(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년03월27일
(11) 등록번호 10-1720477
(24) 등록일자 2017년03월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/604 (2013.01)
H04L 63/101 (2013.01)
(21) 출원번호 10-2016-7012818(분할)
(22) 출원일자(국제) 2010년06월16일
심사청구일자 2016년05월16일
(85) 번역문제출일자 2016년05월16일
(65) 공개번호 10-2016-0062184
(43) 공개일자 2016년06월01일
(62) 원출원 특허 10-2011-7030199
원출원일자(국제) 2010년06월16일
심사청구일자 2015년05월20일
(86) 국제출원번호 PCT/US2010/038776
(87) 국제공개번호 WO 2010/148059
국제공개일자 2010년12월23일
(30) 우선권주장
12/486,738 2009년06월17일 미국(US)
(56) 선행기술조사문헌
JP2006120015 A
KR1020080084715 A

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
사도브스키 블라디미르
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
올라리그 섬퐁 폴
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인

전체 청구항 수 : 총 20 항 심사관 : 문남두

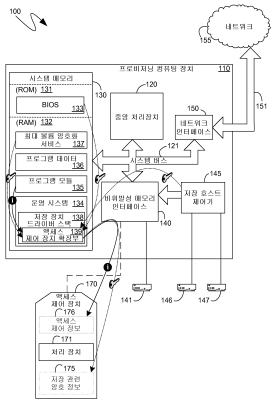
(54) 발명의 명칭 **저장 장치의 원격 액세스 제어**

(57) 요 약

액세스 제어 장치는 저장 장치에 통신 가능하게 결합될 수 있고, 그에 대한 액세스를 제어할 수 있다. 액세스 제어 장치는 허가받은 개체의 식별 정보 등과 같은 정보를 포함하여, 액세스 제어 장치가 연관된 저장 장치에 대한 액세스를 제공할지 여부를 독립적으로 결정하도록 할 수 있다. 이와 다르게, 액세스 제어 장치는 허가 컴퓨

(뒷면에 계속)

대 표 도 - 도1



팅 장치에 대한 안전한 접속을 형성하기 위한 정보를 포함할 수 있고, 액세스 제어 장치는 허가 컴퓨팅 장치의 결정을 구현할 수 있다. 액세스 제어 장치는 특정 펌웨어 명령어를 실행하여 데이터 저장 관련 요청에 대한 의미 있는 응답을 방지하도록 저장 장치에 명령함으로써 액세스를 제어할 수 있다. 액세스 제어 장치는 또한 데이터를 암호화 및 복호화하기 위해 저장 장치에 의해 이용되는 저장 관련 암호 정보를 포함할 수 있다. 이러한 경우에, 액세스 제어 장치는 저장 장치에 대해 저장 관련 암호 정보를 공개하지 않음으로써 액세스를 제어할 수 있다.

(52) CPC특허분류
H04L 9/32 (2013.01)
H04L 9/3271 (2013.01)
H04L 2209/34 (2013.01)
H04L 2209/80 (2013.01)

(72) 발명자
리오네티 크리스
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

해밀턴 제임스 로버트
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

명 세 서

청구범위

청구항 1

액세스 제어 장치를 프로비저닝(provisioning)하기 위한 방법으로서,

상기 액세스 제어 장치를 프로비저닝 컴퓨팅 장치에 통신 연결하는 단계 - 상기 액세스 제어 장치는 메모리 카드의 물리적 구성을 가짐 - 와,

상기 프로비저닝 컴퓨팅 장치를 이용하여, 상기 액세스 제어 장치 상에 액세스 제어 정보의 제1 집합을 저장하는 단계 - 상기 액세스 제어 정보의 제1 집합은 상기 액세스 제어 장치가, 상기 액세스 제어 장치에 통신 연결될 저장 장치로 하여금 상기 저장 장치 상에 저장된 데이터의 제1 집합으로 향하는 데이터 저장 관련 요청에 의미 있는 응답(meaningfully respond)을 하도록 허용하는지 여부를 식별함 - 와,

상기 프로비저닝 컴퓨팅 장치를 이용하여, 상기 액세스 제어 장치 상에 상기 액세스 제어 정보의 제1 집합과 상이한 상기 액세스 제어 정보의 제2 집합을 저장하는 단계 - 상기 액세스 제어 정보의 제2 집합은 상기 액세스 제어 장치가 상기 저장 장치로 하여금 상기 저장 장치 상에 마찬가지로 저장되며 상기 데이터의 제1 집합과는 상이한 데이터의 제2 집합으로 향하는 데이터 저장 관련 요청에 의미 있는 응답을 하도록 허용하는지 여부를 식별함 -

를 포함하고,

상기 액세스 제어 장치는 하나 이상의 프로세싱 유닛을 포함하되, 상기 하나 이상의 프로세싱 유닛은 상기 저장된 액세스 제어 정보의 제1 집합 또는 상기 저장된 액세스 제어 정보의 제2 집합에 적어도 일부 기초하여 상기 저장 장치가 상기 데이터 저장 관련 요청에 대해 의미 있는 응답을 하도록 허용할 것인지 여부를 결정하도록 구성된

액세스 제어 장치의 프로비저닝 방법.

청구항 2

제1항에 있어서,

상기 액세스 제어 정보의 제1 집합 및 상기 액세스 제어 정보의 제2 집합 중 적어도 하나는 상기 액세스 제어 장치 외부의 허가 컴퓨팅 장치(authorization computing device)와 보안 통신 터널을 설정하기 위한 액세스 제어 암호화 정보를 포함하는

액세스 제어 장치의 프로비저닝 방법.

청구항 3

제2항에 있어서,

상기 액세스 제어 장치는, 상기 보안 통신 터널을 통해 상기 허가 컴퓨팅 장치로부터 수신된 정보에 기초하여 데이터 저장 요청에 의미 있는 응답을 하도록 상기 저장 장치를 선택적으로 허용하는

액세스 제어 장치의 프로비저닝 방법.

청구항 4

제1항에 있어서,

상기 액세스 제어 정보의 제1 집합 및 상기 액세스 제어 정보의 제2 집합 중 적어도 하나는 하나 이상의 개체의

하나 이상의 식별자를 포함하며, 상기 하나 이상의 개체의 하나 이상의 식별자는 상기 액세스 제어 장치가 상기 저장 장치로 하여금 상기 하나 이상의 개체로부터의 데이터 저장 관련 요청에 의미 있는 응답을 할 수 있도록 하는

액세스 제어 장치의 프로비저닝 방법.

청구항 5

제4항에 있어서,

상기 액세스 제어 정보의 제1 집합 또는 상기 액세스 제어 정보의 제2 집합은 상기 하나 이상의 개체 중 적어도 일부와 연관된 인증 정보를 포함하는

액세스 제어 장치의 프로비저닝 방법.

청구항 6

제1항에 있어서,

상기 저장하는 단계들 이후, 상기 액세스 제어 장치 상에, 상기 저장 장치의 하드웨어 암호화 시스템에 의해 사용 가능한 저장 관련 암호화 정보를 저장하는 단계 - 상기 저장 관련 암호화 정보는 상기 저장 장치에 제공된 데이터를 저장하기 이전에 상기 제공된 데이터를 암호화하고 상기 저장 장치에 의해 저장된 암호화 데이터를 복호화하기 위해 상기 하드웨어 암호화 시스템에 의해 사용 가능하며, 상기 액세스 제어 정보는 상기 저장 장치의 상기 하드웨어 암호화 시스템에게 상기 저장 관련 암호화 정보에 선택적으로 액세스를 제공하도록 상기 액세스 제어 장치에 의해 사용 가능함 - 를 더 포함하는

액세스 제어 장치의 프로비저닝 방법.

청구항 7

제6항에 있어서,

상기 저장 관련 암호화 정보를 저장하는 단계 이후, 상기 액세스 제어 장치 상에, 다른 저장 장치의 하드웨어 암호화 시스템에 의해 사용 가능한 추가적인 저장 관련 암호화 정보를 저장하는 단계 - 상기 액세스 제어 정보는 상기 다른 저장 장치의 상기 하드웨어 암호화 시스템에게 상기 추가적인 저장 관련 암호화 정보에 선택적으로 액세스를 제공하도록 상기 액세스 제어 장치에 의해 사용 가능함 - 를 더 포함하는

액세스 제어 장치의 프로비저닝 방법.

청구항 8

제6항에 있어서,

상기 저장 관련 암호화 정보를 저장하는 단계 이후, 상기 액세스 제어 장치에게 상기 저장 관련 암호화 정보의 적어도 일부를 삭제하라고 지시하는 단계를 더 포함하는

액세스 제어 장치의 프로비저닝 방법.

청구항 9

제1항에 있어서,

상기 액세스 제어 장치는 상기 저장 장치의 일부인 물리적 수용기에 연결 가능하고 분리 가능한 물리적 커넥터를 포함하고, 상기 물리적 커넥터는 상기 데이터 저장 관련 요청을 저장 장치에 발행하는 호스트 컴퓨팅 장치와

상기 저장 장치 사이의 물리적 연결에 독립적인

액세스 제어 장치의 프로비저닝 방법.

청구항 10

제1항에 있어서,

상기 저장하는 단계들 이후,

상기 데이터 저장 관련 요청을 상기 저장 장치에 발행하는 호스트 컴퓨팅 장치를 상기 저장 장치에 통신 연결하는 단계와,

상기 호스트 컴퓨팅 장치에서, 상기 액세스 제어 장치가 상기 저장 장치에 통신 연결되었다는 표시를 상기 저장 장치로부터 수신하는 단계와,

상기 저장 장치를 통해 상기 호스트 컴퓨팅 장치와 상기 액세스 제어 장치 사이의 통신 연결을 수립하는 단계와,

상기 호스트 컴퓨팅 장치로부터 상기 액세스 제어 장치로 식별 정보를 제공하는 단계와,

상기 호스트 컴퓨팅 장치에서, 상기 액세스 제어 장치가 상기 저장 장치로 하여금 상기 저장 장치로 향하는 상기 데이터 저장 관련 요청들에 대해 의미 있는 응답을 하도록 허용한 경우, 상기 저장 장치로 향하는 상기 데이터 저장 관련 요청들에 대해 의미 있는 응답을 수신하는 단계

를 더 포함하고,

상기 액세스 제어 장치의 상기 하나 이상의 프로세싱 유닛들은 상기 제공된 식별 정보에 적어도 일부 기초하여, 상기 의미 있는 응답을 상기 저장 장치가 제공하는 것을 허용할지 여부를 결정하도록 더 구성되는

액세스 제어 장치의 프로비저닝 방법.

청구항 11

저장 장치에 저장된 데이터에 액세스하는 방법으로서,

상기 저장 장치를 상기 저장 장치에 데이터 저장 관련 요청들을 발행하는 호스트 컴퓨팅 장치로 통신 연결하는 단계와,

상기 호스트 컴퓨팅 장치에서, 메모리 카드의 물리적 구성을 가지는 액세스 제어 장치가 상기 저장 장치에 통신 연결되었다는 표시를 상기 저장 장치로부터 수신하는 단계와,

상기 저장 장치를 통해 상기 호스트 컴퓨팅 장치와 상기 액세스 제어 장치 사이의 통신 연결을 수립하는 단계와,

상기 호스트 컴퓨팅 장치로부터 상기 액세스 제어 장치로 식별 정보를 제공하는 단계와,

상기 호스트 컴퓨팅 장치에서, 상기 액세스 제어 장치가 상기 저장 장치로 하여금 상기 저장 장치로 향하는 상기 데이터 저장 관련 요청들에 대해 의미 있는 응답을 하도록 허용한 경우, 상기 저장 장치로 향하는 상기 데이터 저장 관련 요청들에 대해 의미 있는 응답을 수신하는 단계

를 포함하고,

상기 액세스 제어 장치의 하나 이상의 프로세싱 유닛들은 상기 제공된 식별 정보에 적어도 일부 기초하여, 의미 있는 응답을 상기 저장 장치가 제공하는 것을 허용할지 여부를 결정하도록 구성되는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 12

제11항에 있어서,

상기 저장 장치는 하드웨어 암호화 시스템을 더 포함하고, 상기 액세스 제어 장치는 저장 관련 암호화 정보를 포함하고, 상기 데이터 저장 관련 요청에 대한 의미 있는 응답을 수신하는 것은 상기 액세스 제어 장치가 상기 저장 장치의 상기 하드웨어 암호화 시스템에게 상기 저장 관련 암호화 정보로의 액세스를 제공하는 것 이후에 수행되는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 13

제11항에 있어서,

상기 식별 정보를 제공하는 단계 이전에, 상기 호스트 컴퓨팅 장치에서, 상기 액세스 제어 장치로부터의 인증 요구(challenge)를 수신하는 단계를 더 포함하고,

상기 액세스 제어 장치에 상기 식별 정보를 제공하는 단계는, 상기 인증 요구에 응답하여 인증을 상기 액세스 제어 장치에 제공하는 단계를 포함하는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 14

제11항에 있어서,

상기 의미 있는 응답을 수신하는 단계 이전에,

상기 호스트 컴퓨팅 장치에서, 상기 액세스 제어 장치로부터 상기 액세스 제어 장치 외부의 인증 컴퓨팅 장치에 제공될 제1 정보를 수신하는 단계와,

상기 호스트 컴퓨팅 장치로부터, 상기 인증 컴퓨팅 장치와 통신 연결을 수립하는 단계와,

상기 호스트 컴퓨팅 장치로부터, 상기 인증 컴퓨팅 장치로 상기 제1 정보를 제공하는 단계와,

상기 호스트 컴퓨팅 장치에서, 상기 인증 컴퓨팅 장치로부터 상기 액세스 제어 장치에 제공될 제2 정보를 수신하는 단계와,

상기 호스트 컴퓨팅 장치로부터 상기 액세스 제어 장치로 상기 제2 정보를 제공하는 단계

를 더 포함하고,

상기 액세스 제어 장치는 상기 제공된 제2 정보에 더 기초하여 상기 저장 장치가 의미 있는 응답을 제공할지 여부를 결정하도록 하는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 15

제14항에 있어서,

상기 인증 컴퓨팅 장치와 통신 연결을 수립하는 단계 이전에, 상기 호스트 컴퓨팅 장치로부터 네트워크로 통신 연결을 수립하는 단계 및 상기 네트워크로의 통신 연결의 수립의 일부로서 허가 컴퓨팅 장치의 네트워크 어드레스를 수신하는 단계를 더 포함하고, 상기 인증 컴퓨팅 장치와 통신 연결을 수립하는 단계는 상기 호스트 컴퓨팅 장치로부터 상기 허가 컴퓨팅 장치의 상기 수신된 네트워크 어드레스를 사용하여 상기 인증 컴퓨팅 장치와 네트워크 통신 연결을 수립하는 단계를 포함하는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 16

제14항에 있어서,

상기 인증 컴퓨팅 장치와 통신 연결을 수립하는 단계 이전에, 상기 호스트 컴퓨팅 장치 상에서, 상기 인증 컴퓨팅 장치로 동작하는 가상 프로세스를 구현하는 단계를 더 포함하고, 상기 인증 컴퓨팅 장치와 통신 연결을 수립하는 단계는 상기 가상 프로세스와 통신 연결을 수립하는 단계를 포함하는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 17

제11항에 있어서,

상기 호스트 컴퓨팅 장치 상에서, 상기 액세스 제어 장치가 상기 저장 장치에 통신 연결되었다는 표시를 상기 저장 장치로부터 수신하는 것에 응답하여, 저장 장치 드라이버 스택(storage device driver stack)에 의해 액세스 제어 장치 확장부(access control extension)를 로딩하는 단계를 더 포함하고, 상기 액세스 제어 장치 확장부는 상기 액세스 제어 장치와 통신 연결을 수립하고 상기 액세스 제어 장치에 상기 식별 정보를 제공하기 위한 컴퓨팅 실행 가능한 명령어들을 포함하는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 18

제17항에 있어서,

상기 액세스 제어 장치 확장부를 로딩하는 단계 이후에, 상기 액세스 제어 장치 및 상기 저장 장치 사이에 보안 통신 연결을 수립하는 단계를 더 포함하고, 상기 액세스 제어 장치 및 상기 저장 장치 각각은 상기 호스트 컴퓨팅 장치에 독립적으로 통신 연결되고, 상기 액세스 제어 장치 확장부는 상기 액세스 제어 장치와 상기 저장 장치 사이에 상기 보안 통신 연결을 수립하기 위한 컴퓨터 실행 가능한 명령어들을 더 포함하는

저장 장치에 저장된 데이터로의 액세스 방법.

청구항 19

시스템으로서,

메모리 카드의 물리적 구성을 가지는 액세스 제어 장치 및 프로비저닝 컴퓨팅 장치를 포함하고,

상기 액세스 제어 장치는,

상기 액세스 제어 장치가 통신 연결될 저장 장치로 하여금, 데이터 저장 관련 요청에 의미 있는 응답을 하도록 허용할 것인지 여부를 결정하도록 구성된 하나 이상의 프로세싱 유닛을 포함하고, 상기 결정은 상기 액세스 제어 장치에 저장된 액세스 제어 정보의 제1 집합 또는 상기 액세스 제어 장치에 또한 저장된 액세스 제어 정보의 제2 집합에 적어도 일부 기초하며,

상기 프로비저닝 컴퓨팅 장치는,

상기 액세스 제어 장치로의 통신 접속(communicational coupling)과,

하나 이상의 프로세싱 유닛과,

컴퓨터 실행 가능한 명령어들을 포함하는 컴퓨터 판독가능 저장 매체를 포함하고,

상기 컴퓨터 실행 가능한 명령어들은 상기 하나 이상의 프로세싱 유닛에 의해 실행되어 상기 프로비저닝 컴퓨팅 장치로 하여금

상기 액세스 제어 장치 상에, 상기 액세스 제어 정보의 제1 집합을 저장 - 상기 액세스 제어 정보의 제1 집합은

상기 액세스 제어 장치가 통신 연결될 상기 저장 장치가, 상기 저장 장치에 저장된 데이터의 제1 집합으로 향하는 데이터 저장 관련 요청에 의미 있는 응답을 하도록 상기 액세스 제어 장치가 허용할 것인지 여부를 식별함 - 하게 하고,

상기 액세스 제어 장치 상에, 상기 액세스 제어 정보의 제2 집합을 저장 - 상기 액세스 제어 정보의 제2 집합은 상기 액세스 제어 정보의 제1 집합과 상이하고, 상기 액세스 제어 정보의 제2 집합은 상기 저장 장치가, 상기 저장 장치에 저장된 데이터의 제2 집합으로 향하는 데이터 저장 관련 요청에 의미 있는 응답을 하도록 상기 액세스 제어 장치가 허용할 것인지 여부를 식별하며, 상기 데이터의 제2 집합은 상기 데이터의 제1 집합과 상이함 - 하게 하는

시스템.

청구항 20

제19항에 있어서,

호스트 컴퓨팅 장치를 더 포함하고, 상기 호스트 컴퓨팅 장치는

상기 저장 장치로의 통신 접속과,

하나 이상의 프로세싱 유닛과,

컴퓨터 실행 가능한 명령어들을 포함하는 컴퓨터 판독가능 저장 매체를 포함하고,

상기 컴퓨터 실행 가능한 명령어들은 상기 하나 이상의 프로세싱 유닛에 의해 실행되어 상기 호스트 컴퓨팅 장치로 하여금

상기 액세스 제어 장치가 상기 저장 장치에 통신 연결되었다는 표시를 상기 저장 장치로부터 수신하고,

상기 저장 장치를 통해 상기 호스트 컴퓨팅 장치와 상기 액세스 제어 장치 사이의 통신 연결을 수립하고,

상기 액세스 제어 장치로 식별 정보를 제공하고,

상기 액세스 제어 장치가 상기 저장 장치로 하여금 상기 저장 장치로 향하는 상기 데이터 저장 관련 요청들에 대해 의미 있는 응답을 하도록 허용한 경우, 상기 저장 장치로 향하는 상기 데이터 저장 관련 요청들에 대해 의미 있는 응답을 수신하게 하며,

상기 액세스 제어 장치의 상기 하나 이상의 프로세싱 유닛은, 상기 저장 장치가 상기 제공된 식별 정보에 적어도 일부 기초하여 상기 의미 있는 응답을 제공하는 것을 허용할지 여부를 결정하도록 구성되는

시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 저장 장치와, 물리적으로 분리되고, 통신 가능하게 분리될 수 있는 액세스 제어 장치를 포함하는 저장 시스템에 관한 것이다.

배 경 기 술

[0002] 점차적으로, 컴퓨팅 장치는 비공개로 유지되도록 의도된 데이터 및 정보에 대해 작동하고 그것을 저장하는 데 활용되고 있다. 이러한 데이터 및 정보는 행정 기관용 보안 사항을 포함할 수 있지만, 이러한 정보가 악의성이 있는 자 또는 적대적인 자에게 획득될 경우 한 명 이상의 개인에게 손해를 끼칠 수 있는 사업 및 개인 정보를 더 많이 포함할 수 있다. 이와 같이, 컴퓨팅 장치의 하드웨어와 관련하여 또한 컴퓨팅 장치의 소프트웨어와 관련하여 여러 보안 메커니즘이 구현되어 왔다. 이러한 하드웨어 보안 메커니즘의 예시는 지문 등과 같은 생물학적 정보에 기초한 보안용 암호 및 키보드 잠금, 통신 포트 잠금, 등과 같이 컴퓨팅 장치에 대한 물리적 액세스 장벽을 생성하도록 설계된 주변 장치를 포함한다. 컴퓨팅 장치의 소프트웨어와 연관된 보안 메커니즘의 예시는 다양한 암호화 기술 및 다양한 액세스 제어 기술을 포함한다.

발명의 내용

해결하려는 과제

[0003] 그러나 하나 이상의 컴퓨터 판독 가능 매체에 저장된 데이터의 보호는 때때로 컴퓨팅 장치와 전혀 직접적으로 연결되지 않은 동작 동안에는 약해진다. 예를 들면, 하나 이상의 컴퓨터 판독 가능 매체에 저장된 데이터는, 하드 디스크 드라이브 등과 같이 컴퓨터 판독 가능 매체를 포함하는 저장 장치의 물리적 출하(shipment)가 적절한 보안 수단을 갖지 않고, 그 결과로 손실 또는 도난당할 때 위험에 노출될 수 있고 노출되었다. 마찬가지로, 하나 이상의 컴퓨터 판독 가능 매체에 저장된 데이터는, 컴퓨터 판독 가능 매체를 포함하는 저장 장치가 호스트로부터의 액세스에 장애가 있고, 그에 따라 폐기되었을 때 위험에 노출될 수 있고 노출되었다. 때때로 이러한 "장애(failed)" 저장 장치는 컴퓨팅 장치에 의해 검색 및 액세스될 수 있는 형태로 그 컴퓨터 판독 가능 매체에 저장된 상당히 높은 비율의 데이터를 보유한다.

[0004] 특히 이러한 매체를 포함하는 저장 장치가 악의적인 자 또는 적대적인 자에게 물리적으로 액세스 가능하게 되는 경우에, 컴퓨터 판독 가능 매체에 저장된 데이터의 보안을 강화하기 위해서, "최대 볼륨(full volume)" 암호화 방법이 개발되었는데, 이것에 의해 저장 장치의 컴퓨터 판독 가능 저장 매체에 저장된 거의 모든 데이터가 암호화된 형태로 저장되어, 악의적인 자 또는 적대적인 자가 이러한 저장 장치에 대한 물리적 제어를 획득한다고 해도, 적절한 복호화 키(decryption key)가 없어 데이터를 복호화할 수 없을 것이다. 더 큰 성능을 제공하기 위해서, 저장 장치에 저장된 데이터의 암호화는, 컴퓨팅 장치의 하나 이상의 중앙 처리 장치에게 이러한 데이터를 저장 및 검색하는 부담을 지우는 것보다는 저장 장치 그 자체의 일부분인 전용 암호 하드웨어에 의해 실행될 수 있다.

[0005] 최대 볼륨 암호화 방법에 추가하여, 중요 데이터가 저장되어 있는 컴퓨터 판독 가능 저장 매체 또는 전체 저장 장치의 적절한 방식으로 된 물리적 복호화는 마찬가지로 이러한 데이터의 보호 및 보안을 강화할 수 있다. 예를 들면, 보호되어야 하는 데이터를 저장할 수 있는 컴퓨터 판독 가능 저장 매체는 물리적으로 조각나거나 임의적이고, 강한 자기장에 노출되어 이러한 데이터가 물리적으로 일치하지 않거나, 컴퓨터 판독 가능 매체로부터 물리적으로 복구 불가능하게 할 수 있다. 이와 다르게, 저장 장치를 물리적으로 파괴하는 것 대신에, 컴퓨터 판독 가능 저장 매체에 저장된 중요 데이터는 사전 정의된 보안 삭제 정책에 따라서 여러 번 컴퓨팅 장치에 의해 덮어쓰기(overwritten)될 수 있다. 불행하게도, 컴퓨터 판독 가능 저장 매체 및 저장 장치의 물리적 파괴는 비용이 많이 들고, 시간 소모적일 수 있으며, 효율성이라는 것은 시간과 비용을 감소하고자 하는 것이므로 이러한 매체에 저장된 데이터의 보호 및 파괴를 절충할 수 있는 지름길을 이용함으로써, 물리적 파괴에 드는 노력을 감소시킬 수 있다. 다른 비효율성을 추가하자면, 정부 보안 규정 또는 개인 정보 보호 규정 등과 같은 여러 규정은, 컴퓨터 판독 가능 저장 매체의 적절한 파괴를 특정 방식으로 의무화하고 문서화하는 조건 등과 같은 추가적인 부담을 지울 수 있다.

[0006] 서버 환경 또는 기업형 정보 기술(IT) 환경 등과 같은 많은 사용 시나리오에서, 저장 장치는 때때로 호스트 사이에서 이동된다. 이러한 환경에서, 액세스 제어 강화의 형태가 유용할 수 있다. 불행하게도, 액세스 제어의 형태를 갖는 프로비저닝(provisioning) 저장 장치는 복잡할 수 있고, 많은 추가적인 하드웨어 부품, 개발 및 후속 고장 수리 비용을 초래할 수 있다.

과제의 해결 수단

[0007] 저장 장치는, 본 명세서에서 "액세스 제어 장치"로 지칭되고 저장 장치의 나머지 부분으로부터 물리적 및 통신 가능하게 분리될 수 있는 물리적 개체와 연관될 수 있다. 추가하여, 컴퓨팅 장치는 저장 장치와는 독립적으로 액세스 제어 장치와 통신할 수 있는 컴퓨터 실행 가능 명령어를 포함할 수 있다.

[0008] 일실시예에서, 액세스 제어 장치는 저장 장치의 컴퓨터 판독 가능 매체에 저장된 데이터를 직접 또는 간접적으로 암호화 및 복호화하는 데 있어서 저장 장치의 하드웨어 암호 시스템에 의해 활용될 수 있는 암호 정보를 제공받을 수 있다. 액세스 제어 장치는 그 암호 정보를 저장 장치의 하드웨어 암호 시스템으로 선택적으로만 제공하고, 그에 의해 저장 장치가 그곳에 저장된 데이터에 대한 선택적인 액세스를 제공하게 하는 방식으로 제공받을 수 있다. 결과적으로, 액세스 제어 장치가 연관된 저장 장치에 대해 통신 가능하게 결합된 경우에도, 액세스 제어 장치는 사전 결정된 조건이 충족될 때 저장 장치의 하드웨어 암호 시스템에 그 암호 정보를 릴리스(release)하기만 함으로써 저장 장치에 저장된 암호화된 데이터에 대한 액세스를 제한할 수 있다.

[0009] 다른 실시예에서, 액세스 제어 장치는 액세스 제어 장치와 연관된 저장 장치에 저장된 데이터를 액세스하도록

허용될 수 있는 컴퓨팅 장치 또는 사용자 등과 같은 개체의 목록을 제공받을 수 있다. 다음에 액세스 제어 장치는 자신과 연관된 저장 장치에게 열거된 개체에 속하지 않는 개체로부터의 데이터 저장 관련 통신에 의미 있는 응답을 하지 않도록 명령할 수 있다. 이와 다르게 또는 추가하여, 액세스 제어 장치가 암호 정보를 제공받는다면, 이 장치는 그 암호 정보를 저장 장치의 하드웨어 암호 시스템에 제공할 수 있고, 그에 따라 저장 장치가 저장된 데이터를 액세스하고자 하는 개체가 열거된 개체 중에 속하는 경우에만 그 저장된 데이터에 대한 액세스를 제공하도록 허용한다. 저장된 데이터를 액세스하고자 하는 개체는, 요구/응답 인증 메커니즘의 환경 내에서 등과 같이 보안된 환경에서 제공될 수 있는 사용자 패스워드, 컴퓨팅 장치 식별자 또는 다른 유사 정보를 통해 자신의 신분을 증명할 수 있다.

[0010] 다른 실시예에서, 액세스 제어 장치는 허가 컴퓨팅 장치와 보안된 통신 터널을 형성할 수 있게 하는 암호 정보를 제공받을 수 있다. 액세스 제어 장치와 연관된 저장 장치에 저장된 데이터를 액세스하고자 하는 컴퓨팅 장치는 액세스 제어 장치가 보안된 터널을 통해 허가 컴퓨팅 장치와 통신할 수 있게 하는 데 이용될 수 있다. 다음에 액세스 제어 장치는 허가 컴퓨팅 장치에게 관련 정보를 제공할 수 있고, 허가 컴퓨팅 장치가 그 동작이 적절하다고 표시한 경우에만 그와 연관되어 있는 저장 장치에 대해 요청한 장치에게 데이터를 제공하게 하거나 그와 같이 하도록 명령할 수 있다.

[0011] 또 다른 실시예에서, 액세스 제어 장치는 액세스 제어 장치가 자신을 업데이트하거나 맞춤화하여 소비자 특정 액세스 제어 로직 및 알고리즘을 제공하게 할 수 있는 실행 가능 명령어를 제공받을 수 있다. 이러한 실행 가능 명령어의 집합, 또는 "스크립트릿(scriptlets)"은 프로비저닝 동안에 액세스 제어 장치에 제공될 수 있고, 보안되고 신뢰 가능한 방식으로 외부 컴퓨팅 장치로부터 업데이트될 수 있다. 액세스 제어 장치는 연관된 저장 장치 또는 컴퓨팅 장치와는 공간적, 시간적, 또는 공간 및 시간적으로 그와 별개로 개시되는 방식으로 제공될 수 있다.

[0012] 또 다른 실시예에서, 액세스 제어 장치는 액세스 제어 장치가 연관된 저장 장치에 저장된 데이터를 삭제할 수 있게 하거나, 액세스 제어 장치에 저장된 임의의 암호 정보를 삭제할 수 있게 함으로써, 이러한 암호 정보를 이용하여 암호화되어 연관된 저장 장치에 있는 데이터가 판독 불가능하고 액세스 불가능하게 하는 실행 가능 명령어를 제공받을 수 있다. 액세스 제어 장치는 그 자신의 결정에 기초하거나 허가 컴퓨팅 장치로부터 수신된 것과 같이 다른 곳으로부터 수신된 명령어에 기초하여 이러한 실행 가능 명령어를 활성화할 수 있다.

[0013] 이 요약은 이하의 상세한 설명에서 보다 상세하게 설명되는 개념의 선택을 단순화된 형태로 도입하고자 제시된 것이다. 이 요약은 청구 대상의 액세스 제어 특성 또는 본질적인 특성을 식별하도록 의도된 것이 아니며, 청구 대상의 범주를 제한하는 데 이용되도록 의도된 것도 아니다.

[0014] 추가적인 특징 및 이점은 첨부된 도면을 참조하여 이하의 상세한 설명을 읽어 내려감으로써 명확해질 것이다.

[0015] 이하의 상세한 설명은 첨부된 도면과 함께 읽을 때 가장 잘 이해될 수 있을 것이다.

발명의 효과

[0016] 본 발명은 식별 정보 등과 같은 중요 데이터의 보안에 드는 부담과 비용을 증가하지 않으면서 보안성을 제공하는 액세스 제어 장치 및 그 방법을 제공한다.

도면의 간단한 설명

[0017] 도 1은 예시적인 프로비저닝 컴퓨팅 장치 및 예시적인 액세스 제어 장치를 도시하는 블록도.

도 2는 예시적인 액세스 컴퓨팅 장치, 예시적인 액세스 제어 장치 및 예시적인 저장 장치를 도시하는 블록도.

도 3은 예시적인 액세스 컴퓨팅 장치, 예시적인 액세스 제어 장치 및 예시적인 저장 장치를 도시하는 다른 블록도.

도 4는 액세스 제어 장치와 저장 장치 사이의 예시적인 통신을 도시하는 블록도.

도 5는 액세스 제어 장치와 저장 장치 사이의 추가적인 예시적인 통신을 도시하는 블록도.

도 6은 예시적인 프로비저닝 컴퓨팅 장치의 예시적인 동작을 도시하는 흐름도.

도 7은 예시적인 액세스 컴퓨팅 장치의 예시적인 동작을 도시하는 흐름도.

발명을 실시하기 위한 구체적인 내용

[0018] 이하의 설명은 저장 장치와, 물리적으로 분리되고, 통신 가능하게 분리될 수 있는 액세스 제어 장치를 포함하는 저장 시스템에 관한 것으로, 여기에서 액세스 제어 장치는 저장 장치에 저장된 데이터가 그것을 액세스하고자 하는 개체에게 이용 가능하게 될 때를 제어하기 위해 액세스 제어 장치에 의해 활용될 수 있는 액세스 제어 정보를 포함한다. 액세스 제어 장치는 저장 장치가 허가받지 않은 개체와 통신하는 것을 방지할 수 있는데, 그것은, 그와 같은 개체로부터의 저장 장치에 이미 저장되어 있는 데이터에 대해 요청하는 통신 및 제공된 데이터가 저장 장치에 저장되도록 요청하는 통신을 포함하는 데이터 저장 관련 통신에 대하여 의미 있는 응답을 하지 않도록 명령함으로써 이루어진다. 액세스 제어 장치는 또한 암호 정보를 포함할 수 있고, 저장 장치의 하드웨어 암호 시스템에 대한 그 암호 정보의 선택적 규정은 저장 장치에 저장된 암호화된 데이터에 대한 액세스를 제어할 수 있다. 허가는 액세스 제어 장치가 허가된 개체의 사전 제공된 목록에 대하여 액세스하고자 하는 개체의 식별 정보를 비교하는 것에 의한 것 등과 같이 액세스 제어 장치 자체에 의해 제공될 수 있거나, 액세스 제어 장치에 통신 가능하게 결합될 수 있고 액세스 컴퓨팅 장치를 이용하여 액세스 제어 장치에 허가 명령어를 제공할 수 있는 허가 컴퓨팅 장치에 의해 제공될 수 있다.

[0019] 본 명세서에 개시된 기술은 저장 장치와, 물리적 분리 및 통신 가능하게 분리되는 액세스 제어 장치에 집중하고 있으나 이것으로 한정되지는 않는다. 또한, 그 경우에 액세스 제어 장치와 저장 장치가 물리적으로 분리되어 있을 때 존재하는 보안상의 이점이 제공되지는 않겠지만, 이하에 개시된 액세스 제어 메커니즘은 단일 저장 장치 내에서 분리되지 않는 이산 부품(discrete components)으로 동등하게 구현될 수 있다. 그러나 이러한 보안상의 이점은 이하에 설명된 액세스 제어 메커니즘에 의해 제공되는 보안성과는 무관하고, 그러므로 이하에 설명되는 메커니즘의 적용 가능성을 특정한 하드웨어 구성으로 한정하지 않는다. 결과적으로, 이하의 설명은 물리적으로 분리 가능한 액세스 제어 장치와 연관된 저장 장치를 참조하여 이루어졌으나, 그 설명의 범주 자체는 그것으로 한정되도록 의도되지 않았다.

[0020] 필수적인 것은 아니지만 추가적으로, 이하의 설명은 하나 이상의 처리 장치에 의해 실행되는 프로그램 모듈 등과 같은 컴퓨터 실행 가능 명령어의 일반적인 문맥에서 이루어질 것이다. 보다 구체적으로, 설명은 다르게 표시되지 않았다면 하나 이상의 처리 장치에 의해 실행되는 동작을 표시하는 단계 및 기호를 참조할 것이다. 그러므로 때때로 컴퓨터 실행용으로 지칭되는 이러한 단계 및 동작이 구조화된 형태로 데이터를 표시하는 전기 신호가 처리 장치에 의해 처리되는 것을 포함한다는 점을 이해할 것이다. 이 처리는 메모리 내의 위치에서 데이터를 변환하거나 그것을 유지하는데, 이것은 당업자에게 잘 알려진 방식으로 처리 장치 또는 그것에 접속된 주변 장치의 동작을 재조정하거나 변경한다. 데이터가 유지되어 있는 데이터 구조는 데이터의 형식에 의해 정의된 특정한 특성을 갖는 물리적 위치이다.

[0021] 일반적으로, 프로그램 모듈은 특정한 작업을 실행하거나 특정한 추상화 데이터 종류를 구현하는 루틴(routines), 프로그램, 객체(objects), 부품, 데이터 구조 등을 포함한다. 더욱이 당업자라면 참조된 처리 장치가 종래의 퍼스널 컴퓨팅 처리 장치로 반드시 한정되는 것은 아니고, 주변 장치, 휴대형 장치, 멀티-프로세서 시스템, 마이크로 프로세서 기반 또는 프로그래밍 가능 소비 가전 내에서 때때로 발견되는 전용 프로세서, 전용 프로세서, 통신 프로세서, 버스 프로세서, 제어기 등을 포함하는 다른 프로세서 구성을 포함한다는 것을 이해할 것이다. 마찬가지로, 작업들이 통신 네트워크를 통해 링크된 원격 처리 장치에 의해 실행되는 분산형 컴퓨팅 환경에서도 이러한 메커니즘이 실현될 수 있기 때문에 이하의 설명에서 참조된 컴퓨팅 장치는 독립형 컴퓨팅 장치로 한정되어야만 하는 것은 아니다. 분산형 컴퓨팅 환경 내에서, 프로그램 모듈은 지역 및 원격 메모리 저장 장치 모두에 위치될 수 있다.

[0022] 도 1로 돌아가서, 예시적인 프로비저닝 컴퓨팅 장치(110) 및 예시적인 액세스 제어 장치(170)를 포함하는 예시적인 시스템(100)이 도시되어 있다. 도시된 바와 같이, 프로비저닝 컴퓨팅 장치(110)는 액세스 제어 장치가 연관된 저장 장치에 대한 액세스를 제한할 수 있게 하는 정보를 액세스 제어 장치에 제공하는 것 등에 의해 액세스 제어 장치(170)를 제공하는 데 활용될 수 있다.

[0023] 먼저 프로비저닝 컴퓨팅 장치(110)로 되돌아가면, 하나 이상의 중앙 처리 장치(CPU)(120)와, 시스템 메모리(130)와, 처리 장치(120)에 연결된 시스템 메모리(130)를 포함하는 여러 시스템 부품들을 결합하는 시스템 버스(121)를 포함할 수 있지만 이것으로 한정되지 않는다. 시스템 버스(121)는 다양한 버스 또는 점대점(point-to-point) 아키텍처 중 임의의 것을 이용하는 메모리 버스 또는 메모리 제어기, 주변 버스, 및 지역 버스를 포함하는 몇몇 종류의 버스 구조 중 어느 하나일 수 있다. 특정 물리적 구현에 기초하여, 하나 이상의 CPU(120) 및 시스템 메모리(130)는 단일 칩 상에서 위치되는 것 등과 같이 물리적으로 동일 위치(co-located)일 수 있다.

이러한 경우에, 일부 또는 전부의 시스템 버스(121)는 단일 칩 구조 내의 실리콘 경로에 불과할 수 있고, 도 1에 도시된 그 도면은 설명을 목적으로 순전히 표기의 편의를 제공하기 위한 것일 수 있다.

[0024] 프로비저닝 컴퓨팅 장치(110)는 또한 전형적으로 프로비저닝 컴퓨팅 장치(110) 등과 같이 컴퓨팅 장치에 의해 액세스될 수 있는 임의의 이용 가능한 매체를 포함할 수 있는 컴퓨터 판독 가능 매체를 포함하고, 휘발성 및 비휘발성 매체 및 탈착 가능 및 탈착 불가능 매체를 모두 포함한다. 제한 사항이 아닌 예시로서, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터 등과 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현되는 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, DVD(digital versatile disks) 또는 다른 광학 디스크 저장부, 자기 카세트, 자기 테이프, 자기 디스크 저장부 또는 다른 자기 저장 장치, SSD(solid state disks) 또는 다른 고체 상태 기반의 저장 장치, 또는 원하는 정보를 저장하는 데 사용될 수 있고, 프로비저닝 컴퓨팅 장치(110) 등과 같은 컴퓨팅 장치에 의해 액세스될 수 있는 임의의 다른 매체를 포함하지만 이것으로 한정되지 않는다. 통신 매체는 전형적으로 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터를 반송파(carrier wave) 또는 다른 전송 메커니즘 등과 같은 변조된 데이터 신호로 구현하고, 임의의 정보 전달 매체를 포함한다. 제한 사항이 아닌 예시로서, 통신 매체는 유선 네트워크 또는 직접 유선 접속 등과 같은 유선 매체와, 음파, RF, 적외선 및 다른 무선 매체 등과 같은 무선 매체를 포함한다. 상술된 것 중 임의의 것의 조합도 또한 컴퓨터 판독 가능 매체의 범주 내에 포함되어야 한다.

[0025] 시스템 메모리(130)는 판독 전용 메모리(ROM)(131) 및 랜덤 액세스 메모리(RAM)(132) 등과 같은 휘발성 및/또는 비휘발성 메모리의 형태를 갖는 컴퓨터 저장 매체를 포함한다. 시동 중에서 등과 같이 컴퓨팅 장치(100) 내의 소자들 간의 정보 전달을 돕는 기본 루틴을 포함하는 기본 입/출력 시스템(133)(BIOS)은 전형적으로 ROM(131)에 저장된다. RAM(132)은 전형적으로 즉시 액세스 가능 및/또는 처리 장치(120)에 의해 곧 작동되는 데이터 및/또는 프로그램 모듈을 포함한다. 제한 사항이 아닌 예시로서, 도 1은 운영 시스템(134), 다른 프로그램 모듈(135) 및 프로그램 데이터(136)를 도시한다. 또한 몇몇 실시예에서, 운영 시스템(134)의 일부분이 될 수 있는 최대 볼륨 암호화 서비스(137)가 도시되어 있다. 최대 볼륨 암호화 서비스(137)는 프로비저닝 컴퓨팅 장치(110) 등과 같은 컴퓨팅 장치가, 하나 이상의 컴퓨터 판독 가능 저장 매체에 저장되거나, 컴퓨팅 장치의 운영 시스템(134) 또는 다른 저장 제어기에 의해 개별 볼륨으로서 정의되는 부분 등과 같은 상기 저장 매체의 일부분에 저장된 거의 모두 또는 전부의 정보에 대한 암호화를 제공할 수 있게 한다.

[0026] 선택적으로 추가하여 최대 볼륨 암호화 서비스(137)를 포함하는 프로비저닝 컴퓨팅 장치(110)의 운영 시스템(134)은 또한 저장 장치 드라이버 스택(138)을 포함할 수 있다. 저장 장치 드라이버 스택(138)은 이하에 설명된 것 등과 같은 하나 이상의 저장 장치와 통신을 형성 및 유지하는 것과 관련된 컴퓨터 판독 가능 명령어를 포함할 수 있다. 추가하여, 저장 장치 드라이버 스택(138)은 액세스 제어 장치(170) 등과 같이 액세스 제어 장치와 통신을 형성 및 유지하는 것과 관련된 컴퓨터 실행 가능 명령어를 포함할 수 있는 액세스 제어 장치 확장부(139)를 포함할 수 있다. 액세스 제어 장치(170) 등과 같은 액세스 제어 장치가 프로비저닝 컴퓨팅 장치(110)에 대해 통신 가능하게 결합되어 있다는 표시를 저장 장치 드라이버 스택이 수신하면, 액세스 제어 장치 확장부(139)는 저장 장치 드라이버 스택(138)에 의해 요청되고 로딩될 수 있다. 이하에서 더 설명되는 바와 같이, 액세스 제어 장치(170) 등과 같은 액세스 제어 장치는 유선 또는 무선 통신 접속을 통한 것 등과 같이 직접적으로 또는 액세스 제어 장치가 통신 가능하게 결합되어 있는 저장 장치 등과 유사한 다른 중간 장치를 통해서 프로비저닝 컴퓨팅 장치(110) 등과 같은 컴퓨팅 장치에 대해 통신 가능하게 결합될 수 있다.

[0027] 프로비저닝 컴퓨팅 장치(110)는 설명된 것에 추가하여 탈착 가능/탈착 불가능, 휘발성/비휘발성 컴퓨터 저장 장치를 포함하는 저장 장치를 포함할 수 있다. 오로지 예시로서, 도 1은 탈착 불가능, 비휘발성 자기 매체를 판독하거나 기록하는 하드 디스크 저장 장치(141, 146, 147)를 도시한다. 예시적인 컴퓨팅 장치와 사용 가능한 다른 탈착 가능/탈착 불가능, 휘발성/비휘발성 컴퓨터 저장 매체는 자기 테이프 카세트, 플래시 메모리 카드, 고체 상태 드라이브(solid state drives : SSD) 및 다른 고체 상태 기반 저장 장치, DVD(digital versatile disks), 디지털 비디오 테이프, 고체 상태 RAM, 고체 상태 ROM 등을 포함하지만 이것으로 한정되지 않는다. 하드 디스크 저장 장치(141, 146, 147) 또는 다른 탈착 가능/탈착 불가능, 휘발성/비휘발성 컴퓨터 저장 매체 중 어느 하나는 전형적으로 인터페이스(140) 등과 같은 메모리 인터페이스를 통해 시스템 버스(121)에 대해 직접 또는 간접적으로 접속되어 있다. 도 1에 도시된 예시적인 프로비저닝 컴퓨팅 장치(110)에서, 하드 디스크 저장 장치(141)는 프로비저닝 컴퓨팅 장치(110) 내부의 물리적 접속 또는 포트를 경유하여 노출된 외부 접속 등을 통해서 비휘발성 메모리 인터페이스(140)에 직접 접속되도록 도시되어 있는 한편, 하드 디스크 저장 장치(146,

147)는 예를 들면, RAID(Redundant Array of Inexpensive Devices) 제어기 등과 같은 저장 호스트 제어기(145)에 접속된 다음, 컴퓨팅 장치(100)에 대해 물리적으로 내부에 있는 접속 등을 통해 인터페이스(140)에 접속되는 것으로 도시되어 있다. 비휘발성 메모리 인터페이스(140)는 USB(Universal Serial Bus) 인터페이스, IEEE1394 명세서 중 임의의 하나 이상에 준하는 인터페이스, SATA(Serial AT Attachment) 인터페이스 또는 다른 유사 인터페이스를 포함하지만 이것으로 한정되지 않는 임의의 비휘발성 메모리 인터페이스일 수 있다.

[0028] 프로비저닝 컴퓨팅 장치(110)는 하나 이상의 원격 컴퓨팅 장치에 대한 지역 접속부를 이용하는 네트워크형 환경에서 동작할 수 있다. 설명의 단순성을 위하여, 프로비저닝 컴퓨팅 장치(110)는 임의의 특정한 네트워크 또는 네트워킹 프로토콜로 한정되지 않는 네트워크(155)에 접속된 것으로 도 1에 도시되어 있다. 도 1에 도시된 로직 접속은 LAN(local area network), WAN(wide area network) 또는 다른 네트워크일 수 있는 범용 네트워크 접속(151)이다. 프로비저닝 컴퓨팅 장치(110)는 시스템 버스(121)에 접속되어 있는 네트워크 인터페이스 또는 어댑터(150)를 통해서 범용 네트워크 접속(151)에 접속된다. 네트워크형 환경에서, 프로비저닝 컴퓨팅 장치(110) 또는 그 부분 또는 주변 장치와 관련하여 도시된 프로그램 모듈은 범용 네트워크 접속(151)을 통해 프로비저닝 컴퓨팅 장치(110)에 통신 가능하게 결합된 하나 이상의 다른 컴퓨팅 장치의 메모리 내에 저장될 수 있다. 예를 들면, 이하에서 보다 상세하게 도시되는 것과 같은 허가 컴퓨팅 장치는 그 동작이 이하에 설명되어 있는 컴퓨터 실행 가능 명령어의 일부 또는 전부에 대한 호스트로서 작용할 수 있다. 도시된 네트워크 접속은 예시적인 것이고, 컴퓨팅 장치들 간에 통신 링크를 형성하는 다른 수단도 이용 가능하다는 것을 이해할 것이다.

[0029] 이하의 설명과 관련하여, 프로비저닝 컴퓨팅 장치(110)는 도 1에 도시된 액세스 제어 장치(170) 등과 같은 액세스 제어 장치에 통신 가능하게 결합될 수 있다. 액세스 제어 장치(170)는 유선 또는 무선 접속을 통한 것을 포함하여 프로비저닝 컴퓨팅 장치(110)에 직접 통신 가능하게 결합되거나, 액세스 제어 장치는 액세스 제어 장치가 직접 통신 가능하게 결합되어 있는 저장 장치를 통해 프로비저닝 컴퓨팅 장치에 대해 간접적으로 통신 가능하게 결합될 수 있다. 도 1의 시스템(100)에서, 액세스 제어 장치(170)는 비휘발성 메모리 인터페이스(140)를 통한 것 등과 같이 프로비저닝 컴퓨팅 장치(110)에 직접 통신 가능하게 결합된 것으로 도시되어 있다. 도 1의 점선은 액세스 제어 장치(170)가 프로비저닝 컴퓨팅 장치(110)에 대해 탈착형으로 통신 가능하게 결합될 수 있다는 것을 나타낸다. 일실시예에서, 제조 효율을 위해, 액세스 제어 장치(170)는 표준 메모리 카드 명세서에 준할 수 있고, 그러므로 예를 들면, 프로비저닝 컴퓨팅 장치에 통신 가능하게 접속된 내부 메모리 카드 판독기 또는 외부 메모리 카드 판독기 주변 기기를 통한 것 등과 같이 동일한 명세서에 준하는 임의의 다른 이러한 메모리 카드와 동일한 방식으로 프로비저닝 컴퓨팅 장치(110)에 통신 가능하게 결합될 수 있다.

[0030] 액세스 제어 장치(170)는 입력의 집합에 기초하여 그 출력을 조정할 수 있는 제어기 또는 다른 부품을 포함할 수 있는 하나 이상의 처리 장치(171)를 포함할 수 있다. 더 이하에서 설명되는 바와 같이, 액세스 제어 장치(170)의 처리 장치(171)는 저장 장치가 통신 가능하게 접속되어 있는 액세스 컴퓨팅 장치에 연관된 저장 장치가 데이터를 제공하거나 데이터를 저장할 수 있도록 허용 및 가능하게 하는지 여부를 결정하는 것과 연관된 동작을 실행하는 데 활용될 수 있다.

[0031] 이러한 게이트-키핑(gate-keeping)과 관련된 동작을 실행하는 데 있어서, 액세스 제어 장치(170)의 처리 장치(171)는 시스템(100)에서 도시된 바와 같이 프로비저닝 컴퓨팅 장치(110)에 의해 제공될 수 있는 액세스 제어 정보(176)를 이용할 수 있다. 일실시예에서, 액세스 제어 정보(176)는 액세스 제어 장치(170)의 암호 정보로 암호화된 데이터를 액세스하도록 허용될 수 있는 개체의 목록을 포함할 수 있고, 결과적으로 액세스 제어 장치가 이러한 개체가 액세스를 요청하였다고 결정할 때, 액세스 제어 장치는 연관된 저장 장치가 요청하는 개체의 액세스를 허용하도록 할 수 있다. 예를 들면, 액세스 제어 정보(176)는 MAC(Media Access Control) 어드레스, WWN(World Wide Names), 또는 다른 고유한 장치 또는 개체 식별자 등과 같은 식별자의 목록을 포함할 수 있다. 액세스 제어 정보(176)는 또한 개체의 패스워드를 포함하여, 개체는 액세스 제어 장치가 암호 정보를 공개하기 전에 그 패스워드를 제공하는 것에 의해 액세스 제어 장치(170)에 그 식별 정보를 증명하도록 요구될 수 있다. 유사한 요구/응답 템플릿에 기초한 다른 메커니즘을 포함하는 다른 암호 메커니즘은 액세스 제어 장치(170)가 통신 가능하게 결합되어 있는 저장 장치에 의해 저장된 데이터를 액세스하고자 하는 개체들이 액세스 제어 장치(170)에 대해 인증을 제공하는 데 활용될 수 있다.

[0032] 일실시예에서, 액세스 제어 장치(170)는 이러한 저장 장치의 저장 매체에 저장될 데이터를 암호화하고 이미 저장 매체에 저장된 암호화된 데이터를 복호화할 때 저장 장치에 의해 활용될 수 있는 저장 관련 암호 정보(175)를 더 포함할 수 있다. 이러한 것을 가지고, 액세스 제어 장치(170)는 저장 장치 및 그 데이터에 대한 액세스를 요청하는 개체가 액세스 제어 정보(176)에 의해 액세스가 허용되도록 표시된 개체 중 하나라고 액세스 제어 장치가 결정할 때까지, 저장 장치에 암호 정보를 제공하지 않음으로써 저장 장치의 데이터에 대한 액세스를 제

어하는 데 저장 관련 암호 정보(175)를 이용할 수 있다. 액세스 제어 정보(176)가 허용 가능 개체의 리스트 또는 액세스가 거부되어야 할 개체의 리스트를 포함하는 실시예는 데이터에 액세스할 수 있는 개체가 한정되고 비교적 고정된 가정 또는 소규모 사업 환경 내에서 특히 유용할 수 있다.

[0033] 그러나 다른 실시예에서, 허가 컴퓨팅 장치 등과 같이 액세스 제어 장치(170) 외부의 컴퓨팅 장치는 액세스 제어 장치가 통신 가능하게 결합되어 있는 저장 장치에 대한 액세스를 허용할 것인지 여부를 결정할 때 액세스 제어 장치에 의해 참조될 수 있다. 이러한 실시예에서, 액세스 제어 장치(170)는 액세스를 허용해야 하거나 허용하지 않아야 할 때를 통지하기 위해 허가 컴퓨팅 장치에 의존할 수 있다. 당업자들에게 알려진 바와 같이, 이러한 실시예는 소정의 데이터를 액세스하도록 허용될 수 있는 개체가 때때로 변경될 수 있는 기업 환경 내에서 유용할 수 있다. 추가하여, 이하에 더 설명되는 바와 같이, 액세스 제어 장치(170)가 다른 컴퓨팅 장치를 참조하는 실시예는 기업에 의해 전형적으로 구현되는 기존의 액세스 제어 기술과 통합될 수 있다.

[0034] 상술된 실시예에서, 프로비저닝 컴퓨팅 장치(110)에 의해 액세스 제어 장치(170)에게 제공된 액세스 제어 정보(176)는 허가 컴퓨팅 장치와 보안된 통신을 형성하는 것에 관한 정보를 포함할 수 있다. 예를 들면, 액세스 제어 정보(176)는 허가 컴퓨팅 장치의 공개 액세스 제어 등과 같은 암호 정보, 또는 액세스 제어 장치(170)가 허가 컴퓨팅 장치와의 보안된 통신을 제공하는 공유 비밀 또는 다른 이러한 암호 도구를 협상할 수 있게 하는 다른 이러한 정보를 포함할 수 있다. 액세스 제어 정보(176)는 또한 허가 컴퓨팅 장치의 DNS(Domain Name Server) 이름 또는 그 네트워크 어드레스 등과 같은 허가 컴퓨팅 장치의 식별 정보를 포함할 수 있다. 아래에 더 설명되는 다른 실시예에서, 이러한 식별 정보는 그 대신에 액세스 제어 장치(170)가 통신 가능하게 결합되어 있는 저장 장치에 있는 데이터를 액세스하고자 하는 컴퓨팅 장치에 제공될 수 있다.

[0035] 시스템(100)에 도시된 바와 같이, 일실시예에서, 프로비저닝 컴퓨팅 장치(110)의 운영 시스템(134)은 액세스 제어 장치(170)와 통신하기 위해 저장 장치 드라이버 스택(138)을 이용할 수 있다. 보다 구체적으로, 표시된 바와 같이, 저장 장치 드라이버 스택(138)은 저장 장치 드라이버 스택이 액세스 제어 장치(170)의 존재를 검출할 때 액세스 제어 장치 확장부(139)를 개시 또는 로딩할 수 있다. 그러면 액세스 제어 장치 확장부(139)는 액세스 제어 정보(176)의 제공을 포함하여 액세스 제어 장치(170)와의 통신을 처리할 수 있다. 일실시예에서, 도시된 바와 같이 프로그램 모듈(135)의 일부분이 될 수 있는 보안 관련 프로그램 등과 같은 하나 이상의 프로그램은 액세스 제어 장치 확장부(139)로 제공될 수 있고, 거기에서부터 상술된 바와 같이 그 액세스가 승인될 것이거나, 상술된 바와 같이, 액세스 제어 장치(170)에 대해 외부에 있는 허가 컴퓨팅 장치에 대한 보안된 통신 접속을 형성 및 유지하기 위하여 암호 정보를 포함하는 정보를 포함할 수 있는 개체의 목록을 포함할 수 있는 액세스 제어 정보(176)는 액세스 제어 장치(170)로 제공될 수 있다.

[0036] 프로비저닝 컴퓨팅 장치(110)는, 액세스 제어 장치 확장부(139)를 통하는 것 등과 같이 액세스 제어 장치(170)에 액세스 제어 정보(176)를 제공할 수 있고, 또한 선택적으로 액세스 제어 장치에 저장 관련 암호 정보(175)를 제공할 수 있다. 저장 관련 암호 정보(175) 및 연관된 통신은 이들이 선택적임을 나타내기 위해서 시스템(100) 내에서 점선으로 도시되어 있다. 액세스 제어 장치(170)가 저장 장치로부터 통신 가능하게 접속 해제될 때, 저장 관련 암호 정보(175)의 부재는 이러한 저장 장치의 저장 매체에 저장된 암호화된 데이터를 액세스 불가능하게 할 수 있다. 결과적으로, 이러한 저장 장치로부터 액세스 제어 장치(170)의 통신 접속 해제는 저장 장치가 물리적으로 손실 또는 도난되었을 때에 대한 추가적인 보호층을 제공하고, 또한 이것은 이러한 저장 장치의 저장 매체에 저장된 암호화된 데이터의 암호 삭제 또는 파괴의 증거로서 작용할 수 있다.

[0037] 일실시예에서, 저장 관련 암호 정보(175)는 당업자들에게 잘 알려진 방식으로 암호화 및 복호화를 위한 액세스 제어로서 활용될 수 있는 일련의 비트일 수 있는 "물리적 액세스 제어"를 포함할 수 있다. 그러므로 이하의 설명에 사용된 바와 같은 "물리적 액세스 제어"라는 용어는, 액세스 제어 장치(170) 등과 같은 물리적 탈착 가능 소스로부터 제공되고 그곳에 저장되어 있는 암호 액세스 제어로서 활용되는 데이터의 집합을 지칭하도록 의도되었다. 이러한 물리적 액세스 제어는, 이러한 액세스 제어로 암호화된 데이터가 저장되어 있는 매체로부터 물리적으로 분리 불가능한 "로직 액세스 제어"와는 반대가 되도록 의도되었다.

[0038] 프로비저닝 컴퓨팅 장치(110)에 의해 액세스 제어 장치(170)에 선택적으로 제공된 저장 관련 암호 정보(175)는 액세스 제어 장치 확장부(139)를 통해서 프로비저닝 컴퓨팅 장치의 다수의 서브-시스템 중 임의의 하나에 의해 제공될 수 있다. 예를 들면, 로직 액세스 제어를 이용하는 것에 추가하여, 최대 볼륨 암호화 서비스(137)는 물리적 액세스 제어를 생성하고, 그것을 저장 관련 암호 정보(175)의 최소의 부분으로서 액세스 제어 장치(170)에 제공하는 그 기존의 기능성에 영향력을 줄 수 있다. 이와 다르게, 물리적 액세스 제어 또는 다른 저장 관련 암호 정보(175)는 저장 호스트 제어기(145) 또는 다른 저장 인터페이스에 존재할 수 있는 하드웨어 등과 같은 전

용 하드웨어에 의해 생성될 수 있다. 또 다른 대안으로서, 저장 관련 암호 정보(175)는 BIOS(133)로부터 액세스 제어 장치(170)에 제공될 수 있다.

[0039] 액세스 제어 장치(170)에 제공된 선택적 저장 관련 암호 정보(175)의 보안 및 기밀성을 유지하기 위해서, 이러한 정보는 프로비저닝 컴퓨팅 장치(110)에서 실행되는 악의적인 컴퓨터 실행 가능 명령어를 통한 것 등과 같이 이러한 정보가 적대적인 자에 의해 획득될 가능성을 최소화하는 방식으로 프로비저닝 컴퓨팅 장치(110)에 의해 제공될 수 있다. 그러므로 일실시예에서, 액세스 제어 장치(170)에 제공된 저장 관련 암호 정보(175)는 프로비저닝 컴퓨팅 장치(110)의 부팅(booting)의 완료 이전에 제공될 수 있고, 제공된 정보는 또한 프로비저닝 컴퓨팅 장치의 부팅의 완료 이전에 프로비저닝 컴퓨팅 장치로부터 삭제될 수 있다. 악의적인 컴퓨터 실행 가능 명령어는 전형적으로 호스트 컴퓨팅 장치의 부팅이 완료되기 전에 작동할 수 없기 때문에, 프로비저닝 컴퓨팅 장치(110)의 부팅이 완료되기 전에 액세스 제어 장치(170)에 저장 관련 암호 정보(175)를 제공하고 폐기하는 것에 의해 제공된 정보는 프로비저닝 컴퓨팅 장치에서 이후에 실행될 수 있는 임의의 악의적인 컴퓨터 실행 가능 명령어로부터 보호될 수 있다.

[0040] 예를 들면, 예를 들면, 운영 시스템(134)의 실행을 개시하는 것을 포함하는 프로비저닝 컴퓨팅 장치에서의 임의의 다른 처리를 개시하기 전에 BIOS(133)는 프로비저닝 컴퓨팅 장치(110)의 인터페이스에 통신 가능하게 접속된 액세스 제어 장치(170)의 존재를 검출할 수 있고, 액세스 제어 장치(170)에 저장 관련 암호 정보(175)를 제공할 수 있다. 마찬가지로, 제어기가 처음으로 개시되고, 운영 시스템(134)의 부팅이 개시되지 않았다면 적어도 완료되기 전에 저장 호스트 제어기(145)는 액세스 제어 장치(170)의 존재를 검출할 수 있다. 마찬가지로 제어기(145)는 액세스 제어 장치(170)에 저장 관련 암호 정보(175)를 제공할 수 있고, 임의의 악의적인 컴퓨터 실행 가능 명령어가 프로비저닝 컴퓨팅 장치(110)에서 실행하기 전에 그것을 폐기할 수 있다. 다른 대안으로서, 최대 볼륨 암호화 서비스(137)는 프로비저닝 컴퓨팅 장치(110)에서 실행하는 악의적인 컴퓨터 실행 가능 명령어로부터 그 로직 액세스 제어를 보호하도록 설계되는 메커니즘을 이미 포함하고 있을 것이므로, 최대 볼륨 암호화 서비스(137)는 이러한 메커니즘을 이용하여 액세스 제어 장치(170)에 저장 관련 암호 정보(175)를 보안 상태로 제공한 다음, 프로비저닝 컴퓨팅 장치(110)에서 그것이 발견될 가능성을 더 감소하기 위해 폐기할 수 있다. 이러한 실시예에서, 액세스 제어 장치 확장부(139)를 참조하여 상술된 기능성 중 적어도 일부는 BIOS(133) 또는 저장 호스트 제어기(145)에 의한 것 등과 같이 운영 시스템(134)의 외부에서 구현될 수 있다.

[0041] 액세스 제어 장치(170)가 프로비저닝 컴퓨팅 장치(110)에 의해 제공되었다면, 액세스 제어 장치(170)는 통신 가능하게 될 수 있고, 선택적으로 프로비저닝 컴퓨팅 장치(110)로부터 물리적으로 접속 해제된 다음 저장 장치와 결합하여 이용되어 저장 장치가 암호화된 데이터를 저장하게 하고, 저장 장치 등과 같은 컴퓨터 판독 가능 매체에 이미 저장된 암호화된 데이터를 액세스하게 할 수 있다.

[0042] 도 2를 참조하면, 시스템(200)은 액세스 컴퓨팅 장치(210)와, 액세스 제어 장치(170)와, 액세스 제어 장치가 통신 가능하게 결합될 수 있는 예시적인 저장 장치(270)를 포함하도록 도시되어 있다. 이하에 더 설명되는 바와 같이, 액세스 제어 장치(170)와 예시적인 저장 장치(270) 사이의 통신 결합은 물리적 결합일 수 있지만 반드시 그러한 것은 아니다. 예시적인 저장 장치(270)는 액세스 컴퓨팅 장치(210)에 통신 가능하게 결합된 것으로 도시된 저장 장치(241, 246 또는 247) 중 임의의 하나 이상을 나타낼 수 있다. 액세스 컴퓨팅 장치(210)는 이하에 상세하게 설명되는 프로비저닝 컴퓨팅 장치(110)와는 상이한 컴퓨팅 장치이거나, 예를 들면, 그것을 프로비저닝 컴퓨팅 장치로서 사용할 수 있는 관리자 및 그것을 액세스 컴퓨팅 장치로서 사용할 수 있는 사용자 모두에 의해 이용될 수 있는 컴퓨팅 장치 등과 같이 동일한 컴퓨팅 장치일 수 있다. 그러므로 참조 및 설명의 용이성을 위해서, 프로비저닝 컴퓨팅 장치(210)의 구성 요소는 그 기능이 유사하거나 동일할 수 있음에도 컴퓨팅 장치(110)의 유사한 구성 요소와는 상이하게 번호가 할당되어 있다. 그러므로 CPU(220), 시스템 버스(221), 시스템 메모리(230), 선택적인 비휘발성 메모리 인터페이스(240) 및 저장 호스트 제어기(245)는 모두 상술된 CPU(120), 시스템 버스(121), 시스템 메모리(130), 인터페이스(140) 및 저장 호스트 제어기(145)와 유사하다. 마찬가지로, BIOS(233)를 갖는 ROM(231)과, 저장 장치 드라이버 스택(238) 및 액세스 제어 장치 확장부(239)를 포함한 운영 시스템(234), 프로그램 모듈(235), 프로그램 데이터(236) 및 최대 볼륨 암호화 서비스(237)를 갖는 RAM(232)은, 또한 상술된 ROM(131), BIOS(133), RAM(132), 운영 시스템(134), 저장 장치 드라이버 스택(138), 액세스 제어 장치 확장부(139), 프로그램 모듈(135), 프로그램 데이터(136) 및 최대 볼륨 암호화 서비스(137)와 유사하다. 그러나 액세스 제어 장치(170)는 위에 상세하게 설명된 것과 동일한 액세스 제어 장치일 수 있다.

[0043] 도 2에 도시된 시스템(200)의 저장 장치(270)로 되돌아가면, 저장 장치(270)는 상술된 저장 장치(141, 146, 147) 중 어느 하나와 동일한 방식으로 사용될 수 있고, 그것을 대체하거나 그와 같이 동작할 수 있으며, 그 유사한 대상은 도 2에서 저장 장치(241, 246, 247)로 도시되어 있다. 게다가, 도식적으로 그에 근접하게 표시된

바와 같이, 저장 장치(270)는 보다 상세하게는 액세스 컴퓨팅 장치(210)에 통신 가능하게 결합된 임의의 하나 이상의 저장 장치(241, 246, 247)를 나타내도록 의도되었다.

[0044] 저장 장치(270)는 상술된 것 중 어느 하나를 포함하는 탈착 불가능, 비휘발성 자기 매체, 탈착 불가능, 비휘발성 고체 상태 기반의 저장 매체 또는 다른 탈착 가능/탈착 불가능, 휘발성/비휘발성 컴퓨터 저장 매체를 포함할 수 있는 하나 이상의 컴퓨터-판독 가능 매체(290)를 포함할 수 있다. 저장 장치(270)의 컴퓨터 판독 가능 매체(290)는 이러한 컴퓨팅 장치를 위한 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 다른 데이터를 저장하는 컴퓨팅 장치에 의해 이용될 수 있다. 예를 들면, 저장 장치(270)의 컴퓨터 판독 가능 매체(290)는 저장 장치(270)에 의해 제공될 때 액세스 컴퓨팅 장치(210)의 운영 시스템(234), 다른 프로그램 모듈(235) 또는 프로그램 데이터(236) 일부 또는 전부를 위한 기초가 되는 데이터일 수 있는 데이터(295)를 저장하는 것으로 도시되어 있다.

[0045] 컴퓨터 판독 가능 매체(290)에 추가하여, 예시적인 저장 장치(270)는 또한 컴퓨터 판독 가능 매체(290)에 저장을 위해 저장 장치(270)에 제공되는 데이터를 암호화할 수 있고, 컴퓨터 판독 가능 매체로부터 판독된 다음 액세스 컴퓨팅 장치(210)에 제공될 데이터를 복호화할 수 있는 하드웨어 암호 시스템(280)을 선택적으로 포함할 수 있다. 이와 같이, 하드웨어 암호 시스템(280)은, 액세스 컴퓨팅 장치(210)의 CPU(220) 또는 일실시예에서, 데이터 암호화 및 복호화와 관련되지 않고 임의의 다른 저장 장치와 동일한 방식으로 저장 장치(270)를 취급할 수 있는 액세스 컴퓨팅 장치(210)의 다른 구성 요소에 부담을 주지 않고 그 암호 기능을 실행할 수 있다. 더욱이, 액세스 컴퓨팅 장치(210)가 최대 볼륨 암호화 서비스(237) 등과 같은 관련 암호 성분을 포함하지 않는다면, 연관된 액세스 제어 장치(170)의 저장 관련 암호 정보(175)는 하드웨어 암호 시스템(280)에 의해 관리될 수 있다. 하드웨어 암호 시스템(280)은 액세스 제어 장치(170)의 저장 관련 암호 정보(175)와 거의 동일하게 선택적인 구성 요소임을 표시하기 위해 도 2에서 점선으로 도시되어 있다.

[0046] 그러나 저장 장치(270)의 하드웨어 암호 시스템(280)이 선택적이기는 하지만, 하나 이상의 처리 장치(281) 및 펌웨어(283) 등과 같이 하부 구성 요소로서 도시되어 있는 다른 구성 요소는 하드웨어 암호 시스템의 존재 여부에 무관하게 존재할 수 있다. 보다 구체적으로, 일실시예에서, 처리 장치(281) 및 펌웨어(283)는 예를 들면, 여러 유지 및 통신 작업 등과 같은 적어도 원시 명령어를 독립적으로 처리하는 능력을 저장 장치(270)에 제공할 수 있다. 그러나 다른 실시예에서, 처리 장치(281) 및 펌웨어(283)는 저장 장치에 제공되는 데이터의 암호화 및 컴퓨터 판독 가능 매체(290)로부터 판독되는 데이터의 복호화 등과 같은 암호 기능을 적어도 부분적으로 실행하는 데 이용될 수 있다. 이러한 실시예에서, 처리 장치(281) 및 펌웨어(283)는 적어도 부분적으로 하드웨어 암호 시스템(280)의 일부분으로 간주할 수 있다. 추가하여, 액세스 제어 장치(170)의 처리 장치(171)와 마찬가지로, 저장 장치(270)의 처리 장치(281)는 입력의 집합에 기초하여 그 출력을 조정할 수 있는 제어기 또는 다른 구성 요소를 포함할 수 있다.

[0047] 앞서 제시되어 있는 실시예에서, 액세스 제어 장치(170)의 저장 관련 암호 정보(175)는 저장 장치(270)의 하드웨어 암호 시스템(280)에 의해 참조될 수 있고, 그것에 의해 실행된 암호화 및 복호화를 통지할 수 있다. 일실시예에서, 하드웨어 암호 시스템(280)은 액세스 제어 장치(170)의 저장 관련 암호 정보(175) 및 예를 들면, 액세스 컴퓨팅 장치(210) 또는 다른 유사 암호 시스템에서 실행되는 최대 볼륨 암호화 서비스(237)에 의해 제공되는 것 등과 같은 추가적인 암호 정보를 모두 참조하여 그 암호 기능을 실행할 수 있다.

[0048] 상기 상세히 설명된 방식으로 앞서 제공될 수 있었던 액세스 제어 장치(170)는 도 2의 양방향 통신 점선 화살표로 표시된 바와 같이 저장 장치(270)에 통신 가능하게 접속될 수 있다. 이하에 상세히 설명되는 바와 같이, 액세스 제어 장치(170)와 저장 장치(270) 사이의 이러한 통신 접속은 유선 또는 무선일 수 있고, 액세스 컴퓨팅 장치(210)를 통과하는 것 등과 같이 직접적 또는 간접적일 수 있다.

[0049] 액세스 컴퓨팅 장치(210)는 저장 장치에 적절한 판독 명령어를 전달하는 것에 의해 저장 장치(270)의 데이터(295)를 액세스하도록 시도할 수 있다. 액세스 제어 장치(170)가 저장 장치(270)에 통신 가능하게 접속되지 않았다면, 저장 장치는 일실시예에서, 액세스 컴퓨팅 장치(210)에게 데이터(295)에 대한 액세스를 제공할 수 없다고 통지할 수 있다. 그러나 다른 실시예에서, 액세스 제어 장치(170)의 부재는 저장 장치(270)가 종래의 방식으로 이용될 수 있게 한다. 액세스 제어 장치(170)는 저장 관련 암호 정보(175)를 포함해야 하므로, 이러한 실시예에서 액세스 제어 장치가 저장 장치에 통신 가능하게 결합되지 않았다면, 저장 장치는 암호화된 데이터를 복호화하기 위해서 저장 장치의 하드웨어 암호 시스템(280)에 의해 필요한 저장 관련 암호 정보(175)가 이용 불가능하기 때문에 데이터(295)(이것은 이 실시예에서 암호화된 형태를 가질 것임)를 액세스할 수 없다는 것을 액세스 컴퓨팅 장치(210)에게 통지할 수 있다. 다른 한편으로, 액세스 제어 장치(170)가 저장 장치(270)에 통신

가능하게 결합되었다면, 액세스 제어 장치는 액세스 컴퓨팅 장치(210)에게 데이터(295)에 대한 액세스를 제공하도록 저장 장치(270)를 허용할 것인지 여부에 관하여 결정하거나 그 결정을 수신할 수 있다. 이러한 액세스는, 액세스 제어 장치(170)에 의해 통지받거나 실시되고, 액세스 컴퓨팅 장치(210)가 데이터(295)를 액세스하는 것을 거부하도록 동작하는 처리 장치(281)에 의해 이루어지는 것 등과 같이 명령의 실행을 통해 거부될 수 있다. 이러한 액세스는 추가적으로 또는 그 대신에, 암호화된 데이터를 복호화는 데 필요한 저장 관련 암호 정보(175)에 대한 액세스의 거부를 통해 거부될 수 있다.

[0050] 저장 장치(270)는 적절한 저장 관련 통신 프로토콜을 이용하여 액세스 제어를 구현하는 액세스 제어 장치(170)의 존재에 관해 액세스 컴퓨팅 장치에게 통지할 수 있다. 이하에 추가로 설명되는 바와 같이, 저장 장치(270)는 저장 장치의 저장 매체(290)에 저장된 데이터(295)의 액세스를 시도하는 것에 응답하여 액세스 컴퓨팅 장치(210)에게 에러 메시지를 리턴할 수 있다. 이러한 에러 메시지는 액세스 컴퓨팅 장치(210)에게 통신 가능하게 결합된 액세스 제어 장치(170)의 존재에 관해 표시할 수 있다. 저장 장치(270)와 통신하기 위해 운영 시스템(234)에 의해 로딩되었던 저장 장치 드라이버 스택(238)에 의해 수신될 수 있는 이러한 에러 메시지에 응답하여, 저장 장치 드라이버 스택(238)은 액세스 컴퓨팅 장치(210)가 액세스 제어 장치(170)와 통신할 수 있게 하는 액세스 제어 장치 확장부(239)를 개시하거나 로딩되도록 유도할 수 있다. 액세스 제어 장치 확장부(239)는 DLL(Dynamically Loaded Library module), 프리 로딩 루틴(pre-loaded routine) 또는 임의의 다른 런타임 바운드(run-time bound) 실행 가능 컴퓨터 코드로서 구현될 수 있다.

[0051] 일실시예에서, 도 2의 시스템(200)에 의해 도시된 것 등과 같이, 액세스 컴퓨팅 장치(210)의 액세스 제어 장치 확장부(239)는 액세스 제어 장치(170)와 통신하고 정보를 제공함으로써, 액세스 제어 장치의 처리 장치(171)가 액세스 제어 장치가 제공받았던 액세스 제어 정보(176)에 기초하여 액세스 제어 결정을 내리게 할 수 있다. 예를 들면, 액세스 제어 장치(170)에 의해 요청되고 그것에 제공된 정보는 액세스 컴퓨팅 장치(210) 또는 저장 장치(270)의 식별 정보를 포함할 수 있다. 이러한 식별 정보는 액세스 제어 장치(170)가 액세스 제어 정보(176)에 기초하여, 액세스 컴퓨팅 장치(210) 및 저장 장치(270)가 승인된 개체인지 여부를 결정할 수 있게 한다. 이러한 방식으로, 데이터(295)에 대한 액세스는 보안 구역 내에 있는 것 또는 WAN 액세스가 되지 않는 것들 과 같은 오로지 특정 액세스 컴퓨팅 장치(210)로 한정될 수 있다. 다른 예로서, 신뢰성 및 성능 이유를 위하여, 상술된 저장 호스트 제어기(145)와 유사한 저장 호스트 제어기(245) 등과 같은 제어기의 제조자는, 오로지 특정 종류의 저장 장치만이 자신의 제어기로 이용되도록 요구할 수 있다. 이러한 경우에, 액세스 제어 장치(170)는 액세스 제어 정보(176)의 형태로 연관된 저장 장치(270)가 공동 작동하도록 허용될 수 있는 하나 이상의 제어기의 하나 이상의 식별자를 제공받을 수 있다. 또는 이와 다르게, 액세스 제어 장치(170)는 저장 장치(270) 등과 같은 특정 저장 장치 및 액세스 컴퓨팅 장치(210)의 저장 호스트 제어기(245) 등과 같은 특정 제어기(이들은 서로 공동 작동하도록 허용됨)의 식별자를 제공받을 수 있다. 저장 장치 및 액세스 컴퓨팅 장치가 모두 액세스 제어 정보(176)에 의해 지정된 바와 같이 개별적으로 승인된 개체라고 해도, 데이터(295)에 대한 액세스는 저장 장치(270)가 적절한 액세스 컴퓨팅 장치(210)에 통신 가능하게 접속되었다는 것을 검증하는 방식으로 제한될 수 있다.

[0052] 다른 실시예에서, 액세스 제어 장치(170)는 저장 관련 암호 정보(175)의 다수의 집합을 포함하여, 저장 장치(270) 내에서 암호화된 상태로 저장될 수 있는 데이터(295)의 개별 분할 또는 다른 세그먼트 등이 저장 관련 암호 정보 및 그것에 제공된 액세스를 참조하여 개별적으로 복호화될 수 있다. 이러한 실시예에서, 액세스 컴퓨팅 장치에 의해 제공된 정보는 사용자 이름 및 패스워드 등과 같이, 사용자가 자신을 적절하게 증명하였는지, 액세스 제어 정보(176)에 의해 유지된 승인 목록 내에 있는지 여부를 결정하기 위해 액세스 제어 장치(170)의 처리 장치(171)에 의해 이용될 수 있는 사용자 식별 정보를 포함할 수 있다. 액세스 제어 정보(176)는 특정 사용자에게 있어서, 저장 장치(270)에게 제공될 수 있는 저장 관련 암호 정보(175)가 오로지 사용자가 액세스하도록 허가받은 컴퓨터 판독 가능 매체(290)의 사전 형성된 분할로 정의되는 것 등과 같이 암호화된 데이터의 일부분을 복호화할 수 있다는 것을 지정할 수 있다. 이러한 실시예는 다중 사용자 또는 시간 공유 액세스 컴퓨팅 장치(210)에 있어서 유용할 수 있다.

[0053] 시스템(200)에서 도시된 바와 같이, 액세스 컴퓨팅 장치(210)에 의해 제공되는 정보는 액세스 제어 장치가 프로비저닝 컴퓨팅 장치(110)에 의해 제공받은 액세스 제어 정보(176)로서 액세스 제어 장치(170)의 처리 장치(171)에 의해 고려될 수 있고, 액세스 제어 장치의 처리 장치는 이러한 고려에 기초하여 저장 장치(270)가 액세스 컴퓨팅 장치로부터의 데이터 저장 관련 통신에 대해 의미 있는 응답을 하도록 허용할 것인지 아닌지 결정할 수 있고, 그것에 의해 액세스 컴퓨팅 장치(210)가 컴퓨터 판독 가능 매체(290)에서 데이터(295)를 판독하거나 추가적인 데이터를 기록하도록 허용할 것인지 허용하지 않을 것인지 결정할 수 있다. 일실시예에서, 상술된 바와

같이, 저장 장치(270)가 데이터 저장 관련 통신에 대해 의미 있는 응답을 하도록 허용할 것인지 여부에 관한 결정은 펌웨어(283)로부터의 적절한 명령어를 실행하도록 저장 장치(270)의 처리 장치(281)에게 명령하는 액세스 제어 장치(170)의 처리 장치(171)에 의해 구현될 수 있다. 예를 들어, 처리 장치(171)가 액세스 컴퓨팅 장치(210)는 저장 장치(270)에 데이터를 저장하거나 데이터를 판독하도록 허용되지 않아야 한다고 결정한다면, 처리 장치(171)는 컴퓨터 판독 가능 매체(290)에 데이터를 기록하거나 이미 거기에 저장되어 있는 데이터(295)를 판독하기 원하는 그 요청이 거부되었다는 것을 액세스 컴퓨팅 장치(210)에게 통지하는 펌웨어(283)로부터의 명령어를 실행하도록 처리 장치(281)에게 명령할 수 있다. 추가하여, 펌웨어(283)로부터 실행된 명령어는 적절한 에러 코드 등과 같이 거부에 대한 이유의 표시를 액세스 컴퓨팅 장치(210)에게 제공할 수 있다. 상술되어 있는 다른 실시예에서, 저장 장치(270)가 데이터 저장 관련 통신에 의미 있는 응답을 하도록 허용할 것인지 여부에 대한 결정은 액세스 제어 장치(170)의 처리 장치(171)에 의해서 저장 장치(270)의 하드웨어 암호 시스템(280)의 처리 장치(281)에 대해 저장 관련 암호 정보(175)를 공개하거나 공개하지 않고, 그것에 의해 하드웨어 암호 시스템(280)이 데이터(295)(암호화된 형태로 저장됨)를 복호화하도록 허용하거나 허용하지 않음으로써, 액세스 컴퓨팅 장치(210)에 대한 이러한 데이터의 액세스를 제공하는 것으로 구현될 수 있다. 액세스 제어 장치(170)에 의해 제공된 이러한 액세스 제어는, 저장 장치(270)로부터 저장 관련 암호 정보(175)를 포함하여 액세스 제어 장치(170)를 통신 가능한 접속을 해제하고, 그것에 의해 필수적인 저장 관련 암호 정보를 저장 장치에게 제공하여 저장 장치가 그곳에 저장된 암호화된 데이터를 액세스할 수 있게 하는 임의의 능력에 대한 통신 가능성을 차단함으로써 달성될 수 있는 액세스 불능화(disabling)를 추가할 수 있다.

[0054] 다른 실시예에서, 도 3의 시스템(300)에 의해 도시된 것과 같이, 액세스 제어 장치(170)는 액세스 제어 정보(176)에 의해 통지받은 것 등과 같이 자신의 결정에 기초한 것이 아니라 액세스 제어 장치(170)가 통신 가능하게 결합될 수 있는 허가 컴퓨팅 장치(310)의 결정에 기초하여 액세스 컴퓨팅 장치(210)로부터의 데이터 저장 관련 통신에 의미 있는 응답하도록 저장 장치(270)에게 허용하거나 허용하지 않을 수 있다. 도 3을 참조하면, 시스템(300)은 시스템(200)의 액세스 컴퓨팅 장치(210), 액세스 제어 장치(170) 및 저장 장치(270)를 포함하도록 도시되어 있다. 그러나 추가하여, 시스템(300)은 또한 액세스 컴퓨팅 장치 및 허가 컴퓨팅 장치가 모두 독립적인 네트워크 접속(251, 351)을 각각 유지하게 하는 네트워크(155)를 통한 것 등과 같이 액세스 컴퓨팅 장치(210)에 통신 가능하게 결합될 수 있는 허가 컴퓨팅 장치(310)를 포함한다.

[0055] 시스템(300)으로 도시된 실시예에서, 액세스 제어 장치(170)는 액세스 제어 정보(176)의 일부분으로서, 액세스 컴퓨팅 장치(210)를 통해 허가 컴퓨팅 장치(310)로 향하는 보안 통신 터널(320)을 형성하는 데 이용될 수 있는 액세스 제어 암호 정보(376)를 구비할 수 있다. 상술된 바와 같이, 액세스 컴퓨팅 장치(210)가 저장 장치(270)에 저장된 데이터(295)를 액세스하고자 시도할 때, 저장 장치는 액세스 제어 장치(170)의 존재에 대해 액세스 컴퓨팅 장치에게 통지할 수 있고, 이것은 액세스 컴퓨팅 장치의 운영 시스템(234)의 저장 장치 드라이버 스택(238)이 액세스 컴퓨팅 장치와 액세스 제어 장치 사이에 통신을 가능하게 할 수 있는 액세스 제어 장치 확장부(239)를 로딩하거나 실행될 수 있게 한다. 이러한 통신을 통해서, 액세스 제어 장치(170)는 액세스 컴퓨팅 장치(210)의 액세스 제어 장치 확장부(239)가 액세스 제어 장치로부터 허가 컴퓨팅 장치(310)로 메시지를 전달하고, 반대로 허가 컴퓨팅 장치로부터 액세스 제어 장치로 메시지를 제공하도록 요청할 수 있다. 이러한 방식으로, 액세스 제어 장치(170)는 허가 컴퓨팅 장치(310)와의 보안 통신 터널(320)을 형성할 수 있다.

[0056] 액세스 제어 장치(170)로부터 허가 컴퓨팅 장치(310)로 메시지를 제공하기 위해서, 액세스 제어 장치 확장부(239)는 액세스 컴퓨팅 장치(210)의 네트워크 인터페이스(250)가 허가 컴퓨팅 장치에 대해 통신 접속을 형성하도록 요청할 수 있다. 일실시예에서, 그 네트워크 어드레스 또는 DNS 이름 등과 같은 허가 컴퓨팅 장치(310)의 위치는 액세스 제어 장치(170)의 액세스 제어 정보(176)로부터 액세스 제어 장치 확장부(239)로 제공되고, 그것에 의해 네트워크 인터페이스(250)로 제공될 수 있다. 다른 실시예에서, 허가 컴퓨팅 장치(310)의 위치는 액세스 컴퓨팅 장치(210)에게 이미 알려져 있을 수 있다. 예를 들면, 전형적으로 액세스 컴퓨팅 장치(210) 등과 같은 컴퓨팅 장치가 네트워크(155)와의 네트워크 접속(251)을 형성할 때, 컴퓨팅 장치는 예를 들면, DNS 서버의 어드레스 및 컴퓨팅 장치에 공급하는 라우터의 어드레스를 포함하는 소정 네트워크 정보를 제공받는다. 유사한 방식으로, 상술된 실시예에 따르면 액세스 컴퓨팅 장치(210) 등과 같은 컴퓨팅 장치는, 네트워크(155) 상에서 또는 컴퓨팅 장치가 접속되어 있는 네트워크의 동일 부분 상에서 컴퓨팅 장치에 공급할 수 있는 허가 컴퓨팅 장치(310) 등과 같은 허가 컴퓨팅 장치에 대한 네트워크 어드레스 또는 다른 위치 정보를 구비할 수 있다.

[0057] 액세스 제어 암호 정보(376)는 허가 컴퓨팅 장치(310)의 공용 액세스 키, 허가 컴퓨팅 장치와 액세스 제어 장치(170) 사이의 공유된 비밀 또는 액세스 제어 장치(170)와 허가 컴퓨팅 장치(310)가 PPTP(Point-to-Point Tunneling Protocol) 또는 L2TP(Level 2 Tunneling Protocol)과 유사하거나 동일한 프로토콜을 포함하여 표준

터널링 메커니즘을 통한 것 등과 같은 보안 통신 터널(320)을 형성할 수 있게 하는 임의의 유사 암호 정보를 포함할 수 있다. 당업자에게 알려진 바와 같이, 이러한 터널링 메커니즘은 공유 패스워드 또는 액세스 제어 등과 같은 여러 보안 증명서의 교환에 의지하거나, 케베로스(Kerberos) 또는 라디우스(RADIUS) 서버 등과 같은 독립형 증명자에 의해 제공되는 보안 증명서에 의존할 수 있는데, 이들 일부 또는 전부는 액세스 제어 암호 정보(376)로서 액세스 제어 장치(170)에 제공될 수 있다. 보안 터널(320)을 이용하면, 그 메시지가 액세스 컴퓨팅 장치(210)에 의해 중계되고, 그에 따라 액세스 컴퓨팅 장치에서 실행되는 구성 요소 및 프로세스에게 노출됨에도 불구하고, 허가 컴퓨팅 장치(310)가 별도로 이러한 저장 관련 암호 정보의 제공이 적절하다고 표시하지 않았을 때라면 이러한 구성 요소 및 프로세스는 이러한 메시지의 내용을 이해할 수 없고, 그에 따라 액세스 제어 장치(170)가 저장 관련 암호 정보(175)를 제공할 수 없게 한다. 앞서 표시된 바와 같이, 보안 통신 터널(320)을 형성하는 데 이용되는 증명서 및 다른 정보를 포함할 수 있는 액세스 제어 암호 정보(376)는 제공하는 동안에 프로비저닝 컴퓨팅 장치(110)에 의해 액세스 제어 장치(170)로 제공될 수 있다.

[0058] 일실시예에서, 허가 컴퓨팅 장치(310)는 NAP(Network Access Protection), NAC(Network Admission Control), SNA(Secure Network Access) 또는 다른 유사 기술 등과 같은 기존의 액세스 제어 기술 및 방법과 통합될 수 있다. 예를 들면, 기존의 NAP 서버 컴퓨팅 장치는 업데이트된 악성 프로그램 제거(anti-malware) 소프트웨어, 적용된 운영 시스템 업데이트 및 다른 유사 정보에 의해 정량화된 컴퓨팅 장치의 보안을 미리 인식할 수 있다. 기존의 NAP 서버 컴퓨팅 장치에 의해 결정된 바와 같이 보안의 임계 레벨을 충족하지 않는 컴퓨팅 장치는 마찬가지로 허가 컴퓨팅 장치(310)에 의해 식별될 수 있고, 허가 컴퓨팅 장치는 이러한 컴퓨팅 장치에 통신 가능하게 결합된 저장 장치에 저장 관련 암호 정보(175)를 제공하지 않도록 액세스 제어 장치(170)에게 명령할 수 있다.

[0059] 그러므로 도 3에 도시된 바와 같이, 액세스 제어 장치(170)는 또한 액세스 컴퓨팅 장치(210)에서 실행되는 저장 장치 드라이버 스택(238)의 액세스 제어 장치 확장부(239)와의 통신을 통해서 액세스 컴퓨팅 장치 및 액세스 제어 장치가 현재 통신 가능하게 결합되어 있는 저장 장치(270)와 연관된 특정 정보를 습득할 수 있다. 상술된 바와 같이 액세스 컴퓨팅 장치(210), 액세스 컴퓨팅 장치 그 자체, 저장 호스트 제어기(245), 저장 장치(270) 및 다른 유사 정보를 이용하여 사용자의 식별 정보를 포함할 수 있는 이러한 정보는, 액세스 제어 장치(170)에 의해서 보안 터널(320)을 통해 허가 컴퓨팅 장치(310)로 제공될 수 있다. 이러한 제공된 정보 및 상술된 NAP 정보 등과 같이 이용 가능하게 된 다른 정보에 기초하여, 허가 컴퓨팅 장치(310)는 저장 장치(270)가 액세스 컴퓨팅 장치(210)로부터의 데이터 저장 관련 통신에 대해 의미 있는 응답을 제공하도록 허용할 것인지 여부를 결정할 수 있다. 허가 컴퓨팅 장치(310)로부터 액세스 제어 장치(170)로의 명령어는 도시된 바와 같이 보안 터널(320)을 통해 수신될 수 있다. 일실시예에서, 허가 컴퓨팅 장치(310)로부터의 명령어는 액세스 제어 장치(170)의 처리 장치(171)에 의해 수신될 수 있고, 처리 장치는 상술된 바와 같이 액세스 컴퓨팅 장치(210)로부터의 데이터 저장 관련 통신에 의미 있는 응답을 하거나, 액세스 컴퓨팅 장치(210)로부터의 저장 관련 통신 또는 요청에 대해 적절한 에러 또는 다른 거부로 응답하도록, 펌웨어(283)로부터의 적절한 명령어를 실행하도록 저장 장치(270)의 처리 장치(281)에게 명령할 수 있다. 다른 실시예에서, 허가 컴퓨팅 장치(310)로부터의 명령어는 액세스 제어 장치(170)의 처리 장치(171)에 의해 수신될 수 있고, 처리 장치는 또한 상술된 바와 같이 저장 장치(270)의 처리 장치(281)에게 저장 관련 암호 정보(175)를 제공 또는 거부하여 액세스 컴퓨팅 장치(210)로부터의 데이터 저장 관련 통신에 대해 저장 장치(270)가 의미 있는 응답을 하게 하거나 그것을 방지할 수 있다.

[0060] 일실시예에서, 액세스 컴퓨팅 장치(210)와는 분리되어 있는 독립형 컴퓨팅 장치에서 실행하는 것 대신에, 허가 컴퓨팅 장치(310)에서 실행되는 허가 프로세스는 액세스 컴퓨팅 장치의 보호된 공간 내에서 실행될 수 있다. 이러한 실시예에서 허가 컴퓨팅 장치(310)는 가상 머신이거나 액세스 컴퓨팅 장치(210)에서 실행되는 다른 보호된, 독립된 프로세스일 수 있다. 상술된 실시예에서, 액세스 컴퓨팅 장치(210)가 허가 컴퓨팅 장치(310)로 및 허가 컴퓨팅 장치(310)로부터 메시지를 전달하였으므로, 대신에 허가 컴퓨팅 장치는 액세스 제어 장치(170)에 변화를 주지 않고 액세스 컴퓨팅 장치에서 컴퓨터 실행 가능 명령어를 실행하는 것을 통해 구현될 수 있다.

[0061] 도 4를 참조하면, 도 2 및 도 3에서 점선 통신 화살표로 도시되어 있는 것 등과 같은 액세스 제어 장치(170)와 저장 장치(270) 사이의 통신 접속이 보다 상세하게 도시되고 설명되어 있다. 일실시예에서, 시스템(400)으로 나타낸 바와 같이, 저장 장치(270)는 오로지 상술된 하드웨어 암호 시스템(280) 및 컴퓨터 판독 가능 매체(290)만을 포함하는 것이 아니라, 액세스 제어 장치 인터페이스(410)도 포함할 수 있다. 액세스 제어 장치 인터페이스(410)는 오로지 예시로서 저장 장치(270) 상의 슬롯 또는 커넥터일 수 있으므로, 액세스 제어 장치(170)는 액세스 제어 장치 인터페이스(410)에 삽입 또는 접속되었을 때 액세스 제어 장치(170)가 저장 장치(270)의 규모를 실질적으로 변경하지 않도록 물리적으로 삽입되거나, 접속될 수 있다. 이러한 경우에, 저장 장치(270)는 상

술된 바와 같이, 액세스 제어 장치가 없는 유사한 종류의 임의의 다른 저장 장치에서와 마찬가지로 액세스 컴퓨팅 장치(210) 등과 같은 컴퓨팅 장치에 의해 이용될 수 있다. 예를 들면, 저장 장치(270)가 표준 하드 디스크 드라이브 크기에 따르도록 설계되었다면, 액세스 컴퓨팅 장치(210)는 액세스 제어 장치(170)가 물리적으로 접속되어 있는 저장 장치(270)를 내부 하드 디스크 드라이브로서 이용할 수 있게 되고, 액세스 제어 장치의 존재 또는 부재는 그러한 사용을 저해하는 저장 장치(270)의 물리적 치수 변형을 발생시키지 않을 것이다.

[0062] 다른 예로서, 액세스 제어 장치(170)는 휴대 전화에서 통상적으로 이용되는 것 등과 같은 GSM(Global System for Mobile) 통신 SIM(Subscriber Identity Module)의 형태를 가질 수 있다. 이러한 경우에, 액세스 제어 장치 인터페이스(410)는 또한 전형적으로 휴대 전화 내에 포함되는 GSM SIM 인터페이스일 수 있다. 액세스 제어 장치(170) 및 액세스 제어 장치 인터페이스(410)의 물리적 형태 인자는 모두 통상적으로 사용되고 결과적으로 저렴하기 때문에 이러한 실시예는 비용면에서의 이점을 제공할 수 있다.

[0063] 또 다른 예로서, 액세스 제어 장치(170)는 대응하는 액세스 제어 장치 인터페이스(410) 등과 마찬가지로 USB(Universal Serial Bus) 커넥터 등과 같은 공통 커넥터를 포함할 수 있다. 상술된 바와 같은 GSM SIM 실시예에서와 같이, USB 커넥터는 마찬가지로 그 편재성(ubiquity)에 기인하여 비용면에서의 이점을 제공한다. 이러한 실시예에서, 이하에 설명된 액세스 제어 장치(170)와 하드웨어 암호 시스템(280) 사이의 통신은 공지된 USB 통신 프로토콜을 통해 실행될 수 있다.

[0064] 그러나 액세스 제어 장치(170)가 반드시 저장 장치에 통신 가능하게 접속된 저장 장치(270)에 물리적으로 접속되어야 하는 것은 아니다. 상술된 실시예는 액세스 제어 장치(170)와 저장 장치(270) 사이에 물리적 접속을 제공하여 저장 장치의 공통 종류 인터페이스를 거쳐 임의의 명령어 또는 암호 정보(175)를 처리 장치(281)로 전달하는 것을 방지한다. 이러한 방식으로, 액세스 제어 장치(170) 및 저장 장치(270)의 하드웨어 설계는 처리 장치(171)에 의해 제공된 명령어 또는 저장 관련 암호 정보(175)가 외부 개체에 의해 획득될 수 없도록 보장할 수 있다.

[0065] 다른 실시예에서, 처리 장치(171)에 의해 처리 장치(281)로 제공된 명령어 및 저장 관련 암호 정보(175)는 저장 장치(270)의 외부 통신 인터페이스를 거쳐 적어도 그 일부분이 전달됨에도 불구하고 보안을 유지할 수 있다. 따라서 시스템(450)에 도시된 바와 같이, 액세스 제어 장치(170)와 저장 장치(270)의 물리적 분리에도 불구하고 액세스 컴퓨팅 장치(210)를 통해 액세스 제어 장치(170)와 저장 장치(270) 사이에 통신 접속이 형성될 수 있다. 도시된 바와 같이, 시스템(450)은 액세스 컴퓨팅 장치(210), 액세스 제어 장치(170) 및 저장 장치(270)를 포함할 수 있고, 액세스 제어 장치 및 저장 장치는 모두 액세스 컴퓨팅 장치에 독립적으로 접속된다. 액세스 컴퓨팅 장치(210), 액세스 제어 장치(170) 및 저장 장치(270)가 별개의 물리적 개체로 도시되어 있는 시스템(450)의 일례에도 불구하고, 이러한 물리적 분리가 필수적인 것은 아니다. 예를 들면, 저장 장치(270)는 내부 하드 디스크 드라이브의 형태인 것 등과 같이 액세스 컴퓨팅 장치(210)에 대해 내부적으로 접속될 수 있다. 액세스 제어 장치(170)는 유선 및 무선 인터페이스를 모두 포함하는 유명한 인기 있는 주변 또는 저장 인터페이스 등과 같은 액세스 컴퓨팅 장치(210)의 외부 인터페이스에 접속될 수 있다. 이러한 실시예에서, 액세스 제어 장치(170)와 저장 장치(270) 사이의 통신은 액세스 컴퓨팅 장치(210)의 저장 장치 드라이버 스택(238)에 의해 중계될 수 있고 그 자체의 메커니즘을 통해, 또한 액세스 제어 장치 확장부(239)를 통해서 액세스 제어 장치 및 저장 장치 모두와 통신할 수 있다.

[0066] 도 5를 참조하면, 액세스 컴퓨팅 장치(210)와 액세스 제어 장치(170) 사이의 예시적인 통신 교환은 시스템(500)을 참조하여 보다 상세하게 설명되어 있다. 도 5에 도시된 바와 같이, 시스템(500)은 액세스 제어 장치(170), 저장 장치(270), 액세스 컴퓨팅 장치(210), 및 선택적으로 허가 컴퓨팅 장치(310)를 포함하는 상술된 시스템(200, 300)과 동일한 기본 구성 요소를 포함할 수 있다. 먼저, 통신(510)에 의해 표시된 바와 같이, 액세스 컴퓨팅 장치(210) 및 보다 구체적으로 액세스 컴퓨팅 장치의 운영 시스템(234)(도시하지 않음)의 저장 장치 드라이버 스택(238)은 예를 들면, 판독 요청, 초기화 요청 또는 다른 유사 액세스 요청을 발행하는 것 등에 의해 저장 장치(270)의 데이터 저장 관련 요청을 실행할 수 있다. 데이터 저장 관련 요청(510)에 응답하여, 저장 장치는 에러 코드를 포함하는 에러 통신(520)을 제공할 수 있다. 당업자에게 알려진 바와 같이, 저장 장치 드라이버 스택(238)에 의해 실행되는 것 등과 같은 저장 장치와의 통신은 에러 코드의 형태로 에러 통신을 제공할 수 있고, 여기에서 각각의 코드는 저장 장치(270)의 일부분에서 특정한 에러 또는 에러의 종류를 나타낸다. 일 실시예에서, 저장 장치가 액세스 제어 장치(170)에 통신 가능하게 결합되어 있다는 것을 나타낼 수 있고, 통신 가능하게 결합된 액세스 제어 장치가 예를 들면, 처리 장치(281)에게 그와 같이 하도록 명령하거나 요청된 데이터를 복호화하는 데 필요한 저장 관련 암호 정보(175)를 제공하는 것 등에 의해서 데이터 저장 요청(510)에 대해 의미 있는 응답을 제공하도록 저장 장치(270)에서 허가받지 않았기 때문에 데이터(295)를 액세스하려는 시도

가 실패하였다는 것을 더 나타낼 수 있는 통신(520)의 일부분으로서, 에러 코드는 저장 장치(270)에 의해 저장 장치 드라이버 스택(238)으로 제공될 수 있다.

[0067] 이러한 에러 코드에 대한 응답으로, 저장 장치 드라이버 스택(238)은 동작(530)에 표시된 바와 같이, 액세스 제어 장치 확장부(239)를 로딩하거나, 로딩되도록 유도하거나 실행되게 할 수 있다. 상술된 바와 같이, 액세스 제어 장치 확장부(239)는 이러한 액세스 제어 장치가 오로지 저장 장치를 통한 것 등과 같이 컴퓨팅 장치에 간접적으로 통신 가능하게 결합된 때를 포함하여, 액세스 제어 장치(170) 등과 같은 액세스 제어 장치와 통신하도록 구성된 컴퓨터 실행 가능 명령어를 포함할 수 있다. 액세스 제어 장치 확장부(239)가 로딩되면, 액세스 제어 장치(170)에 대해 통신(540) 등과 같은 직접 통신될 수 있다. 일실시예에서, 통신(540)은 통상적으로 저장 장치(270)로 향하는 것 등과 같은 기록 커맨드를 포함할 수 있지만, 기록 커맨드는 저장 장치에게 통신이 액세스 제어 장치(170)로 향한다는 것을 표시할 수 있는 어드레스 또는 어드레스의 범위를 지정할 수 있다. 따라서 도 5에 도시된 바와 같이, 액세스 제어 장치 확장부(239)로부터의 통신(540)은 먼저 저장 장치(270)로 제공될 수 있고, 지정되어 있는 어드레스에 기초하거나 어드레스의 범위에 기초하여 저장 장치는 액세스 제어 장치(170)에 통신(540)을 추가적으로 제공할 수 있다.

[0068] 액세스 제어 장치(170)는 먼저 액세스 제어 장치에 의해 저장 장치(270)로 제공된 후, 저장 장치로부터 저장 장치 드라이버 스택(238)으로 제공되는 것 등에 의해 액세스 제어 장치 확장부(239)로 다시 전달될 수 있는 응답 통신(550)을 제공할 수 있다. 저장 장치 드라이버 스택(238)은 응답(550)을 수신하면, 그것을 액세스 제어 장치 확장부(239)를 위한 적절한 응답인 것으로 인식할 수 있고, 액세스 제어 장치 확장부를 응답하도록 지시할 수 있다. 상술된 바와 같이, 몇몇 실시예에서, 응답(550) 등과 같은 응답은, 액세스 제어 장치 확장부(239)가 허가 컴퓨팅 장치(310)에 대한 응답(550) 내에 포함될 수 있는 소정의 데이터와 함께 전달되도록 요청할 수 있다. 이러한 경우에, 액세스 제어 장치 확장부(239)는 예를 들면, 네트워크 인터페이스(250)와 함께 액세스 컴퓨팅 장치(210)에서 실행되는 관련 네트워크 프로세스가 요청(560)에 의해 표시된 바와 같이 허가 컴퓨팅 장치(310)에 대한 통신 접속을 형성하도록 요청할 수 있다. 그것에 의해 액세스 제어 장치 확장부(239)는 액세스 제어 장치(170) 및 허가 컴퓨팅 장치(310) 모두로 또한 이들로부터 데이터를 제공함으로써, 액세스 제어 장치 및 허가 컴퓨팅 장치가 보안 통신 터널(320)을 형성할 수 있게 한다.

[0069] 도 6을 참조하면, 흐름도(600)는 도 1의 시스템(100)에 도시되고 상술되어 있는 예시적인 프로비저닝 컴퓨팅 장치(110)에 의해 실행된 것 등과 같이 액세스 제어 장치(170)의 예시적인 공급에 대한 추가적인 설명을 제공한다. 흐름도(600)에서 확인되는 바와 같이, 먼저 단계(610)에서, 액세스 제어 장치(170) 등과 같은 액세스 제어 장치의 공급이 개시될 수 있다. 단계(610)의 공급 개시는 프로비저닝 컴퓨팅 장치에 통신 가능하게 결합된 액세스 제어 장치의 검출에 응답하는 것 등과 같이 자동화된 개시이거나, 프로비저닝 컴퓨팅 장치에서 실행되는 하나 이상의 프로세스에 의해 제공될 수 있는 적절한 사용자 인터페이스를 통한 것 등과 같이 수동 개시 공급 또는 사용자 개시 공급일 수 있다. 그 후에 단계(620)에서, 공급된 액세스 제어 장치가 허가 컴퓨팅 장치와 함께 이용될 것인지 여부, 또는 독립 기반으로 액세스 제어 결정을 실행하게 될 것인지 여부에 관한 결정이 이루어질 수 있다. 단계(620)에서 공급된 액세스 제어 장치가 허가 컴퓨팅 장치와 함께 사용되지 않을 것이라고 결정된다면, 단계(630)에서, 액세스 제어 장치는 액세스 제어 장치가 통신 가능하게 결합되어 있는 저장 장치의 데이터 관련 능력에 대한 액세스가 승인되는 사용자, 컴퓨팅 장치, 저장 장치, 저장 호스트 제어기 또는 그 조합 등과 같은 개체의 식별 정보를 포함할 수 있는 액세스 제어 정보를 공급받을 수 있다. 이와 다르게, 단계(620)에서 공급받은 액세스 제어 장치가 허가 컴퓨팅 장치와 함께 사용될 것이라고 판정되면, 단계(640)에서 액세스 제어 장치는 액세스 제어 장치가 상술된 방식 등에 의해 액세스 컴퓨팅 장치를 통해 허가 컴퓨팅 장치와 보안 통신 터널을 형성하게 하는 액세스 제어 암호 정보를 포함하는 액세스 제어 정보를 공급받을 수 있다.

[0070] 액세스 제어 장치가 단계(630)에서 독립형 액세스 제어 동작을 공급받던지, 아니면 단계(640)에서 허가 컴퓨팅 장치와의 상호 작용을 공급받던지에 무관하게, 이 모든 경우에 처리는 점선으로 경계가 그려져 선택적임을 나타내도록 도시된 선택적인 단계(650)로 진행될 수 있고, 여기에서 액세스 제어 장치는 액세스 제어 장치가 통신 가능하게 결합된 저장 장치에 의해 사용되어 저장 장치에 저장되어 있거나 저장될 데이터를 암호화 또는 복호화할 수 있는 저장 관련 암호 정보를 공급받을 수 있다. 일실시예에서, 단계(650)에서 저장 관련 암호 정보의 공급은, 액세스 제어 장치와 통신하는 각각의 후속 저장 장치가 다음의 물리적 액세스 제어를 획득할 수 있고, 그것을 사용 중인 것으로 표시할 수 있게 하는 예를 들면, 물리적 액세스 제어의 다수의 집합을 액세스 제어 장치에 공급할 수 있다. 이러한 방식으로, 단일 액세스 제어 장치는 다수의 저장 장치에 의해 공유되거나 다수의 저장 장치와 함께 활용될 수 있다. 단계(650)에서 저장 관련 암호 정보가 선택적으로 액세스 제어 장치에 공급

되면, 도시된 바와 같이 관련 처리는 단계(660)에서 종료될 수 있다.

[0071] 도 7을 참조하면, 상술되어 있는 예시적인 액세스 컴퓨팅 장치(210) 등과 같은 액세스 컴퓨팅 장치의 예시적인 동작을 추가적으로 나타내는 흐름도(700)가 도시되어 있다. 흐름도(700)를 참조하면, 먼저 도시된 바와 같이 단계(705)에서, 액세스 컴퓨팅 장치는 액세스 요청 등과 같은 데이터 저장 관련 요청을 액세스 컴퓨팅 장치가 통신 가능하게 결합되어 있는 저장 장치에 발행할 수 있다. 단계(705)에서 이러한 데이터 저장 관련 요청에 응답하여, 액세스 컴퓨팅 장치는 단계(710)에서 액세스된 저장 장치가 액세스 제어 장치에 통신 가능하게 결합되어 있다는 것을 나타내는 에러를 수신할 수 있다. 이러한 에러가 단계(710)에서 수신되지 않으면, 액세스 컴퓨팅 장치는 단계(715)에서 통상적인 방식으로 저장 장치를 활용하도록 진행될 수 있다. 다음에 관련 처리는 단계(760)에서 종료될 수 있다.

[0072] 단계(710)에서 저장 장치가 액세스 제어 장치에 통신 가능하게 결합되어 있다는 것을 나타내는 에러를 액세스 컴퓨팅 장치가 저장 장치로부터 수신하면, 액세스 컴퓨팅 장치는 단계(720)에서 액세스 제어 장치 확장부를 로딩할 수 있고, 상술된 바와 같이, 액세스 제어 장치와 통신하기 위해 액세스 제어 장치 확장부를 이용할 수 있다. 단계(725)에서, 액세스 제어 장치가 정보를 요청하였는지 여부에 대한 결정이 이루어질 수 있다. 액세스 제어 장치가 정보를 요청하였다면, 단계(730)에서 요청된 정보가 제공될 수 있다. 상술된 바와 같이, 이러한 요청된 정보는 액세스 컴퓨팅 장치의 식별 정보, 이러한 컴퓨팅 장치를 이용하는 사용자, 저장 장치를 액세스하는 저장 호스트 제어기의 식별 정보 및 저장 장치 자체의 식별 정보를 포함할 수 있다. 또한 상술된 바와 같이, 이러한 식별 정보는 패스워드 또는 다른 보안 메커니즘을 통해 인증될 수 있고, 이러한 경우에 단계(730)에서 제공된 요청된 정보는 단계(725)에서 액세스 제어 장치에 의해 제공될 수 있는 요구에 대한 패스워드 또는 다른 응답을 포함할 수 있다. 요청된 정보가 단계(730)에서 제공되면, 처리는 단계(725)로 되돌아가서 액세스 제어 장치로부터의 추가 정보 요청을 대기할 수 있다.

[0073] 단계(725)에서 액세스 제어 장치가 임의의 정보를 요청하지 않으면, 처리는 단계(735)로 진행될 수 있고, 액세스 제어 장치가 허가 컴퓨팅 장치에 대한 접속을 요청하였는지 여부를 결정할 수 있다. 단계(735)에서 이러한 접속이 요청되지 않았다면, 관련 처리는 단계(760)에서 종료될 수 있다. 그러나 단계(735)에서, 이러한 접속이 요청되었다면, 단계(740)에서 요청하는 컴퓨팅 장치는 상기 내용에서 설명된 방식 등으로 허가 컴퓨팅 장치와의 접속을 형성할 수 있다. 그 후에 단계(745)에서 액세스 제어 장치와 허가 컴퓨팅 장치 사이의 데이터 교환은 또한 상술된 바와 같은 액세스 컴퓨팅 장치에 의해 촉진될 수 있다.

[0074] 단계(750)에서, 액세스 제어 장치가 허가 컴퓨팅 장치에 대한 접속을 종료하도록 요청하였는지 결정하는 검사가 이루어질 수 있다. 이러한 요청이 이루어지지 않았다면, 처리는 단계(745)로 되돌아가고, 액세스 제어 장치와 허가 컴퓨팅 장치 사이에서 데이터 교환이 계속될 수 있다. 그러나 단계(750)에서 액세스 제어 장치가 허가 컴퓨팅 장치에 대한 접속이 종료되도록 요청하였다면, 단계(755)에서 접속은 종료되고 관련 처리는 단계(760)에서 종료될 수 있다.

[0075] 상술된 설명으로부터 확인되는 바와 같이, 저장 장치에 대한 액세스를 제어할 수 있는 액세스 제어 장치가 제공되었다. 본 명세서에 설명된 청구 대상의 여러 가능한 변경을 고려하여, 본 발명은 모든 이러한 실시예를 이하의 청구항 및 그 등가물의 범주에 속할 수 있는 것으로 청구한다.

부호의 설명

[0076] 100: 시스템

110: 프로비저닝 컴퓨팅 장치

120: 중앙 처리 장치 121: 시스템 버스

130: 시스템 메모리

131: 판독 전용 메모리 132: 랜덤 액세스 메모리

133: 기본 입/출력 시스템(BIOS)

134: 운영 시스템 135: 프로그램 모듈

136: 프로그램 데이터 137: 최대 볼륨 암호화 서비스

138: 저장 장치 드라이버 스택

139: 액세스 제어 장치 확장부

140: 비휘발성 메모리 인터페이스 145: 저장 호스트 제어기

141, 146, 147: 하드 디스크 저장 장치

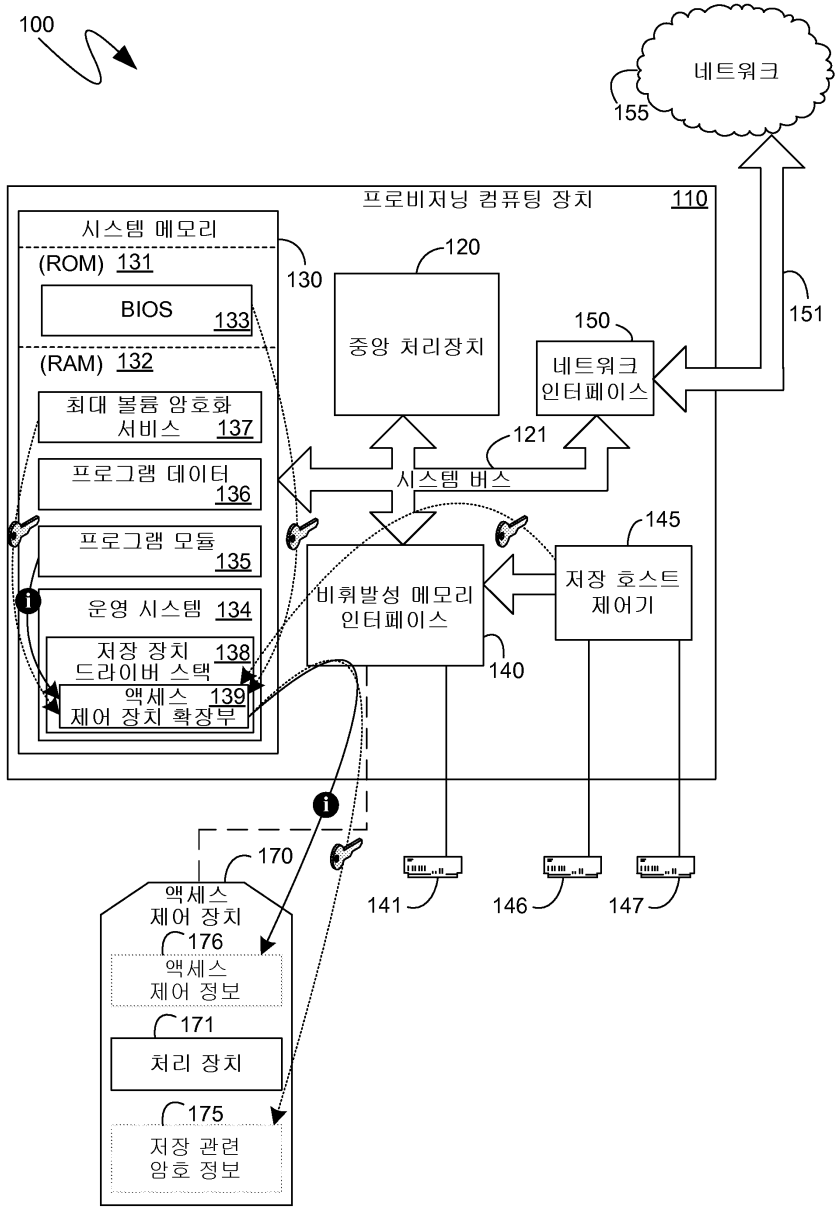
150: 네트워크 인터페이스 또는 어댑터

151: 범용 네트워크 접속 155: 네트워크

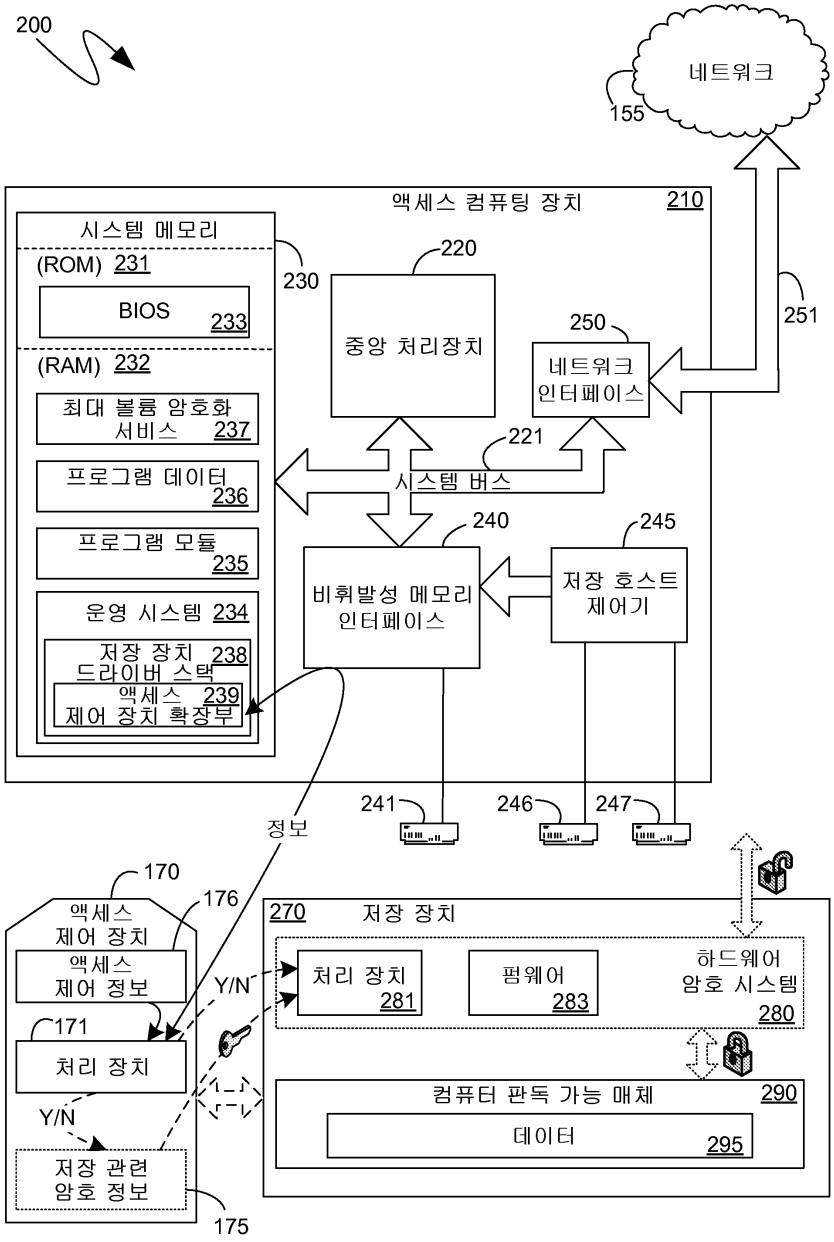
170: 액세스 제어 장치

도면

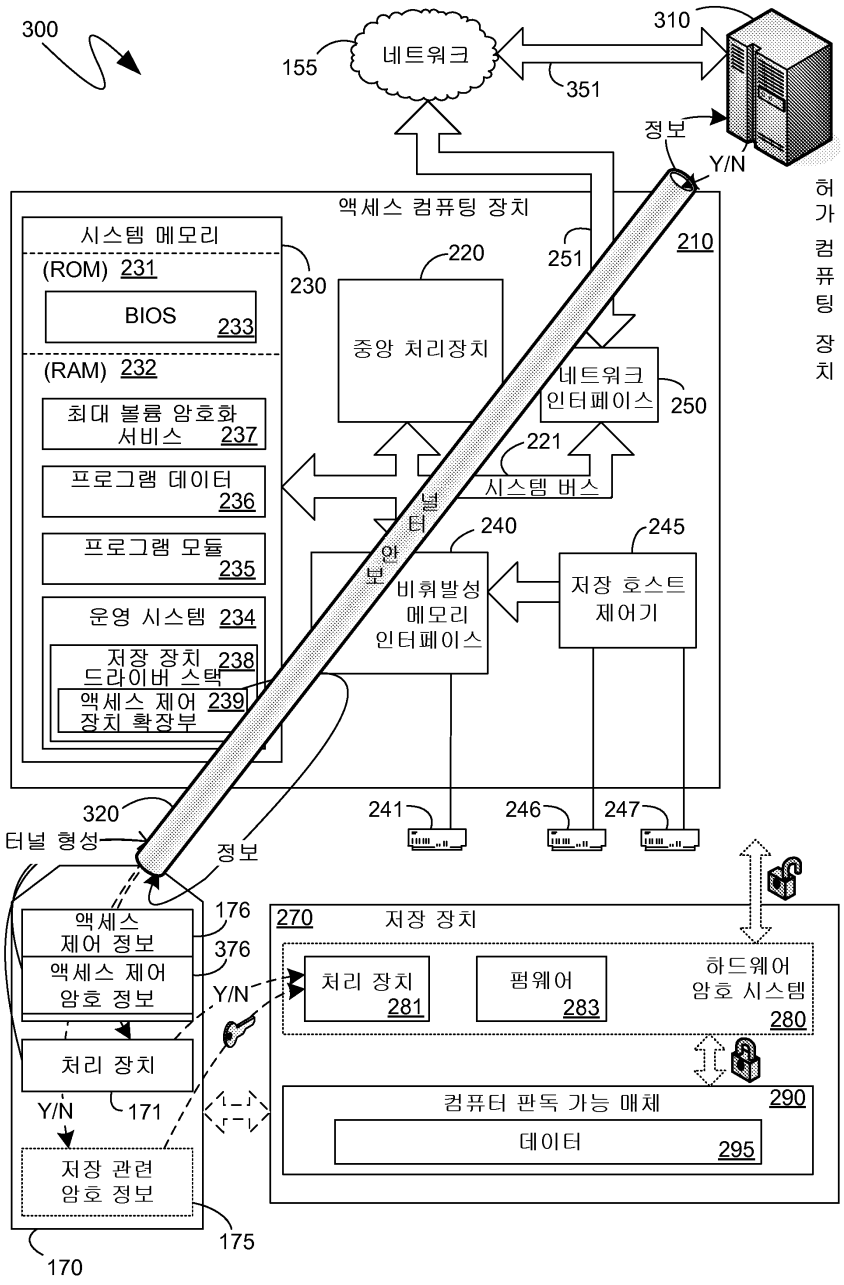
도면1



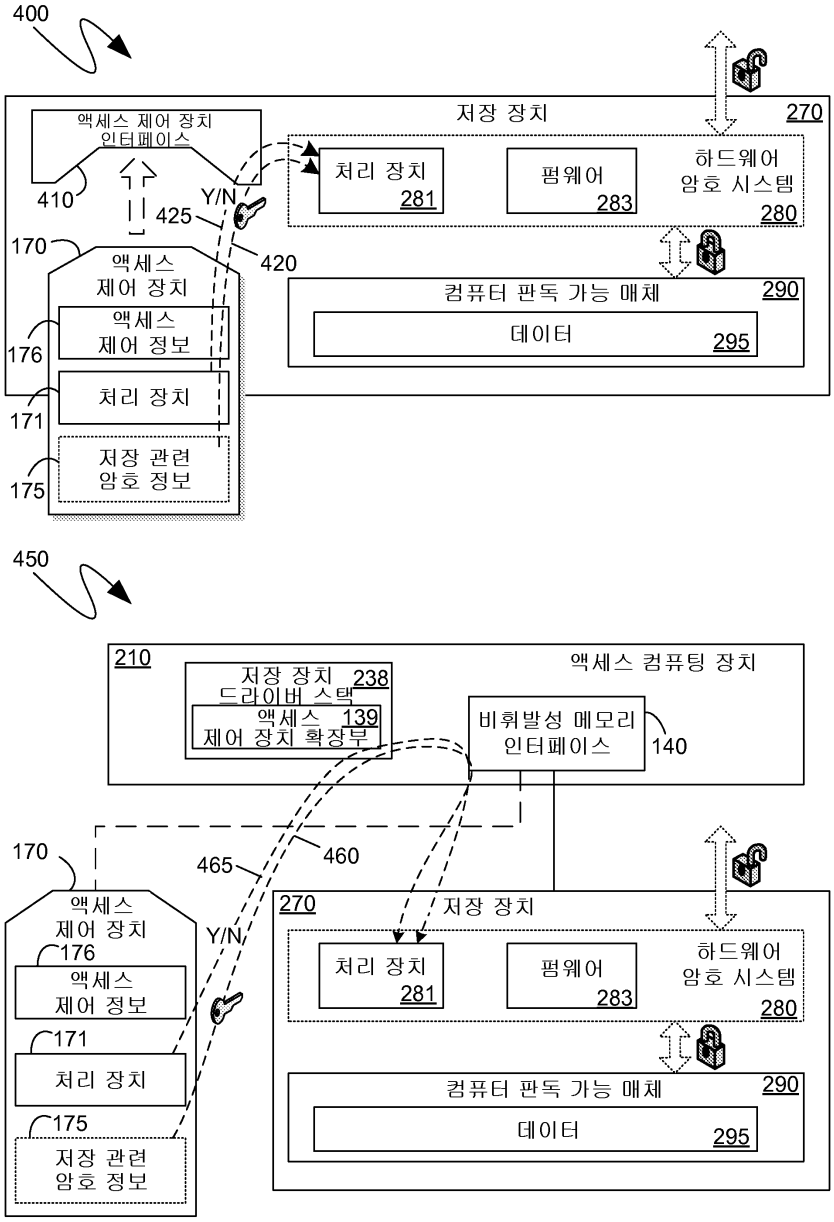
도면2


200
네트워크
155
액세스 컴퓨팅 장치
210
시스템 메모리
(ROM) 231
BIOS
233
(RAM) 232
최대 볼륨 암호화 서비스 237
프로그램 데이터 236
프로그램 모듈 235
운영 시스템 234
저장 장치 드라이버 스택 238
액세스 제어 장치 확장부 239
230
220
중앙 처리장치
250
네트워크 인터페이스
251
221
시스템 버스
240
비휘발성 메모리 인터페이스
245
저장 호스트 제어기
241
246
247
정보
170
액세스 제어 장치
176
액세스 제어 정보
171
처리 장치
Y/N
Y/N
저장 관련 암호 정보
175
270
저장 장치
처리 장치 281
펌웨어 283
하드웨어 암호 시스템 280
컴퓨터 판독 가능 매체
290
데이터
295

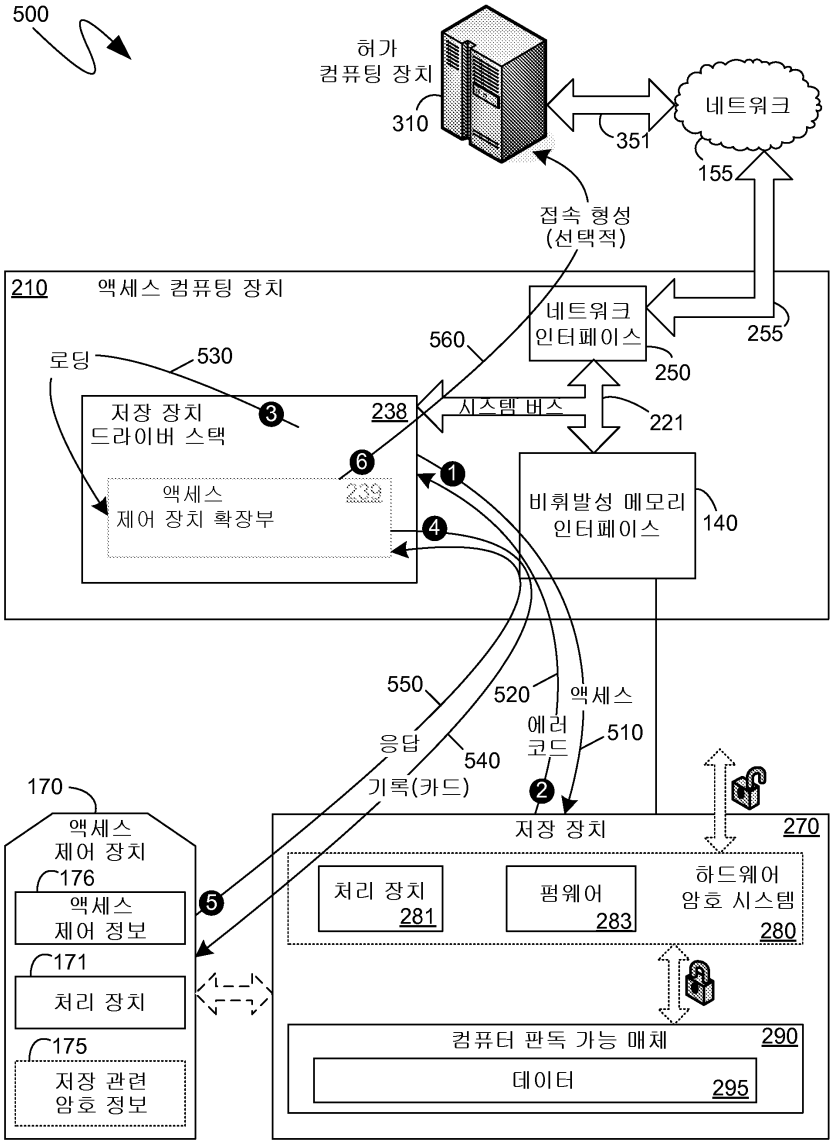
도면3


300
155
네트워크
310
351
정보
Y/N
허가 컴퓨팅 장치
액세스 컴퓨팅 장치
210
시스템 메모리
(ROM) 231
BIOS 233
(RAM) 232
최대 볼륨 암호화 서비스 237
프로그램 데이터 236
프로그램 모듈 235
운영 시스템 234
저장 장치 238 드라이버 스택
액세스 제어 239 장치 확장부
230
220
중앙 처리장치
251
네트워크 인터페이스
250
221
시스템 버스
터널
안보
240
비휘발성 메모리 인터페이스
245
저장 호스트 제어기
241
246
247
320
터널 형성
정보
176
액세스 제어 정보
376
액세스 제어 암호 정보
Y/N
처리 장치
Y/N
171
저장 관련 암호 정보
175
170
270
저장 장치
처리 장치 281
펌웨어 283
하드웨어 암호 시스템 280
290
컴퓨터 판독 가능 매체
데이터 295

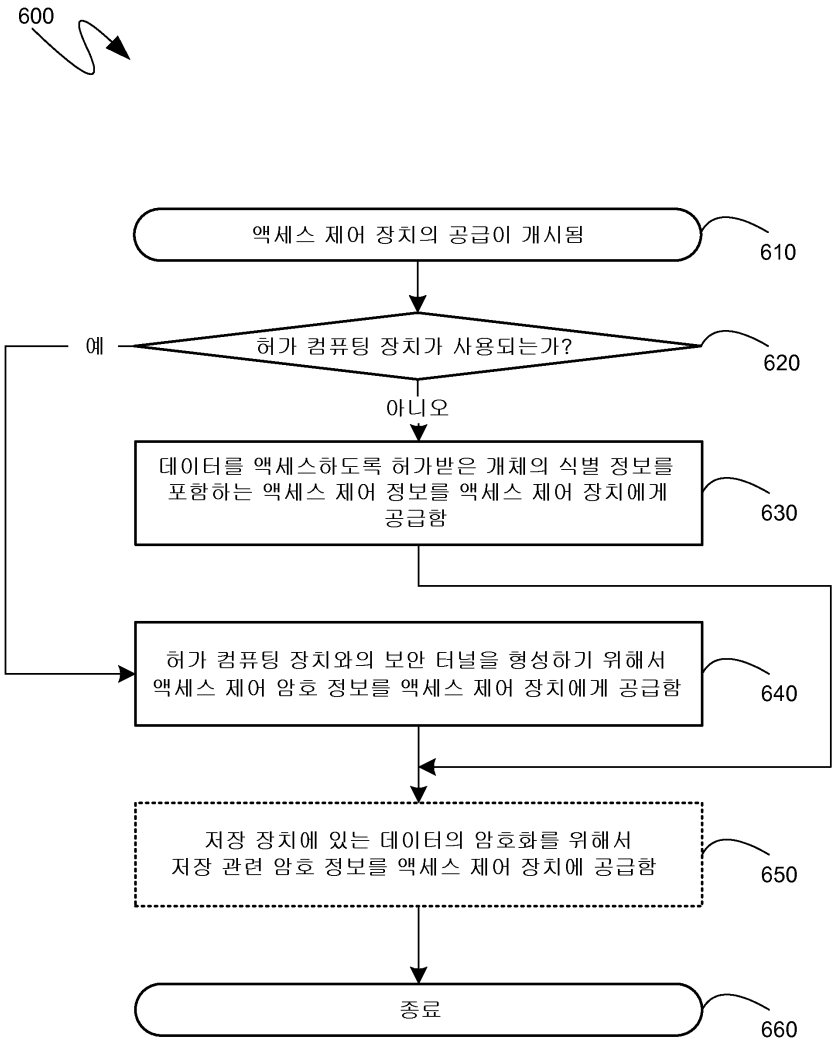
도면4


400
액세스 제어 장치 인터페이스
410
425
Y/N
저장 장치
270
처리 장치 281
펌웨어 283
하드웨어 암호 시스템 280
420
170
액세스 제어 장치
176
액세스 제어 정보
171
처리 장치
175
저장 관련 암호 정보
컴퓨터 판독 가능 매체
290
데이터 295
450
210
액세스 컴퓨팅 장치
저장 장치 238
드라이버 스택
액세스 139 제어 장치 확장부
비휘발성 메모리 인터페이스
140
460
465
170
액세스 제어 장치
176
액세스 제어 정보
171
처리 장치
175
저장 관련 암호 정보
Y/N
270
저장 장치
처리 장치 281
펌웨어 283
하드웨어 암호 시스템 280
컴퓨터 판독 가능 매체
290
데이터 295

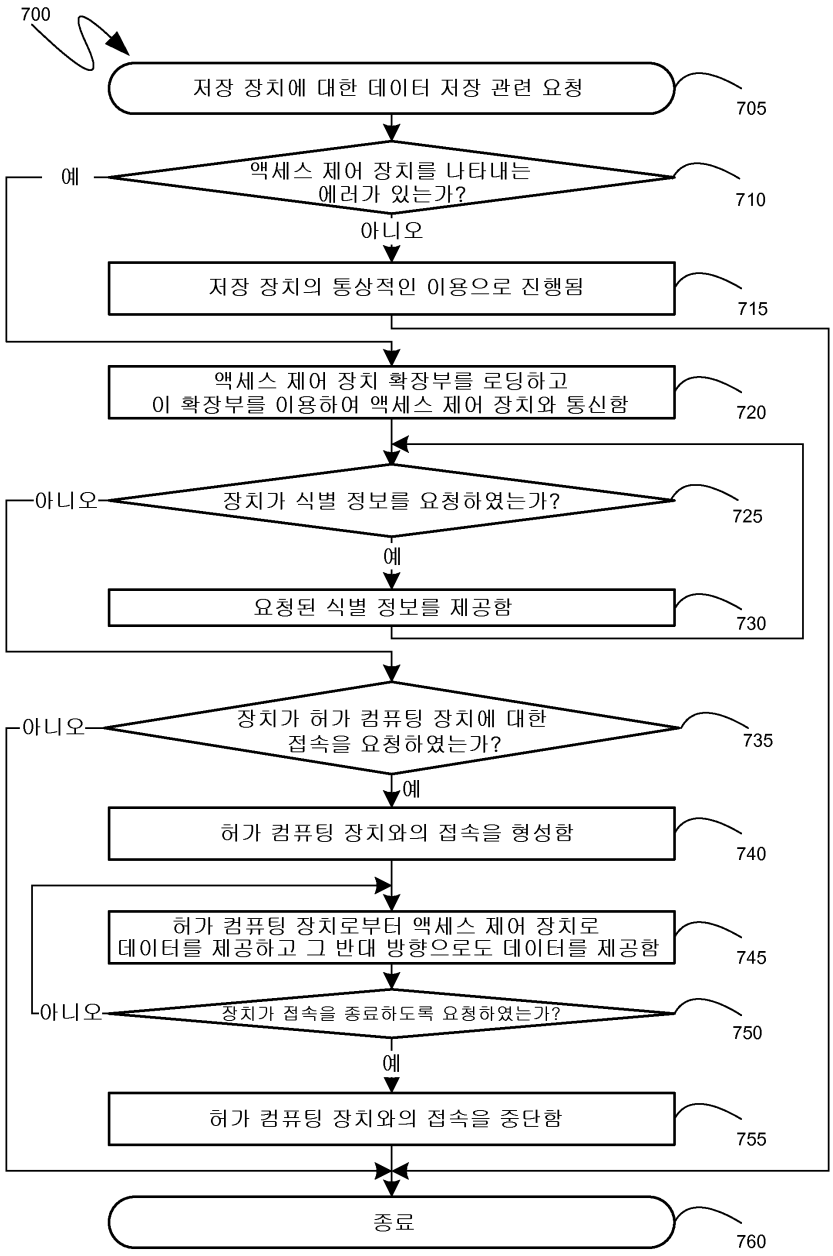
도면5


500
허가
컴퓨팅 장치
310
351
네트워크
155
접속 형성
(선택적)
210
액세스 컴퓨팅 장치
네트워크
인터페이스
250
255
560
로딩
530
저장 장치
드라이버 스택
238
시스템 버스
221
액세스
제어 장치 확장부
239
비휘발성 메모리
인터페이스
140
550
520
액세스
에러
코드
510
응답
540
기록(카드)
170
액세스
제어 장치
176
액세스
제어 정보
171
처리 장치
175
저장 관련
암호 정보
저장 장치
270
처리 장치
281
펌웨어
283
하드웨어
암호 시스템
280
컴퓨터 판독 가능 매체
290
데이터
295

도면6


600
액세스 제어 장치의 공급이 개시됨
610
허가 컴퓨팅 장치가 사용되는가?
620
예
아니오
데이터를 액세스하도록 허가받은 개체의 식별 정보를 포함하는 액세스 제어 정보를 액세스 제어 장치에게 공급함
630
허가 컴퓨팅 장치와의 보안 터널을 형성하기 위해서 액세스 제어 암호 정보를 액세스 제어 장치에게 공급함
640
저장 장치에 있는 데이터의 암호화를 위해서 저장 관련 암호 정보를 액세스 제어 장치에 공급함
650
종료
660

도면7


700
저장 장치에 대한 데이터 저장 관련 요청
705
액세스 제어 장치를 나타내는 에러가 있는가?
710
예
아니오
저장 장치의 통상적인 이용으로 진행됨
715
액세스 제어 장치 확장부를 로딩하고 이 확장부를 이용하여 액세스 제어 장치와 통신함
720
장치가 식별 정보를 요청하였는가?
725
아니오
예
요청된 식별 정보를 제공함
730
장치가 허가 컴퓨팅 장치에 대한 접속을 요청하였는가?
735
아니오
예
허가 컴퓨팅 장치와의 접속을 형성함
740
허가 컴퓨팅 장치로부터 액세스 제어 장치로 데이터를 제공하고 그 반대 방향으로도 데이터를 제공함
745
장치가 접속을 종료하도록 요청하였는가?
750
아니오
예
허가 컴퓨팅 장치와의 접속을 중단함
755
종료
760