(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년09월30일
(11) 등록번호 10-1069500
(24) 등록일자 2011년09월26일

(51) Int. Cl.
H04L 9/32 (2006.01)
(21) 출원번호 10-2008-0090498
(22) 출원일자 2008년09월12일
심사청구일자 2008년09월12일
(65) 공개번호 10-2010-0031408
(43) 공개일자 2010년03월22일
(56) 선행기술조사문헌
KR1020050085015 A*
KR1020070111603 A*
KR1020080050040 A*
US20070180449 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 효자동 산31 포항공과대학교내
(72) 발명자
박찬익
경상북도 포항시 남구 지곡동 교수아파트 9-1503
박우람
경상북도 포항시 남구 효자동 산31 남자기숙사 11-112
(74) 대리인
특허법인이상

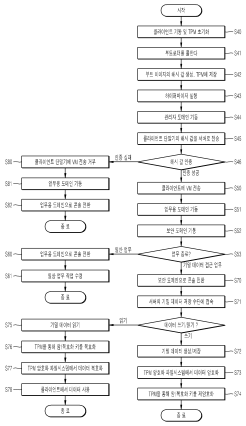
전체 청구항 수 : 총 6 항 심사관 : 이형일

(54) 네크워크 시스템에서 가상화 및 신뢰 플랫폼 모듈을 이용한데이터 보안 처리 방법 및 기록매체

(57) 요 약

본 발명은 가상화(Virtualization) 및 신뢰 플랫폼 모듈 기술을 기반으로 하여 기밀 데이터가 외부로 유출되는 것을 방지하는 데이터 방화벽(Data Firewall) 보안 방법이다. 데이터 서버의 기밀 데이터는 암호화되어 저장되며, 암호화 키는 신뢰 플랫폼 모듈에 의하여 관리되며, 클라이언트 단말기는 가상화 기술에 의하여 업무를 위한 업무용 도메인과 서버에 저장되어 있는 기밀 데이터에 접근하기 위한 보안 도메인으로 구분됨으로써, 기밀 데이터의 외부 유출을 방지하며, 또한 관리자에 의한 데이터의 외부 유출을 막을 수 있는 이점이 있다.

대 표 도 - 도3



특허청구의 범위

청구항 1

클라이언트 단말기의 하드웨어로 구성된 제1 신뢰 플랫폼 모듈(제1 TPM)에서 상기 클라이언트의 단말기에서 동작하는 운영체제 및 프로세서에 대한 해시값을 생성하여 전송하는 과정;

서버에서 수신된 상기 해시값과 상기 서버에 사전에 설정된 해시값이 일치 된 경우 상기 클라이언트 단말기를 인증하고, 가상 머신을 상기 클라이언트 단말기에 전송하는 과정;

상기 클라이언트 단말기에서 상기 가상머신을 기초로 구성한 보안 도메인을 통하여 상기 서버의 기밀데이터 저장수단에 액세스하는 과정; 및

상기 서버에서 상기 기밀데이터를 상기 서버의 제2 신뢰 플랫폼 모듈(제2 TPM)을 통하여 암호화하여 상기 기밀데이터 저장수단에 저장하는 과정을 포함함을 특징으로 하는 네트워크 시스템에서의 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법.

청구항 2

제1항에 있어서, 상기 인증된 클라이언트 단말기에서 상기 기밀데이터를 리드하기 위해 상기 기밀데이터 저장수단에 액세스한 경우, 상기 서버에서 제2 신뢰 플랫폼 모듈에서 생성한 복호화 키를 이용하여 암호화된 상기 기밀데이터를 복호화하는 과정을 더 포함함을 특징으로 하는 네트워크 시스템에서의 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법.

청구항 3

제1항에 있어서, 상기 해시 값에 근거하여 상기 클라이언트 단말기를 인증하는 과정은 상기 서버에서 사전에 설정한 해시 값과 비교하여 일치한 경우에 상기 단말기를 인증함을 특징으로 하는 네트워크 시스템에서의 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법.

청구항 4

제1항에 있어서, 상기 클라이언트 단말기가 인증을 실패한 경우에는,

업무용 도메인을 기동하고 업무용 도메인으로 콘솔을 전환하는 과정을 포함함을 특징으로 하는 네트워크 시스템에서의 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법.

청구항 5

제4항에 있어서, 상기 클라이언트 단말기에서 하이퍼바이저를 이용하여 복수의 도메인이 하나의 시스템에서 동작하도록 제어함을 특징으로 하는 네트워크 시스템에서의 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법.

청구항 6

제2항에 기재된 네트워크 시스템에서의 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 클라이언트 단말기에서 가상화와 신뢰 플랫폼 모듈을 이용하여 서버의 인증을 승인 받고, 특정 도메인을 통하여 보안 관리가 필요한 데이터를 암호화하여 서버에 저장하고 필요시에 한하여 복호화하여 사용시에 데이터의 외부 유출을 방지하는 데이터 보안 처리 방법과 이를 실행하기 위한 프로그램을 저장한 기록매체에 관한 것이다.

배 경 기 술

[0002] 일반적으로 데이터의 보안을 유지하는 방법은 암호화하는 방법과 유출 경로를 차단하는 방법으로 나눌 수 있다. 암호화하여 데이터를 보호하는 방법은 AES(Advanced Encryption Standard)나 RSA(Rivest Shamir Adleman)와 같은 표준 암호화 알고리즘을 이용하여 데이터를 암호화하여 보관하는 방법이다.

[0003] 암호화 알고리즘은 랜덤하게 암호화에 사용할 키를 생성하며, 이 키를 이용하여 데이터를 암호화하고, 암호화된 데이터는 복호화되어야만 사용하는 것이 가능하다. 따라서, 데이터를 복호화하기 위해서는 복호화에 사용할 키가 필요하며, 이것은 암호화 키와 연관성을 가진다.

[0004] 이러한 암호화 키는 대칭키(Symmetric key)와 비대칭키(Asymmetric key)로 구분되며, 대칭키는 AES 암호화 알고리즘, 비대칭키는 RSA 암호화 알고리즘에서 사용된다. 대칭키는 암호화 키와 복호화 키가 동일한 암호화 방식이며, 비대칭키는 암호화 키와 다른 복호화 키를 사용하는 것이다. 그러므로 데이터를 암호화하여 데이터를 보호할 경우, 복호화 키가 외부로 유출되지 않는다면 안전하게 데이터를 보호하는 것이 가능하다.

[0005] 이러한 기술을 응용하여 DRM(Digital Rights Management) 기술이 개발되어 사용되고 있다. DRM은 음악 파일과 같은 미디어 파일에 주로 사용되고 있으며, 구매자에게 암호화한 미디어 파일과, 이를 복호화할 수 있는 복호화 키를 같이 제공하여 준다. 그렇기 때문에 해당 복호화 키를 가지고 있지 않은 다른 사용자는 미디어 파일을 사용할 수 없게 된다.

[0006] DRM은 미디어 파일 뿐 아니라 회사의 기밀문서를 다룰 때도 사용되며, 만약 외부로 기밀문서가 제공되어야 하는 경우가 생긴다면 DRM 키를 관리하고 있는 관리자를 통해 복호화된 후 외부로 제공된다.

[0007] 데이터 유출 경로를 차단하는 방법은 방화벽과 같이 외부로부터 송수신되는 네트워크의 흐름을 감시하거나, 가상화를 통해서 운영체제인 도메인(domain) 간에 서로 독립된 메모리 영역을 사용하도록 하여 각 도메인에서 사용하는 데이터 사이에 교류를 차단함으로써, 데이터의 외부 유출을 막는 방법이 있다.

[0008] 방화벽은 미리 정하여진 규칙에 따라서 허용되지 않은 외부에서의 접근을 차단하며, 네트워크를 사용하는 응용프로그램을 파악하여 허용되지 않은 외부로 패킷이 전송되는 것을 방지한다. 가상화는 하이퍼바이저(Hypervisor)라는 도메인을 관리하여 주는 프로그램 위에서 개개의 운영체제(Operating System)가 독립적인 실행 영역을 가지고 하나의 도메인을 구성하여 수행되는 것을 의미한다. 각 도메인은 하이퍼바이저에 의하여 실행 영역이 할당되며, 다른 도메인이 사용하는 실행 영역에 접근하는 것이 불가능하기 때문에 도메인 간에 데이터의 교류를 차단할 수 있다. 이러한 기술을 통하여 잘못된 데이터의 이동 경로를 파악하고 차단함으로써 기밀 데이터의 외부 유출을 차단할 수 있게 된다.

[0009] 이와 같은 종래의 기술은 기밀 데이터의 외부 유출을 막아줄 수 있는 효과적인 방안이다. 하지만 위에서 제시된 방법은 소프트웨어적인 방법으로 소프트웨어 자체의 결함 혹은 잘못된 사용으로 인하여 데이터의 유출이 발생할 수 있다는 단점을 가지고 있다.

[0010] 또한, 이러한 암호화 방법에서는 사용된 복호화 키는 클라이언트 단말기의 저장공간에 저장되기 때문에 외부의 해킹 등의 침입에 상시 노출되어 있다.

[0011] 도 1은 종래의 DRM 복호화 키를 이용한 데이터 보안을 설명하기 위한 시스템의 블록도이다.

[0012] 도 1에서 도시한 바와 같이 서버(100)의 데이터 저장수단(102)에서 DRM으로 암호화된 데이터를 운영체제(110)로 작동되는 클라이언트 단말기(106)에 전송하면, 클라이언트 단말기(06)에서는 DRM 감시프로세스(108)를 통하여 DRM 복호화키로 암호화된 데이터의 DRM을 해제시켜 사용한다.

[0013] 이 경우 회사나 공공기관에서 많이 사용되고 있는 DRM의 경우 관리자(104)가 암호화에 사용된 DRM 복호화키를 관리하고 있기 때문에 관리자에 의한 기밀 데이터의 유출도 발생할 수 있다. 방화벽이나 가상화의 경우, 잘못된 정책 설정으로 인하여 악의적인 프로그램이 외부 네트워크에 연결될 수 있다.

발명의 내용

해결 하고자하는 과제

[0014] 본 발명은 신뢰 플랫폼 모듈(TPM)을 이용하여 서버의 기밀 데이터의 암호/복호화 키를 하드웨어적으로 관리하며, TPM을 통해 인증된 클라이언트에만 기밀 데이터에 접근할 수 있는 별도의 가상화 도메인을 공급하여

기존 업무 환경에 영향을 받지 않고 독립적으로 동작할 수 있는 보안 환경을 제공받게 함으로써 기밀 데이터의 유출을 방지하는 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법 및 이를 수행하기 위한 프로그램을 저장한 기록 매체를 제공하는 데 있다.

과제 해결수단

[0015] 상기 과제를 달성하기 위한 본 발명에 의한 네트워크 시스템에서의 가상화 및 신뢰 플랫폼 모듈을 이용한 데이터 보안 처리 방법은,

[0016] 클라이언트 단말기의 제1 신뢰 플랫폼 모듈(제1 TPM)에서 생성한 해시값을 전송하는 과정;

[0017] 서버에서 수신된 상기 해시값에 근거하여 상기 클라이언트 단말기가 인증되면, 가상 머신을 상기 클라이언트 단말기에 전송하는 과정;

[0018] 상기 클라이언트 단말기에서 상기 가상머신을 기초로 구성한 보안 도메인을 통하여 상기 서버의 기밀데이터 저장수단에 액세스하는 과정; 및

[0019] 상기 서버에서 상기 기밀데이터를 상기 서버의 제2 신뢰 플랫폼 모듈(제2 TPM)을 통하여 암호화하여 상기 기밀데이터 저장수단에 저장하는 과정을 포함함을 특징으로 한다.

[0020] 또한, 상기 해시 값에 근거하여 상기 클라이언트 단말기를 인증하는 과정은 상기 서버에서 사전에 설정한 해시값과 비교하여 일치한 경우에 상기 단말기를 인증함을 특징으로 한다.

[0021] 또한, 상기 인증된 클라이언트 단말기에서 상기 기밀데이터를 리드하기 위해 상기 기밀데이터 저장수단에 액세스한 경우, 상기 서버에서 제2 신뢰 플랫폼 모듈에서 생성한 복호화키를 이용하여 암호화된 상기 기밀데이터를 복호화하는 과정을 더 포함함을 특징으로 한다.

[0022] 또한, 상기 클라이언트 단말기가 인증을 실패한 경우에는,

[0023] 업무용 도메인을 기동하고 업무용 도메인으로 콘솔을 전환하는 과정을 포함함을 특징으로 한다.

[0024] 또한, 상기 클라이언트 단말기에서 하이퍼바이저를 이용하여 복수의 도메인이 하나의 시스템에서 동작하도록 제어함을 특징으로 한다.

효 과

[0025] 상기한 바와 같은 본 발명의 가상화 및 TPM 기반의 기밀 데이터 보안 처리 방법은 다음과 같은 효과가 있다.

[0026] 첫째, 가상화 기법을 통해 업무용 도메인과 보안 도메인을 구분함으로써 기존 업무 방식에 영향을 받지 않으면서 보안을 강화할 수 있다.

[0027] 둘째, 외부 네트워크에 연결되지 않는 보안 도메인을 통해서만 기밀 데이터에 접근할 수 있기 때문에 보안 도메인을 통해서는 외부로 기밀 데이터가 유출될 가능성이 없다.

[0028] 셋째, 인증된 클라이언트에만 서버에서 변형되지 않은 가상머신을 제공하기 때문에 보안 도메인은 클라이언트에서 악의적인 목적으로 수정하여 사용하는 것이 불가능하다는 장점이 있다.

[0029] 넷째, 암호화 및 복호화에 사용되는 암호/복호화키를 TPM을 이용하여 암호화하고, 키 관리를 하드웨어인 TPM에서 함으로써 기존의 소프트웨어적인 보안 방식을 강화할 수 있다는 장점이 있다.

[0030] 다섯째, TPM을 이용하여 암호화되어 관리되고 있는 기밀 데이터가 외부로 유출되는 경우가 발생하더라도, 암호/복호화 키는 TPM 내부에만 존재하고 있기 때문에 외부에서 기밀 데이터를 복호화하는 것이 불가능 하다는 장점이 있다.

발명의 실시를 위한 구체적인 내용

[0031] 이하, 첨부 도면을 참조하여 본 발명의 바람직한 실시예를 설명하기로 한다.

[0032] 도 2는 본 발명에 의한 가상화 및 TPM 기반의 데이터 보안 처리 방법을 설명하기 위한 시스템의 블록도이다. 클라이언트 단말기(212)는 가상화 기술이 적용되며 초기 시동시 하이퍼바이저(220)와 관리자 도메인(214), 업무용 도메인(216)이 구동된다. 하이퍼바이저(220)는 여러 도메인이 하나의 시스템에서 동작할 수 있도록 관리하여 주며, 관리자 도메인(214)은 다른 도메인을 감시하고 사용자에게 도메인에 대한 제어권을 부여하는 기능을 수행한

다. 업무용 도메인(216)은 일상적인 문서 작업이나 인터넷을 사용할 수 있도록 네트워크에 접속되어 있다.

[0033] 보안 도메인(218)은 네트워크로의 접속이 차단되어 도메인에 허가되지 않은 응용프로그램에 대한 설치가 불가능하고 iSCSI 프로토콜과 같은 네트워크 스토리지 프로토콜을 이용하여 서버(200)의 기밀 데이터 저장수단(208)에 접근할 수 있다.

[0034] 클라이언트 단말기(212)에 있는 데이터 저장수단(222)은 보안 도메인(218)을 제외한 모든 도메인에서 접근이 가능하며, 일상 업무의 데이터 및 응용프로그램의 자유로운 설치 및 삭제가 가능하다. 클라이언트 단말기(212)의 제1 TPM(224)은 시동 과정에서 사용되며 부트로더에서 클라이언트의 시동시에 실행되는 운영체제 및 프로세스에 대한 해시 값(Hash value)을 생성하여, TPM내에 존재하는 레지스터인 PCR(Platform Configuration Register)에 저장한다.

[0035] 서버(200)는 가상화 기술이 적용되지 않은 일반적인 운영체제를 사용하고 있으며, 클라이언트 단말기(106)에 제공할 보안 도메인용 가상머신을 저장하는 가상머신(Virtual Machine; VM) 저장수단(206)과 기밀 데이터를 제2 TPM(210)을 이용하여 암호화하고 관리하는 기밀데이터 저장수단(208)으로 구성된다. 서버(200)에서 사용되는 운영체제에는 클라이언트 단말기(212)로부터 수신한 해시 값을 통하여 해당 클라이언트 단말기(212)를 인증하며, 가상머신을 전송할 수 있는 인증 프레임워크가 구축되어 있으며, 데이터 저장소에 기밀 데이터가 저장될 때 제2 TPM(210)을 이용하여 암호화할 수 있는 파일시스템으로 구성되어 있다.

[0036] VM 저장수단(206)은 클라이언트 단말기(212)에서 사용될 보안 도메인(218)을 구성하기 위한 가상머신이 저장되어 있으며, 암호화되지 않은 상태로 저장된다. 기밀데이터 저장수단(208)은 기밀 데이터를 저장하며 데이터가 저장될 때 제2 TPM(210)을 통하여 암호화되어 저장된다. 서버(100)의 제2 TPM(210)은 기밀데이터 저장수단(208)의 기밀 데이터를 암호화할 때 사용되는 암호/복호화 키를 제2 TPM 내부에서 생성된 키를 이용하여 암호화하여 관리함으로써 소프트웨어적인 보안 기법을 강화시켜준다.

[0037] 서버(200)의 클라이언트 단말기(212)에 대한 검증 및 인증 과정은 클라이언트 단말기(212)에서 제1 TPM(224) 내의 PCR에 저장된 해시 값을 서버(200)에 전송함으로써 이루어지며, 클라이언트 단말기(212)의 인증이 완료되면 서버(200)는 VM 저장수단(206)의 가상머신을 클라이언트 단말기(212)로 전달한다. 클라이언트 단말기(212)는 수신된 가상머신을 기초로 구성된 보안 도메인(218)을 통해 서버의 기밀데이터 저장수단(208)에 접근하며, 보안 도메인(218)을 통해 접근할 경우 제2 TPM(210)에서 생성한 복호화 키를 이용하여 TPM 암호화 파일시스템(204)에서 기밀데이터를 복호화함으로써 클라이언트 단말기(212)에서 액세스하여 사용할 수 있도록 한다.

[0038] 도 3은 본 발명에 의한 네트워트 시스템 상에서 데이터 보안 처리 방법을 설명하기 위한 흐름도이다.

[0039] 클라이언트 단말기(212)는 처음 시동되면 바이오스에서 TPM을 초기화하고(S40) 부트로더를 불러온다(S41). 부트로더는 TPM을 이용하여 시스템 시동시에 사용할 하이퍼바이저(220), 관리자 도메인(214), 업무용 도메인(216)의 이미지에 대한 해시 값을 생성하여 제1 TPM(224)의 PCR 레지스터에 저장한다(S42).

[0040] 부트로더는 하이퍼바이저(220)를 실행시키고, 하이퍼바이저(220)는 관리자 도메인(214)을 기동시킨다(S43, S44). 관리자 도메인(214)이 기동된 후 클라이언트 단말기(212)는 서버에 연결하여 PCR에 저장되어 있는 이미지에 대한 해시 값을 서버로 전달한다(S45). 서버의 운영체제(202)는 클라이언트 단말기(212)로부터 받은 해시 값과 사전에 설정된 해시 값의 비교를 통해 인증하여 정상적인 이미지들을 이용하여 클라이언트 단말기(212)가 시동되었는지 여부를 판단한다(S46).

[0041] 인증을 통해 정상적인 이미지로 시동이 완료되었다고 판단되면 서버는 클라이언트에 보안 도메인(218)을 구동하기 위한 가상머신을 전송한다(S50). 정상적인 이미지로 시동이 완료되지 않았다고 판단되면 서버는 클라이언트 단말기(212)에 가상머신을 전송하지 않으며(S80), 클라이언트 단말기(212)는 업무용 도메인(216)을 기동시킨 후(S81) 업무용 도메인(216)으로 콘솔을 전환하여 시동을 완료한다(S82).

[0042] 클라이언트 단말기(212)로 가상머신이 전송되면 하이퍼바이저(220)는 업무용 도메인(216)과, 보안 도메인(218)을 기동 시킨다(S51, S52). 업무 종류에 따라서 업무용 도메인과 보안 도메인으로 콘솔을 변경할 수 있으며, 업무용 도메인(216)으로 콘솔이 전환되면, 사용자는 이메일을 사용하거나 문서 작업과 같은 일상적인 업무 작업을 수행할 수 있다(S53, S60, S61).

[0043] 보안 도메인(218)으로 콘솔을 전환하면 보안 도메인은 서버의 데이터 저장소에 iSCSI와 같은 네트워크 스토리지 프로토콜을 이용하여 접속한다(S70, S71). 보안 도메인을 통하여 클라이언트 단말기(212)가 서버의 기밀데이터 저장수단(208)에 접속하여 기밀 데이터를 생성하여 저장하면(S72), 서버의 운영체제 내의 TPM 암호화 파일시

스템(204)은 AES와 같은 암호화 알고리즘을 이용하여 데이터를 암호화한다(S73). 암호화에 사용된 대칭키 형태의 암호/복호화키는 제2 TPM(210)에서 생성된 키에 의하여 다시 암호화되어 저장된다(S74). 클라이언트 단말기(212)가 보안 도메인을 통하여 기밀데이터 저장수단(208)에 저장되어 있는 기밀 데이터를 사용하고자 하면(S75), 서버의 운영체제 내의 TPM 암호와 파일시스템(204)은 해당 데이터의 암호/복호화 키를 제2 TPM(210)을 이용하여 복호화한 후(S76), 복호화된 키를 이용하여 기밀 데이터를 복호화하여(S77) 클라이언트 단말기에서 사용할 수 있도록 한다(S78).

[0044] 이와 같이, 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 발명의 범주에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능하다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안 되며 후술하는 특허청구범위 뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 할 것이다.

도면의 간단한 설명

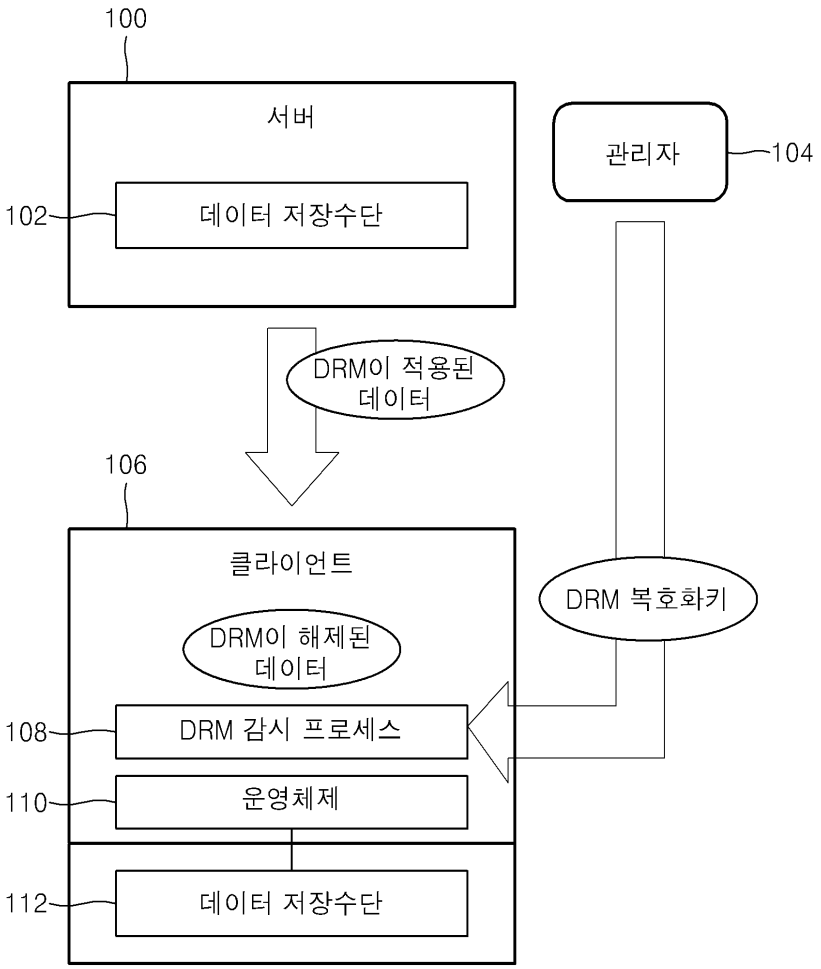
[0045] 도 1은 종래의 DRM 복호화 키를 이용한 데이터 보안을 설명하기 위한 시스템의 블록도이다.

[0046] 도 2는 본 발명에 의한 가상화 및 TPM 기반의 데이터 보안 처리 방법을 설명하기 위한 시스템의 블록도이다.

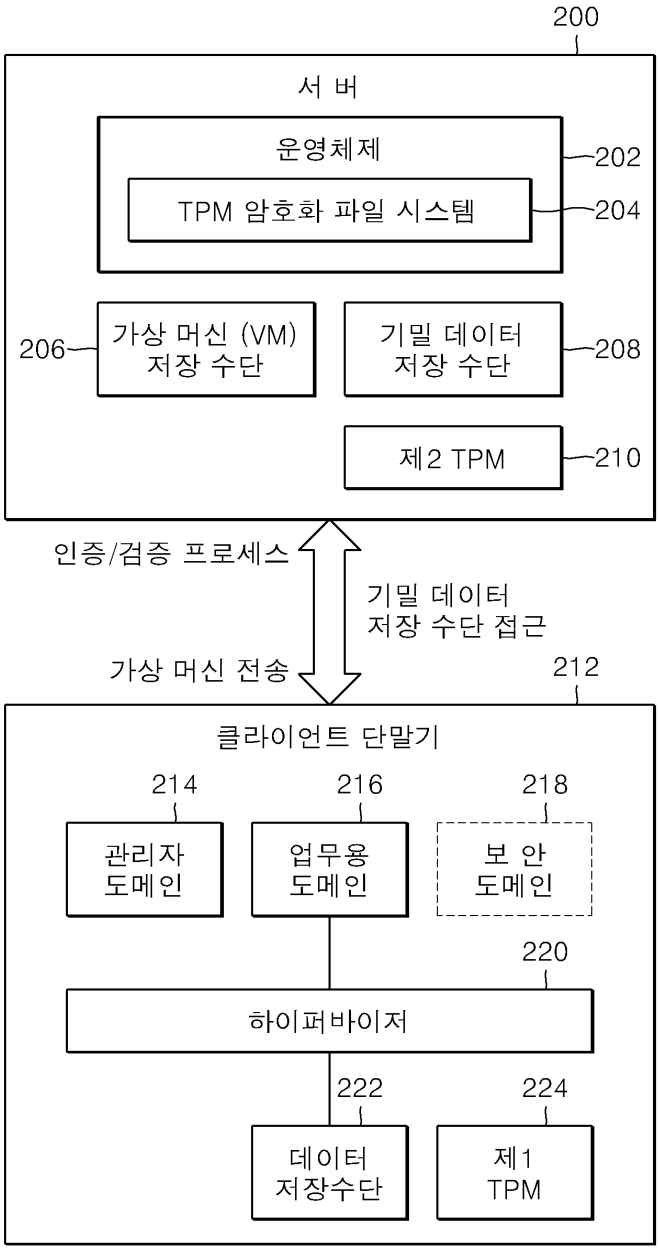
[0047] 도 3은 본 발명에 의한 네트워트 시스템 상에서 데이터 보안 처리 방법을 설명하기 위한 흐름도이다.

도면

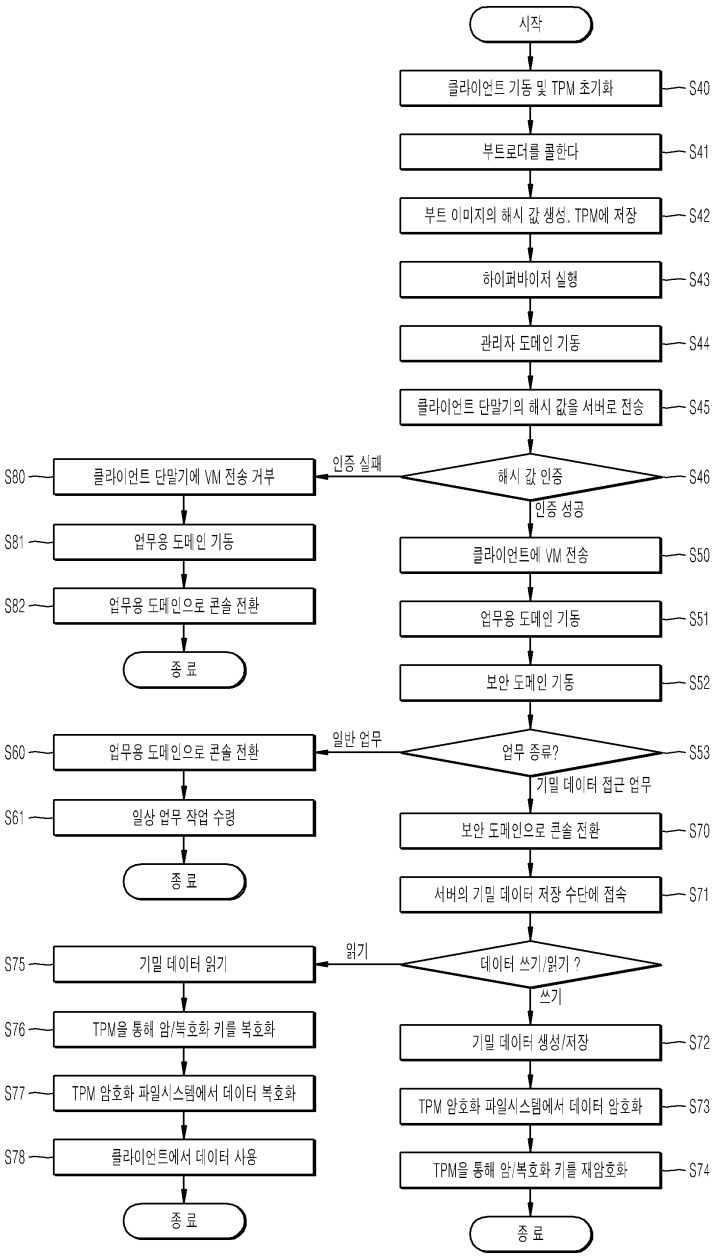
도면1



도면2


200
서 버
운영체제
202
TPM 암호화 파일 시스템
204
206
가상 머신 (VM)
저장 수단
기밀 데이터
저장 수단
208
제2 TPM
210
인증/검증 프로세스
가상 머신 전송
기밀 데이터
저장 수단 접근
212
클라이언트 단말기
214
216
218
관리자
도메인
업무용
도메인
보 안
도메인
220
하이퍼바이저
222
224
데이터
저장수단
제1
TPM

도면3


시작
클라이언트 기동 및 TPM 초기화
S40
부트로더를 콜한다
S41
부트 이미지의 해시 값 생성, TPM에 저장
S42
하이퍼바이저 실행
S43
관리자 도메인 기동
S44
클라이언트 단말기의 해시 값을 서버로 전송
S45
해시 값 인증
S46
인증 실패
S80
클라이언트 단말기에 VM 전송 거부
S81
업무용 도메인 기동
S82
업무용 도메인으로 콘솔 전환
종 료
인증 성공
클라이언트에 VM 전송
S50
업무용 도메인 기동
S51
보안 도메인 기동
S52
업무 종류?
S53
일반 업무
S60
업무용 도메인으로 콘솔 전환
S61
일상 업무 작업 수령
종 료
기밀 데이터 접근 업무
보안 도메인으로 콘솔 전환
S70
서버의 기밀 데이터 저장 수단에 접속
S71
데이터 쓰기/읽기 ?
읽기
S75
기밀 데이터 읽기
S76
TPM을 통해 암/복호화 키를 복호화
S77
TPM 암호화 파일시스템에서 데이터 복호화
S78
클라이언트에서 데이터 사용
종 료
쓰기
기밀 데이터 생성/저장
S72
TPM 암호화 파일시스템에서 데이터 암호화
S73
TPM을 통해 암/복호화 키를 재암호화
S74
종 료