭제할 수도 있다.

[0048] 한편 상기 제어모듈(130)은 상기 인증모듈(120)에 의해 상기 사용자의 인증이 수행되기 전에는 상기 보안영역(10)에 접근하지 못하도록 제어할 수 있다. 즉, 상기 제어모듈(130)은 상기 인증모듈(120)에 의해 상기 사용자의 인증이 수행되기 전에는 사용자가 상기 보안영역(10)에 저장된 데이터를 확인할 수 없도록 제어할 수 있다. 예컨대, 상기 제어모듈(133)은 상기 인증모듈(120)에 의해 상기 사용자의 인증이 수행되기 전에는 상기 보안영역(10)이 상기 호스트에 의해 접근되지 않도록 할 수도 있다.

[0049] 구현 예에 따라서는 상기 제어모듈(130)은 상기 인증모듈(120)에 의해 상기 사용자의 인증이 수행되지 않으면 상기 이동식 저장매체 자체에 접근하지 못하도록 제어할 수도 있다. 예컨대, 상기 사용자가 사용자 인증을 수행하지 않으면 상기 이동식 저장매체에 저장된 데이터를 전혀 확인할 수 없도록 구현될 수도 있다.

[0050] 한편 상기 제어모듈(130)이 상기 보안영역(10)에 저장된 데이터를 삭제하는 방법은 다양하게 구현될 수 있다. 상기 제어모듈(130)은 상기 보안영역(10)에 저장된 데이터를 단순히 삭제하거나 상기 이동식 저장매체를 포맷(format)할 수도 있으나, 이러한 경우 삭제된 데이터의 복구가 가능할 수 있는 문제점이 있을 수 있다. 이처럼 삭제된 데이터의 복구가 가능하게 되면 상기 이동식 저장매체가 악의적인 사용자에 의해 사용될 경우 중요한 데이터의 보안에 큰 문제가 발생할 위험이 있다. 따라서 상기 제어모듈(130)은 상기 보안영역(10)에서 삭제된 데이터의 복구를 방지하기 위한 소정의 보안삭제(secure erase)를 수행할 수 있다. 이러한 일 예를 도 3을 통해 설명하도록 한다.

[0051] 도 3은 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템이 보안영역에 저장된 데이터를 삭제하는 방법의 일 예를 나타낸다.

[0052] 도 3을 참조하면, 상기 제어모듈(130)은 상기 보안영역(10)에 소정의 더미(dummy) 데이터를 기록하는 프로세스를 수행할 수 있다. 일반적으로 상기 보안삭제는 의미 없는 데이터인 상기 더미 데이터를 복수 회 반복적으로 저장매체에 기록하여 덮어씌우는 프로세스가 복수 회 수행되는 것을 의미할 수 있다. 이러한 상기 보안삭제의 방식으로는 예컨대 zero fill 방식, random fill 방식, DoD 5220.22-M 방식, 및/또는 Gutman 방식 등이 공지되어 있으며, 상기 제어모듈(130)은 구현 예에 따라 상기 보안삭제의 방식들 중 어느 하나의 방식으로 상기 보안영역(10)을 완전히 삭제할 수 있다. 예컨대, 상기 Gutman 방식은 최대 35회까지 저장매체의 소정의 영역에 더미 데이터를 반복적으로 기록(즉, 덮어씌우기)할 수 있어 상기 소정의 영역에 저장되어 있던 데이터의 복구가 불가능하도록 할 수 있다.

[0053] 다시 도 1을 참조하면, 상기 인증모듈(120)에 의해 상기 사용자의 인증이 수행되기 전에는 상기 이동식 저장매체에 저장된 데이터의 복제를 방지할 수 있도록 상기 이동식 저장매체 보안시스템(100)에 복제방지 모듈(140)이 더 포함될 수 있다.

[0054] 정당한 사용자가 아닌 다른 사용자가 상기 이동식 저장매체에 저장된 데이터를 사용하지 못하도록 하기 위해서는 상기 정당한 사용자가 인증을 수행하지 않으면 상기 이동식 저장매체에 저장된 데이터의 복제를 방지하는 것이 중요할 수 있다. 만약 상기 인증이 수행되기 전 즉, 전술한 바와 같이 상기 타이머 모듈(110)에 의해 상기 경과시간이 카운트 되는 중에 데이터의 복제가 가능하게 되면 사용자의 인증이나 상기 경과시간의 카운트가 아무런 효용성이 없어질 수 있으며, 따라서 본 발명의 기술적 사상에 의하면 상기 사용자의 인증이 수행되기 전에는 데이터의 복제를 방지할 수 있도록 할 수 있다.

[0055] 상기 복제방지 모듈(140)이 상기 이동식 저장매체에 저장된 데이터의 복제를 방지하는 방식은 다양하게 구현될 수 있다. 예를 들어, 상기 복제방지 모듈(140)은 상기 호스트에서 상기 이동식 저장매체 보안시스템(100)으로 요청되는 소정의 리퀘스트나 메시지 I/O 요청을 후킹(hooking)하는 방식으로 상기 데이터의 복제를 방지할 수 있다. 이를 통해 상기 이동식 저장매체에 저장된 파일들에 대한 드래그 앤 드롭 방지, 이메일 또는 메신저에 파일 첨부 방지, 카피 앤 페이스트(copy & paste) 방지 등이 상기 복제방지 모듈(140)에 의해 수행됨으로써 상기 데이터의 복제를 방지할 수 있다. 이러한 일 예외에도 다양한 방식으로 데이터의 복제를 방지할 수 있음은 물론이다.

[0056] 한편 본 발명의 기술적 사상에 따른 이동식 저장매체 보안시스템(100)이 설치된 이동식 저장매체를 습득한 부당 사용자가 상기 이동식 저장매체를 사용하고자 하는 경우, 상기 타이머 모듈(110)에 의해 카운트 되는 상기 경과시간이 상기 타임아웃시간에 도달하기 전(즉, 상기 보안영역(10)에 저장된 데이터가 삭제되기 전)에 상기 이동식 저장매체를 상기 호스트로부터 분리한 후 다시 재연결하면서 정당한 사용자의 인증정보를 알아내기 위한 시도가 행해질 수 있다. 따라서 본 발명은 이러한 부당 사용자의 시도를 방지하기 위한 기술적 사상을 제공할 수 있다. 이를 도 4를 통해 설명하도록 한다.

[0057] 도 4는 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템이 경과시간의 카운트를 수행하는 일 예를 나타낸다.

[0058] 도 4를 참조하면, 상기 이동식 저장매체 보안시스템(100)은 상기 이동식 저장매체가 상기 호스트(200)에 연결되는 경우, 인증을 위한 타임아웃시간이 예컨대 60초로 설정되어 있을 수 있다. 이때 상기 부당 사용자가 경과시간이 25초가 지났을 때(즉, 카운트 되는 시간이 35초 남았을 때) 상기 이동식 저장매체를 상기 호스트(200)로부터 분리할 수 있다. 이후 상기 부당 사용자가 상기 이동식 저장매체를 다시 상기 호스트(200)에 재연결하게 되면, 상기 타이머 모듈(110)은 상기 이동식 저장매체가 상기 호스트(200)로부터 분리된 시점에 상응하는 경과시간 즉, 35초가 남은 시점부터 연속하여 카운트를 수행할 수 있다.

[0059] 이를 위하여, 상기 타이머 모듈(110)은 일정 주기마다(예컨대, 1초 마다) 카운트 되는 상기 경과시간에 대한 정보를 상기 이동식 저장매체에 저장할 수 있다. 이에 따라 상기 인증모듈(120)에 의해 사용자의 인증이 수행되지 않은 채 상기 이동식 저장매체가 상기 호스트(200)로부터 분리되면, 상기 타이머 모듈(110)은 마지막으로 저장된 시점의 경과시간으로부터 카운트를 연속해서 수행할 수 있다.

[0060] 이와 같은 본 발명의 기술적 사상에 의하면 부당 사용자가 상기 이동식 저장매체를 사용하기 위한 시도를 최소한의 횟수로 줄일 수 있어 상기 이동식 저장매체에 저장된 데이터의 보안이 한층 높아질 수 있는 효과가 있다.

[0061] 한편, 상기 이동식 저장매체 보안시스템(100)은 상기 이동식 저장매체에 저장된 데이터의 보안 향상을 위해 상기 보안영역(10)에는 암호화된 데이터가 저장되도록 할 수 있으며, 상기 이동식 저장매체 보안시스템(100)은 이를 위하여 암복호화 모듈(150)을 더 포함할 수 있다.

[0062] 상기 암복호화 모듈(150)이 데이터를 암호화 또는 복호화하는 방식은 다양하게 구현될 수 있다. 예컨대, 상기 암복호화 모듈(150)은 대칭 암호 알고리즘, 비대칭 암호 알고리즘, 하이브리드 암호 알고리즘 등 다양한 방식의 암복호화 알고리즘을 이용하여 상기 데이터를 암호화 또는 복호화할 수 있다. 예를 들어 상기 암복호화 모듈(150)은 대칭 암호 알고리즘의 하나인 ARIA 해시 알고리즘을 이용하여 상기 데이터를 암호화 또는 복호화할 수 있다. 물론 이외에도 DES 알고리즘, 3DES 알고리즘, AES 알고리즘, IDEA 알고리즘, Rijndael 알고리즘, 또는 SEED 알고리즘 등의 다양한 대칭 암호 알고리즘이 사용될 수 있으며, 구현 예에 따라서는 RSA 알고리즘, ECC 알고리즘, DSA 알고리즘, ELGamal 알고리즘, 또는 Rabin 알고리즘과 같은 비대칭 암호 알고리즘이 사용될 수도 있다. 이러한 다양한 암호 알고리즘에 대해서는 이미 널리 공지된 사항이므로 본 명세서에서 상세한 설명은 생략하도록 한다.

[0063] 한편 본 발명의 실시 예에 따라, 본 발명의 기술적 사상을 구현하기 위한 이동식 저장매체가 제공될 수 있다. 본 발명의 실시 예에 따른 이동식 저장매체는 소프트웨어가 저장되는 저장장치, 및 상기 호스트와 연결되는 인터페이스를 포함할 수 있다.

[0064] 상기 이동식 저장매체는 상기 인터페이스를 통해 상기 이동식 저장매체가 호스트에 연결되면 상기 호스트에서 상기 소프트웨어가 실행될 수 있다. 그러면, 상기 소프트웨어에 의해 구동되는 상기 호스트에 의해, 상기 이동식 저장매체가 상기 호스트에 연결되는 경우 소정의 기준시점으로부터의 경과시간이 카운트 될 수 있다.

[0065] 이때 카운트 되는 상기 경과시간이 미리 설정된 타임아웃시간이 되기 전까지 사용자가 인증되지 않을 경우에는 전술한 바와 같이 상기 이동식 저장매체에 저장된 소정의 데이터가 삭제될 수 있다.

[0066] 도 5는 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템 제공방법의 개략적인 흐름을 나타낸다.

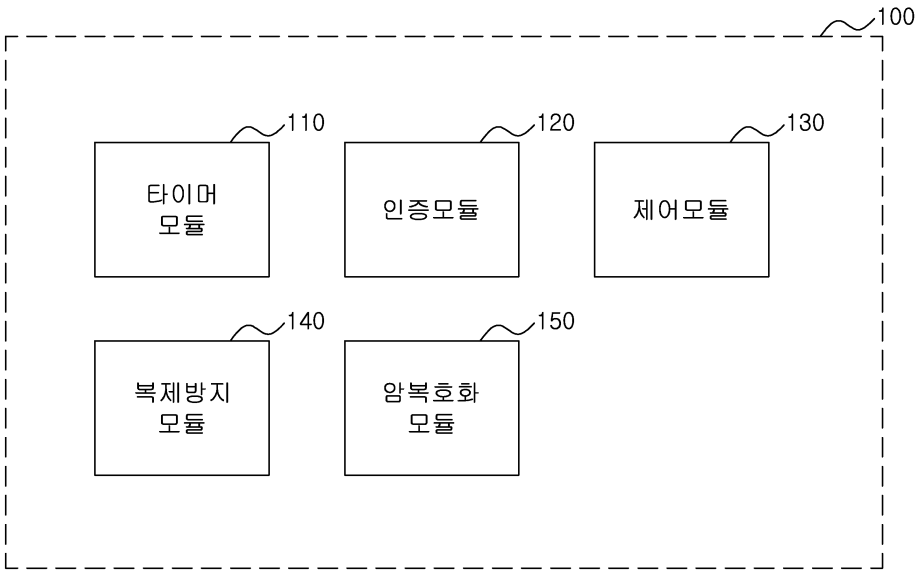
[0067] 도 5를 참조하면, 상기 이동식 저장매체 보안시스템(100)이 설치된 이동식 저장매체가 소정의 호스트에 연결(s100)될 수 있다. 이처럼 상기 이동식 저장매체가 상기 호스트에 연결되면, 상기 이동식 저장매체 보안시스템(100)은 소정의 시점(예컨대, 상기 이동식 저장매체가 상기 호스트에 연결된 시점 또는 상기 이동식 저장매체가 상기 호스트에 의해 인식된 시점)으로부터의 경과시간을 카운트(s110)할 수 있다. 상기 이동식 저장매체 보안시스템(100)에 의해 카운트 되는 상기 경과시간이 미리 설정된 타임아웃시간이 되기 전에 상기 이동식 저장매체 보안시스템(100)은 사용자의 인증을 수행(s120)할 수 있다. 이때 상기 타임아웃시간이 되기 전 상기 사용자의 인증이 성공하면, 상기 이동식 저장매체 보안시스템(100)은 소정의 보안영역(10)에 저장된 데이터를 상기 사용자가 사용할 수 있도록 제어(s130)할 수 있다. 반면 상기 타임아웃시간이 되기 전에 상기 사용자의 인증이 성공하지 못하는 경우, 상기 이동식 저장매체 보안시스템(100)은 상기 보안영역(10)에 저장된 데이터를 삭제(s140)함으로써 정당한 사용자가 아닌 다른 사용자가 상기 이동식 저장매체에 저장된 데이터를 사용할 수 없도록 할 수 있다.

[0068] 본 발명의 실시 예에 따른 이동식 저장매체 보안시스템 제공방법은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로써 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

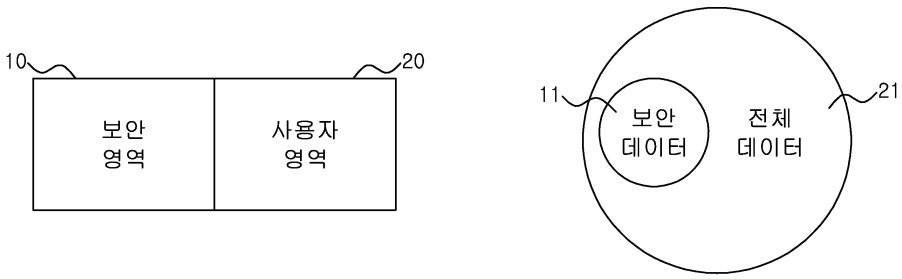
[0069] 본 발명은 도면에 도시된 일 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

도면1

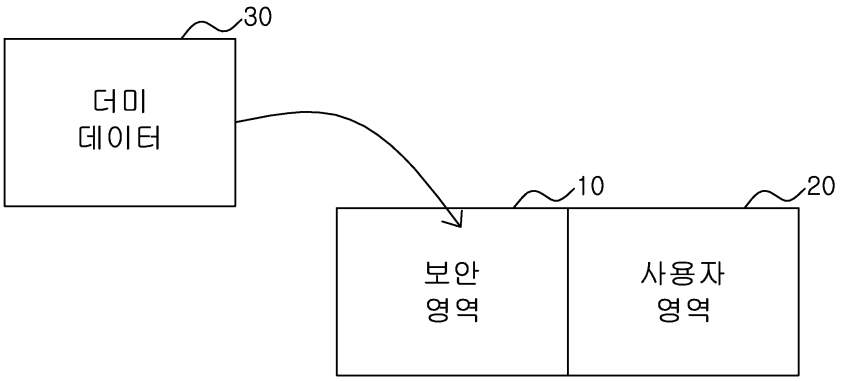

100
110
타이머
모듈
120
인증모듈
130
제어모듈
140
복제방지
모듈
150
암복호화
모듈

도면2

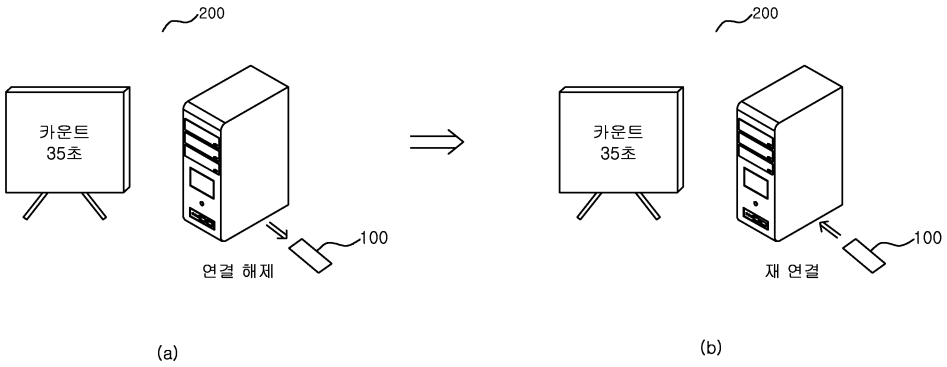

10
보안
영역
20
사용자
영역
11
보안
데이터
21
전체
데이터

(a) (b)

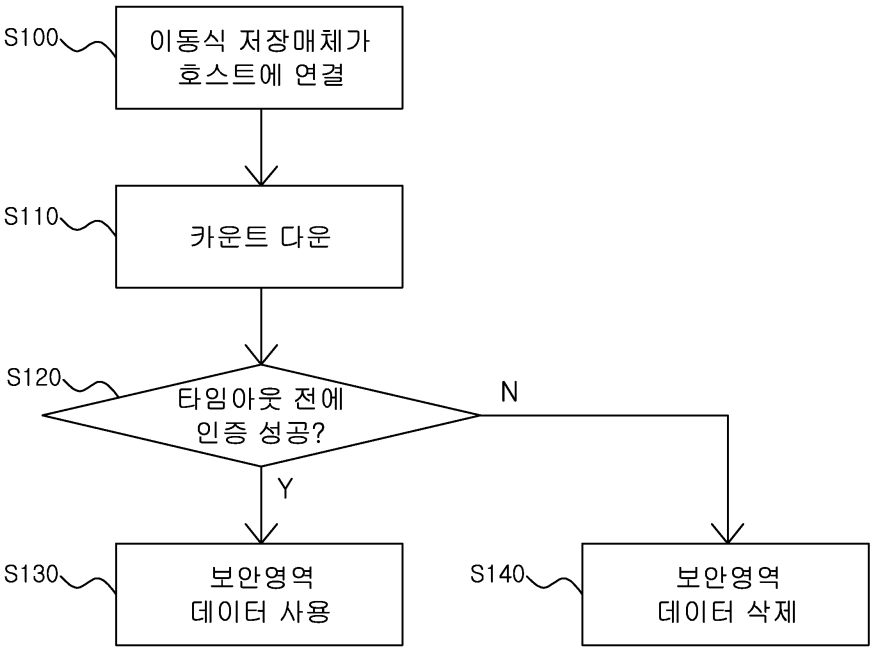
도면3


30
더미
데이터
10
20
보안
영역
사용자
영역

도면4


200
카운트
35초
100
연결 해제
(a)
200
카운트
35초
100
재 연결
(b)

도면5


S100
이동식 저장매체가
호스트에 연결
S110
카운트 다운
S120
타임아웃 전에
인증 성공?
N
Y
S130
보안영역
데이터 사용
S140
보안영역
데이터 삭제