(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년04월08일
(11) 등록번호 10-1508439
(24) 등록일자 2015년03월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01)
(21) 출원번호 10-2013-0128704
(22) 출원일자 2013년10월28일
심사청구일자 2013년10월28일
(56) 선행기술조사문헌
KR1020030078527 A*
KR1020090066053 A
KR1020090078551 A
KR1020030052510 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경북 포항시 남구 지곡로 155, 9동 1503호 (지곡동, 교수아파트)
박우람
경상북도 포항시 남구 효자동 산31 남자기숙사 11동 112호
신재복
경북 포항시 남구 지곡로211번길 50, 342동 403호 (지곡동, 지곡그린빌라)
(74) 대리인
특허법인이상

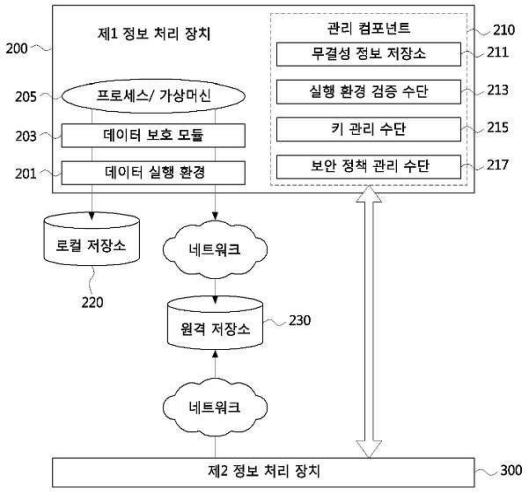
전체 청구항 수 : 총 19 항 심사관 : 구본재

(54) 발명의 명칭 **데이터 기밀성 보장 방법, 이를 이용하는 데이터 공유 방법 및 시스템**

(57) 요 약

데이터 기밀성 보장 방법, 이를 이용하는 데이터 공유 방법 및 시스템이 개시된다. 데이터 보장 방법은 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 수집하는 단계, 바인딩 정보를 기반으로 바인딩 키를 생성하여 제 1 정보 처리 장치에 제공하는 단계, 제 1 정보 처리 장치로부터 바인딩 키로 암호화된 데이터 키를 수신하는 단계 및 암호화된 데이터 키를 바인딩 키로 복호화하여 제 1 정보 처리 장치의 데이터에 접근하는 단계를 포함한다. 따라서, 데이터의 기밀성을 보장함과 동시에 안전하게 데이터를 공유할 수 있다.

대 표 도 - 도7



명 세 서

청구범위

청구항 1

제 1 정보 처리 장치의 데이터에 접근하는 제 2 정보 처리 장치에 의해 수행되는 데이터 기밀성 보장 방법에 있어서,

상기 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 상기 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 수집하는 단계;

상기 바인딩 정보를 기반으로 바인딩 키를 생성하여 상기 제 1 정보 처리 장치에 제공하는 단계;

상기 제 1 정보 처리 장치로부터 상기 바인딩 키로 암호화된 데이터 키를 수신하는 단계; 및

상기 암호화된 데이터 키를 상기 바인딩 키로 복호화하여 상기 제 1 정보 처리 장치의 데이터에 접근하는 단계를 포함하는 데이터 기밀성 보장 방법.

청구항 2

청구항 1에 있어서,

상기 바인딩 키는,

상기 바인딩 정보를 기반으로 바인딩 공개키 및 바인딩 비밀키를 포함하여 생성되는 것을 특징으로 데이터 기밀성 보장 방법.

청구항 3

청구항 2에 있어서,

상기 바인딩 키로 암호화된 데이터 키를 수신하는 단계는,

상기 제 1 정보 처리 장치로부터 상기 바인딩 공개키로 암호화된 데이터 키를 수신하는 것을 특징으로 하는 데이터 기밀성 보장 방법.

청구항 4

청구항 3에 있어서,

상기 제 1 정보 처리 장치의 데이터에 접근하는 단계는,

상기 바인딩 공개키로 암호화된 데이터 키를 수신하여 상기 바인딩 비밀키로 복호화함으로써 상기 제 1 정보 처리 장치의 데이터에 접근하는 것을 특징으로 하는 데이터 기밀성 보장 방법.

청구항 5

데이터를 가진 제 1 정보 처리 장치에 의해 수행되는 데이터 공유 방법에 있어서,

상기 데이터에 접근하고자 하는 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 단계;

상기 무결성이 검증된 제 2 정보 처리 장치에 미리 정의한 제 1 정보 처리 장치의 보안 정책 정보를 전송하여 상기 제 2 정보 처리 장치에 적용시키고 상기 제 2 정보 처리 장치에 적용된 상기 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 단계; 및

상기 제 2 정보 처리 장치에 적용된 상기 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성이 검증됨에 따라 상기 제 2 정보 처리 장치로부터 수신한 제 2 정보 처리 장치의 바인딩 키를 이용하여 상기 제 2 정보 처리 장치와 데이터를 공유하는 단계를 포함하는 것을 특징으로 하는 데이터 공유 방법.

청구항 6

청구항 5에 있어서,

상기 제 2 정보 처리 장치의 실행 환경에 대한 무결성 검증에 실패하거나 상기 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성 검증에 실패하는 경우, 상기 제 2 정보 처리 장치와의 데이터 공유를 중단하는 단계를 더 포함하는 것을 특징으로 하는 데이터 공유 방법.

청구항 7

청구항 5에 있어서,

상기 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 단계는,

공인 인증 기관으로부터 상기 제 2 정보 처리 장치에 대한 인증서를 획득하는 단계;

상기 제 2 정보 처리 장치로부터 상기 제 2 정보 처리 장치에 대한 사용자 정보 및 실행 환경 정보를 포함하는 무결성 정보를 인증서의 비밀키로 전자 서명한 실행 환경 전자 서명을 수신하는 단계; 및

상기 제 2 정보 처리 장치에 대한 인증서의 공개키를 이용하여 실행 환경 전자 서명을 검증하는 단계를 포함하는 것을 특징으로 하는 데이터 공유 방법.

청구항 8

청구항 5에 있어서,

상기 제 2 정보 처리 장치에 적용된 상기 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 단계는,

상기 제 2 정보 처리 장치로부터 상기 제 2 정보 처리 장치에 적용된 상기 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성 정보를 인증서의 비밀키로 전자 서명한 보안 정책 전자 서명을 수신하는 단계; 및

상기 제 2 정보 처리 장치에 대한 인증서의 공개키를 이용하여 상기 보안 정책 전자 서명을 검증하는 단계를 포함하는 것을 특징으로 하는 데이터 공유 방법.

청구항 9

청구항 5에 있어서,

상기 제 2 정보 처리 장치의 바인딩 키는,

상기 제 1 정보 처리 장치의 요청에 따라 상기 제 2 정보 처리 장치로부터 상기 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 상기 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 기반으로 상기 제 2 정보 처리 장치에 대한 바인딩 공개키 및 바인딩 비밀키를 포함하여 생성되는 것을 특징으로 하는 데이터 공유 방법.

청구항 10

청구항 9에 있어서,

상기 제 2 정보 처리 장치와 데이터를 공유하는 단계는,

상기 제 2 정보 처리 장치로부터 수신한 바인딩 키의 바인딩 공개키를 기반으로 데이터 키를 암호화하여 상기 제 2 정보 처리 장치에 전송하면, 상기 제 2 정보 처리 장치에서 상기 암호화된 데이터 키를 바인딩 비밀키로 복호화함에 따라 상기 제 2 정보 처리 장치와 데이터를 공유하는 것을 특징으로 하는 데이터 공유 방법.

청구항 11

데이터를 가진 제 1 정보 처리 장치와 네트워크로 연결된 제 2 정보 처리 장치 간의 데이터 공유에 있어서,

상기 제 2 정보 처리의 실행 환경 및 보안 정책에 대한 무결성을 검증하고, 상기 제 2 정보 처리 장치로부터 수신한 바인딩 키를 이용하여 데이터 키를 관리함으로써 상기 제 2 정보 처리 장치에 데이터를 제공하는 제 1 정보 처리 장치; 및

상기 제 1 정보 처리 장치의 요청에 따라 실행 환경 전자 서명, 보안 정책 전자 서명 및 바인딩 키 중 적어도

하나를 생성하여 상기 제 1 정보 처리 장치에 제공하고, 상기 바인딩 키를 이용하여 상기 제 1 정보 처리 장치의 데이터에 접근함으로써 상기 제 1 정보 처리 장치의 데이터를 제공받는 제 2 정보 처리 장치를 포함하는 데이터 공유 시스템.

청구항 12

청구항 11에 있어서,

상기 제 1 정보 처리 장치는,

상기 제 1 정보 처리 장치 내에 구현된 로컬 저장부 또는 네트워크로 연결된 원격 저장부에 상기 데이터를 기록하며, 상기 제2 정보 처리 장치와 상기 데이터를 공유할 수 있도록 상기 제2 정보 처리 장치로부터 수신한 바인딩 키의 바인딩 공개키를 기반으로 데이터 키를 암호화하여 기록하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 13

청구항 12에 있어서,

상기 제 1 정보 처리 장치는,

상기 로컬 저장부 또는 원격 저장부에 기록된 데이터에 접근하고자 하는 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 실행 환경 검증부;

상기 무결성이 검증된 제 2 정보 처리 장치에 미리 정의한 제 1 정보 처리 장치의 보안 정책 정보를 전송하여 상기 제 2 정보 처리 장치에 적용시키고 상기 제 2 정보 처리 장치에 적용된 상기 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 보안 정책 검증부; 및

상기 제 2 정보 처리 장치에 적용된 상기 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성이 검증됨에 따라, 상기 제 2 정보 처리 장치로부터 수신한 제 2 정보 처리 장치의 바인딩 키를 이용하여 상기 제 2 정보 처리 장치와 데이터를 공유하는 데이터 공유부를 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 14

청구항 13에 있어서,

상기 실행 환경 검증부는,

공인 인증 기관으로부터 상기 제 2 정보 처리 장치에 대한 인증서를 획득하고, 상기 제 2 정보 처리 장치로부터 수신한 실행 환경 전자 서명을 상기 인증서의 공개키를 이용하여 검증함으로써 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 15

청구항 14에 있어서,

상기 보안 정책 검증부는,

상기 제 2 정보 처리 장치로부터 수신한 보안 정책 전자 서명을 상기 인증서의 공개키를 이용하여 검증함으로써 상기 제 2 정보 처리 장치에 적용된 상기 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 16

청구항 13에 있어서,

상기 데이터 공유부는,

상기 제 2 정보 처리 장치로부터 수신한 바인딩 키를 이용하여 데이터 키를 암호화하여 상기 제 2 정보 처리 장치에 전송하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 17

청구항 11에 있어서,

상기 제 2 정보 처리 장치는,

상기 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 상기 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 수집하는 바인딩 정보 수집부;

상기 바인딩 정보를 기반으로 바인딩 공개키 및 바인딩 비밀키를 포함하는 바인딩 키를 생성하는 바인딩 키 생성부; 및

상기 제 1 정보 처리 장치로부터 상기 바인딩 공개키로 암호화된 데이터 키를 수신하고, 상기 암호화된 데이터 키를 상기 바인딩 비밀키로 복호화하여 상기 제 1 정보 처리 장치의 데이터에 접근하는 데이터 접근부를 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 18

청구항 17에 있어서,

상기 제 2 정보 처리 장치는,

상기 제 2 정보 처리 장치에 대한 사용자 정보 및 실행 환경 정보를 기반으로 실행 환경 전자 서명을 생성하고 상기 제 1 정보 처리 장치에 대한 보안 정책 정보를 기반으로 보안 정책 전자 서명을 생성하는 전자 서명 생성부를 더 포함하는 것을 특징으로 하는 데이터 공유 시스템.

청구항 19

청구항 17에 있어서,

상기 바인딩 정보 수집부는,

상기 수집된 바인딩 정보를 데이터가 실행되는 실행 환경과 독립되는 하드웨어 기반의 보안 칩에 기록함으로써 상기 바인딩 정보의 무결성을 보장하는 것을 특징으로 하는 데이터 공유 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 데이터 보안 기술에 관한 것으로, 더욱 상세하게는, 데이터를 암호화하는 데이터 키의 관리를 기반으로 데이터의 기밀성을 보장하는 방법과, 이를 이용하여 데이터를 공유하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 대용량의 스토리지 서비스를 제공하는 클라우드 컴퓨팅 기술과 이동 통신 기술이 발전함에 따라 로컬의 저장소 또는 원격의 저장소에 저장된 데이터를 컴퓨터, 스마트폰(smart phone) 또는 태블릿 PC와 같은 다양한 정보 처리 장치에서 자유롭게 공유할 수 있게 되었다.

[0003] 그러나, 원격의 저장소에 저장된 데이터에 대한 접근은 네트워크를 통해 이루어짐에 따라 데이터를 공유하는 동안 외부에 유출되거나 악의적인 목적을 지닌 공격자에 의해 훼손될 수 있다.

[0004] 따라서, 종래에는 데이터를 생성하는 정보 처리 장치가 데이터를 암호화하여 SSL(Secure Socket Layer) 프로토콜로 보호되는 네트워크를 통해 원격 기기로 전송함으로써 데이터에 대한 기밀성을 보장하는 기법이 제안되었다.

[0005] 또한, 데이터를 암호화하여 파편화한 후 원격 기기로 전송함으로써 네트워크 패킷 피싱(Packet Phishing)으로 데이터의 파편이 유출되더라도 전체 데이터에 대한 접근은 불가능하도록 하여 데이터에 대한 기밀성을 보장하고자 하였다.

[0006] 상술한 바와 같은 종래 기술은 데이터를 데이터 키로 암호화하여 원격 기기로 전송하기 때문에 데이터 키를 가지고 있지 않은 원격 기기에서는 암호화된 데이터를 복호화할 수 없다는 점에서 어느 정도의 데이터에 대한 기밀성은 보장할 수 있다.

[0007] 그러나, 데이터에 접근하는 정보 처리 장치마다 보안 정책과 실행 환경이 상이함에 따라 키로거(key logger), 백도어(backdoor)와 같은 악성 프로그램 또는 제로 데이 공격(zero-day attack)과 같은 실행 환경 버그를 통해

데이터 키가 외부로 유출되거나 훼손될 수 있다.

[0008] 악의적인 목적을 지닌 공격자는 외부로 유출된 데이터 키를 이용하여 로컬 저장소 또는 원격 저장소에 저장된 데이터에 접근할 수 있음에 따라 데이터에 대한 기밀성이 훼손될 수 있다는 문제가 있다.

[0009] 도 1은 종래의 암호화 알고리즘을 이용하여 데이터의 기밀성을 보장하는 것을 설명하는 블록도이다.

[0010] 도 1을 참조하면, 로컬 기기(10)에서 프로세스(12)는 암호화 알고리즘(14)을 이용하여 특정 데이터 키로 데이터를 암호화할 수 있다. 여기서, 암호화된 데이터는 실행 환경(16)을 통해 로컬 저장소(18)에 저장되거나 네트워크로 연결되어 있는 원격 저장소(20)에 저장될 수 있다.

[0011] 그러나, 만약 로컬 기기(10)의 실행 환경(16)에 악성 프로그램이 동작하여 암호화 알고리즘에 이용되는 데이터 키가 외부로 유출되면, 로컬 저장소(18) 또는 원격 저장소(20)에 저장되어 있는 암호화된 데이터가 악의적인 목적으로 복호화되어 이용될 수 있다는 점에서 데이터에 대한 기밀성이 훼손될 수 있다는 문제가 있다.

[0012] 이와 같이 종래 기술은 특정 데이터 키로 데이터를 암호화하여 저장함으로써 데이터의 기밀성을 보장하고자 하였다.

[0013] 그러나, 데이터 키를 이용하여 데이터를 복호화하는 정보 처리 장치에 대한 무결성이 훼손되면 데이터 키가 유출되어 데이터의 기밀성이 훼손될 수 있다는 점에서 문제가 있다.

발명의 내용

해결하려는 과제

[0014] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 데이터를 공유하는 정보 처리 장치에 대한 정보를 기반으로 데이터를 암호화하는 데이터 키를 관리함으로써 데이터의 기밀성을 보장할 수 있는 데이터 기밀성 보장 방법을 제공하는 데 있다.

[0015] 또한, 본 발명의 다른 목적은, 무결성이 검증된 정보 처리 장치에 한하여 데이터 키의 관리를 기반으로 데이터에 대한 접근을 허용함으로써 네트워크로 연결된 정보 처리 장치와의 데이터의 공유를 안전하게 수행할 수 있는 데이터 공유 방법을 제공하는 데 있다.

[0016] 또한, 본 발명의 다른 목적은, 데이터 키를 이용하여 데이터의 기밀성을 보장하는 방법을 이용함으로써 정보 처리 장치 간의 데이터 공유에 있어 데이터의 기밀성을 보장할 수 있는 데이터 공유 시스템을 제공하는 데 있다.

과제의 해결 수단

[0017] 상기 목적을 달성하기 위한 본 발명의 일 측면에 따른 데이터 기밀성 보장 방법은, 제 1 정보 처리 장치의 데이터에 접근하는 제 2 정보 처리 장치에 의해 수행되며 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 수집하는 단계, 바인딩 정보를 기반으로 바인딩 키를 생성하여 제 1 정보 처리 장치에 제공하는 단계, 제 1 정보 처리 장치로부터 바인딩 키로 암호화된 데이터 키를 수신하는 단계 및 암호화된 데이터 키를 바인딩 키로 복호화하여 제 1 정보 처리 장치의 데이터에 접근하는 단계를 포함한다.

[0018] 여기에서, 바인딩 키는 바인딩 정보를 기반으로 바인딩 공개키 및 바인딩 비밀키를 포함하여 생성될 수 있다.

[0019] 여기에서, 바인딩 키로 암호화된 데이터 키를 수신하는 단계는 제 1 정보 처리 장치로부터 바인딩 공개키로 암호화된 데이터 키를 수신할 수 있다.

[0020] 여기에서, 제 1 정보 처리 장치의 데이터에 접근하는 단계는 바인딩 공개키로 암호화된 데이터 키를 수신하여 바인딩 비밀키로 복호화함으로써 제 1 정보 처리 장치의 데이터에 접근할 수 있다.

[0021] 또한, 상기 목적을 달성하기 위한 본 발명의 다른 측면에 따른 데이터 공유 방법은, 데이터를 가진 제 1 정보 처리 장치에 의해 수행되며 데이터에 접근하고자 하는 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 단계, 무결성이 검증된 제 2 정보 처리 장치에 미리 정의한 제 1 정보 처리 장치의 보안 정책 정보를 전송하여 제 2 정보 처리 장치에 적용시키고 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 단계 및 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성이 검증됨에 따라 제 2 정보 처리 장치로부터 수신한 제 2 정보 처리 장치의 바인딩 키를 이용하여 제

2 정보 처리 장치와 데이터를 공유하는 단계를 포함한다.

[0022] 여기에서, 데이터 공유 방법은 제 2 정보 처리 장치의 실행 환경에 대한 무결성 검증에 실패하거나 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성 검증에 실패하는 경우, 제 2 정보 처리 장치와의 데이터 공유를 중단하는 단계를 더 포함할 수 있다.

[0023] 여기에서, 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 단계는 공인 인증 기관으로부터 제 2 정보 처리 장치에 대한 인증서를 획득하는 단계, 제 2 정보 처리 장치로부터 제 2 정보 처리 장치에 대한 사용자 정보 및 실행 환경 정보를 포함하는 무결성 정보를 인증서의 비밀키로 전자 서명한 실행 환경 전자 서명을 수신하는 단계 및 제 2 정보 처리 장치에 대한 인증서의 공개키를 이용하여 실행 환경 전자 서명을 검증하는 단계를 포함할 수 있다.

[0024] 여기에서, 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 단계는 제 2 정보 처리 장치로부터 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성 정보를 인증서의 비밀키로 전자 서명한 보안 정책 전자 서명을 수신하는 단계 및 제 2 정보 처리 장치에 대한 인증서의 공개키를 이용하여 보안 정책 전자 서명을 검증하는 단계를 포함할 수 있다.

[0025] 여기에서, 제 2 정보 처리 장치와 데이터를 공유하는 단계는 제 2 정보 처리 장치로부터 수신한 바인딩 공개키를 기반으로 데이터 키를 암호화하여 제 2 정보 처리 장치에 전송하면 제 2 정보 처리 장치에서 암호화된 데이터 키를 바인딩 비밀키로 복호화함에 따라 제 2 정보 처리 장치와 데이터를 공유할 수 있다.

[0026] 또한, 상기 목적을 달성하기 위한 본 발명의 다른 측면에 따른 데이터 공유 시스템은, 데이터를 가진 제 1 정보 처리 장치와 네트워크로 연결된 제 2 정보 처리 장치 간의 데이터 공유에 있어서 제 2 정보 처리의 실행 환경 및 보안 정책에 대한 무결성을 검증하고, 제 2 정보 처리 장치로부터 수신한 바인딩 키를 이용하여 데이터 키를 관리함으로써 제 2 정보 처리 장치에 데이터를 제공하는 제 1 정보 처리 장치 및 제 1 정보 처리 장치의 요청에 따라 실행 환경 전자 서명, 보안 정책 전자 서명 및 바인딩 키 중 적어도 하나를 생성하여 제 1 정보 처리 장치에 제공하고, 바인딩 키를 이용하여 제 1 정보 처리 장치의 데이터에 접근함으로써 제 1 정보 처리 장치의 데이터를 제공받는 제 2 정보 처리 장치를 포함한다.

[0027] 여기에서, 제 1 정보 처리 장치는 로컬 저장부 또는 원격 저장부에 기록된 데이터에 접근하고자 하는 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 실행 환경 검증부, 무결성이 검증된 제 2 정보 처리 장치에 미리 정의한 제 1 정보 처리 장치의 보안 정책 정보를 전송하여 제 2 정보 처리 장치에 적용시키고 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 보안 정책 검증부 및 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성이 검증됨에 따라 제 2 정보 처리 장치로부터 수신한 제 2 정보 처리 장치의 바인딩 키를 이용하여 제 2 정보 처리 장치와 데이터를 공유하는 데이터 공유부를 포함할 수 있다.

[0028] 여기에서, 제 2 정보 처리 장치는 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 수집하는 바인딩 정보 수집부, 바인딩 정보를 기반으로 바인딩 공개키 및 바인딩 비밀키를 포함하는 바인딩 키를 생성하는 바인딩 키 생성부 및 제 1 정보 처리 장치로부터 바인딩 공개키로 암호화된 데이터 키를 수신하고, 암호화된 데이터 키를 바인딩 비밀키로 복호화하여 제 1 정보 처리 장치의 데이터에 접근하는 데이터 접근부를 포함할 수 있다.

발명의 효과

[0029] 상술한 바와 같은 본 발명의 실시예에 따른 데이터 기밀성 보장 방법, 이를 이용하는 데이터 공유 방법 및 시스템에 따르면, 데이터를 공유하는 정보 처리 장치에 대한 정보를 기반으로 데이터를 암호화하는 데이터 키를 관리함으로써 데이터의 기밀성을 보장할 수 있다.

[0030] 또한, 무결성이 검증된 정보 처리 장치에 한하여 데이터 키의 관리를 기반으로 데이터에 대한 접근을 허용함으로써 네트워크로 연결된 정보 처리 장치와의 데이터의 공유를 안전하게 수행할 수 있다.

[0031] 또한, 데이터 키를 이용하여 데이터의 기밀성을 보장하는 방법을 이용함으로써 정보 처리 장치 간의 데이터 공유에 있어 데이터의 기밀성을 보장할 수 있다.

도면의 간단한 설명

[0032] 도 1은 종래의 암호화 알고리즘을 이용하여 데이터의 기밀성을 보장하는 것을 설명하는 블록도이다.

도 2는 본 발명의 일 실시예에 따른 데이터 기밀성 보장 방법을 설명하는 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 데이터 기밀성 보장 방법을 이용하는 데이터 공유 방법을 설명하는 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 제 2 정보 처리 장치의 실행 환경을 검증하는 것을 설명하는 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책을 검증하는 것을 설명하는 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 데이터 공유 시스템을 나타내는 블록도이다.

도 7은 본 발명의 일 실시예에 따른 데이터를 공유하는 정보 처리 장치의 구성을 설명하는 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0033] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0034] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0035] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0036] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0037] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0038] 이하에서 후술할 정보 처리 장치는 데이터를 생성하고 생성된 데이터에 대한 접근을 제어하는 CPU(Central Processing Unit) 또는 GPU(Graphics Processing Unit)와 같은 연산 장치, 생성된 데이터를 저장하기 위한 저장 장치, 저장된 데이터를 공유하기 위한 통신 모뎀과 같은 통신 장치를 구비할 수 있다. 이 때, 정보 처리 장치에서 생성된 데이터는 통신 장치를 통해 클라우드 저장 장치, 서버와 같은 원격 저장 장치에 기록될 수 있다.

[0039] 따라서, 정보 처리 장치는 연산 장치, 저장 장치 및 통신 장치를 구비하는 스마트폰(smart phone), 태블릿 PC(tablet PC), PMP(Portable Multimedia Player)와 같은 이동 통신 기기와 노트북, 컴퓨터, 스마트 가전 기기와 같은 정보 통신 단말기 및 서버일 수 있으나 이에 한정되는 것은 아니다.

[0040] 이하에서 정보 처리 장치를 제 1 정보 처리 장치와 제 2 정보 처리 장치로 구분하여 기재한 것은 유무선 네트워크로 연결된 정보 처리 장치 간의 데이터 공유에 있어 데이터를 제공하는 정보 처리 장치와 제공된 데이터에 접

근하는 정보 처리 장치에서 수행하는 프로세스가 상이함에 따라 이를 용이하게 구분하기 위함이다.

[0041] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0042] 도 2는 본 발명의 일 실시예에 따른 데이터 기밀성 보장 방법을 설명하는 흐름도이다.

[0043] 도 2를 참조하면, 데이터 기밀성 보장 방법은 바인딩 정보를 수집하는 단계(S100), 바인딩 키를 생성하여 제 1 정보 처리 장치에 제공하는 단계(S110), 제 1 정보 처리 장치로부터 바인딩 키로 암호화된 데이터 키를 수신하는 단계(S120) 및 암호화된 데이터 키를 바인딩 키로 복호화하여 데이터에 접근하는 단계(S130)를 포함할 수 있다.

[0044] 데이터 기밀성 보장 방법은 제 1 정보 처리 장치의 데이터에 접근하는 제 2 정보 처리 장치에 의해 수행될 수 있다. 여기서, 제 1 정보 처리 장치는 데이터를 생성하여 램(RAM: Random Access Memory), 롬(ROM: Read Only Memory), 플래시 메모리(Flash Memory)와 같은 제 1 정보 처리 장치 내의 로컬 저장소 또는 클라우드 서버, 웹 서버와 같은 원격 저장소에 저장할 수 있다.

[0045] 이 때, 제 1 정보 처리 장치와 제 2 정보 처리 장치는 USB(universal Serial Bus), 이더넷(Ethernet), FDDI(Fiber Distributed Data Interface), 와이파이(WiFi: Wireless-Fidelity), 3세대 이동 통신(3Generation), LTE(Long Term Evolution) 등의 다양한 유무선 통신 인터페이스로 연결되어 데이터를 공유할 수 있다.

[0046] 제 1 정보 처리 장치의 데이터에 접근함에 있어 데이터의 기밀성을 보장하기 위하여 먼저, 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 수집할 수 있다(S100).

[0047] 여기서, 바인딩 정보에 제 1 정보 처리 장치에 대한 보안 정책 정보가 포함되어 있는 것은 데이터를 가지는 제 1 정보 처리 장치와 데이터에 접근하는 제 2 정보 처리 장치의 실행 환경 및 보안 정책이 상이하기 때문에 제 2 정보 처리 장치에 데이터 사용시 필요한 제 1 정보 처리 장치의 보안 정책을 적용하기 때문이다.

[0048] 바인딩 정보를 기반으로 바인딩 키를 생성하여 제 1 정보 처리 장치에 제공할 수 있다(S110). 여기서, 바인딩 키는 바인딩 공개키와 바인딩 비밀키의 쌍으로 생성될 수 있다. 이 때, 바인딩 공개키는 데이터 키를 암호화하는데 이용되며 바인딩 비밀키는 데이터 키를 복호화하는데 이용될 수 있다. 따라서, 제 1 정보 처리 장치에 제공하는 바인딩 키는 바인딩 공개키를 의미할 수 있다.

[0049] 제 1 정보 처리 장치는 바인딩 공개키를 이용하여 데이터 키를 암호화하여 제 2 정보 처리 장치로 제공할 수 있다. 즉, 제 1 정보 처리 장치로부터 암호화된 데이터 키를 수신하면(S120) 바인딩 비밀키로 암호화된 데이터 키를 복호화함으로써 제 1 정보 처리 장치의 데이터에 접근할 수 있다(S130).

[0050] 이와 같이, 바인딩 키를 이용하여 데이터 키를 보호하면 허용되지 않은 정보 처리 장치가 데이터를 소유하는 장치의 데이터 키를 가지고 있더라도 바인딩 공개키로 암호화되어 있는 데이터 키에 대한 바인딩 정보를 복호화할 수 없기 때문에 데이터에 접근할 수 없다. 이로써, 데이터에 대한 기밀성을 보장할 수 있다.

[0051] 도 3은 본 발명의 일 실시예에 따른 데이터 기밀성 보장 방법을 이용하는 데이터 공유 방법을 설명하는 흐름도이고, 도 4는 본 발명의 일 실시예에 따른 제 2 정보 처리 장치의 실행 환경을 검증하는 것을 설명하는 흐름도이다.

[0052] 또한, 도 5는 본 발명의 일 실시예에 따른 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책을 검증하는 것을 설명하는 흐름도이다.

[0053] 도 3 내지 도 5를 참조하면, 데이터 공유 방법은 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하는 단계(S200), 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성을 검증하는 단계(S300) 및 제 2 정보 처리 장치의 바인딩 키를 이용하여 제 2 정보 처리 장치와 데이터를 공유하는 단계(S400)를 포함할 수 있다.

[0054] 또한, 제 2 정보 처리 장치의 실행 환경에 대한 무결성 검증 또는 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성 검증 결과에 따라 제 2 정보 처리 장치와의 데이터 공유를 중단하는

단계(S410)를 더 포함할 수 있다.

[0055] 데이터 공유 방법은 데이터를 가진 제 1 정보 처리 장치에 의해 수행될 수 있다.

[0056] 제 1 정보 처리 장치와 네트워크로 연결된 제 2 정보 처리 장치가 제 1 정보 처리 장치에 데이터에 대한 공유를 요청함에 따라 제 1 정보 처리 장치는 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증할 수 있다(S200).

[0057] 보다 구체적으로, 제 2 정보 처리 장치의 실행 환경에 대한 무결성을 검증하기 위해 도 4에 도시된 바와 같이 공인된 인증 기관으로부터 제 2 정보 처리 장치에 대한 인증서를 획득할 수 있다(S210).

[0058] 인증서를 획득한 후, 제 2 정보 처리 장치의 실행 환경에 대한 무결성 정보를 요청하여 실행 환경 전자 서명을 수신할 수 있다(S220). 여기서, 실행 환경 전자 서명은 제 2 정보 처리 장치에서 제 1 정보 처리 장치의 요청을 수신함에 따라 제 2 정보 처리 장치에 대한 사용자 정보 및 실행 환경 정보를 포함하는 무결성 정보를 인증서의 비밀키로 전자 서명하여 생성될 수 있다.

[0059] 그리하여, 실행 환경 전자 서명을 인증서의 공개키를 이용하여 검증함으로써 제 2 정보 처리 장치에 대한 무결성을 검증할 수 있다(S230). 만약, 제 2 정보 처리 장치에 대한 무결성 검증에 실패하는 경우에는 제 2 정보 처리 장치의 실행 환경이 안전하지 않다고 판단하여 데이터의 공유를 중단할 수 있다(S410).

[0060] 제 2 정보 처리 장치의 실행 환경에 대한 무결성이 검증됨에 따라 데이터를 사용하는데 필요한 제 1 정보 처리 장치의 보안 정책 정보를 제 2 정보 처리 장치에 전송하여 적용시킬 수 있다. 이 때, 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보가 훼손되지 않았는지 무결성을 검증할 수 있다(S300).

[0061] 구체적으로, 도 5에 도시된 바와 같이 제 2 정보 처리 장치의 보안 정책에 대한 무결성 정보를 요청하여 보안 정책 전자 서명을 수신할 수 있다(S310). 여기서, 보안 정책 전자 서명은 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성 정보를 인증서의 비밀키로 전자 서명함으로써 생성될 수 있다.

[0062] 그리하여, 보안 정책 전자 서명을 인증서의 공개키를 이용하여 검증함으로써 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보의 무결성을 검증할 수 있다(S320).

[0063] 이 때, 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성 검증에 실패하는 경우 제 1 정보 처리 장치의 보안 정책 정보가 제 2 정보 처리 장치로 전송되는 동안 훼손되거나 유출되었다고 판단하여 제 2 정보 처리 장치와의 데이터 공유를 중단할 수 있다(S410).

[0064] 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보에 대한 무결성이 검증됨에 따라 제 2 정보 처리 장치로부터 수신한 바인딩 키를 이용하여 데이터를 공유할 수 있다(S400).

[0065] 바인딩 키는 제 2 정보 처리 장치에서 제 1 정보 처리 장치의 요청에 따라 제 2 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보 및 제 1 정보 처리 장치에 대한 보안 정책 정보를 포함하는 바인딩 정보를 기반으로 바인딩 공개키와 바인딩 비밀키의 쌍으로 생성될 수 있다.

[0066] 이 때, 바인딩 공개키는 데이터 키를 암호화하는데 이용되며 바인딩 비밀키는 암호화된 데이터 키를 복호화하는데 이용될 수 있다. 따라서, 제 1 정보 처리 장치에 제공된 바인딩 키는 바인딩 공개키를 의미할 수 있다.

[0067] 바인딩 공개키를 이용하여 데이터 키를 암호화하여 제 2 정보 처리 장치에 전송한 후, 제 2 정보 처리 장치에서 암호화된 데이터 키를 바인딩 비밀키로 복호화하면 제 2 정보 처리 장치에 데이터 접근 권한을 부여함으로써 데이터를 공유할 수 있다.

[0068] 도 6은 본 발명의 일 실시예에 따른 데이터 공유 시스템을 나타내는 블록도이다.

[0069] 도 6을 참조하면, 데이터 공유 시스템(100)은 데이터를 제공하는 제 1 정보 처리 장치(110) 및 제 1 정보 처리 장치의 데이터에 접근하는 제 2 정보 처리 장치(120)에 의해 구현될 수 있다.

[0070] 이 때, 제 1 정보 처리 장치(110)와 제 2 정보 처리 장치(120)는 USB(universal Serial Bus), 이더넷(Ethernet), FDDI(Fiber Distributed Data Interface), 와이파이(WiFi: Wireless-Fidelity), 3세대 이동 통신(3Generation), LTE(Long Term Evolution) 등의 다양한 유무선 통신 인터페이스로 연결되어 데이터를 공유할 수 있다.

[0071] 제 1 정보 처리 장치는 데이터를 생성하여 램(RAM: Random Access Memory), 롬(ROM: Read Only Memory), 플래시 메모리(Flash Memory)와 같은 제 1 정보 처리 장치 내의 로컬 저장부(117) 또는 클라우드 서버, 웹 서버와 같은 원격 저장부(130)에 저장할 수 있다.

[0072] 그리하여, 제 1 정보 처리 장치(110)는 로컬 저장소 및 원격 저장소에 저장된 데이터에 접근하고자 하는 제 2 정보 처리(120)의 실행 환경 및 보안 정책에 대한 무결성을 검증하고, 제 2 정보 처리 장치(120)로부터 수신한 바인딩 키를 이용하여 데이터 키를 관리함으로써 제 2 정보 처리 장치(120)에 데이터를 제공할 수 있다.

[0073] 제 1 정보 처리 장치(110)는 실행 환경 검증부(111), 보안 정책 검증부(113) 및 데이터 공유부(115)를 포함할 수 있다.

[0074] 실행 환경 검증부는(111)는 로컬 저장부(117) 또는 원격 저장부(130)에 기록된 데이터에 접근하고자 하는 제 2 정보 처리 장치(120)의 실행 환경에 대한 무결성을 검증할 수 있다.

[0075] 보다 구체적으로, 제 2 정보 처리 장치(120)의 실행 환경에 대한 무결성을 검증하기 위해 공인 인증 기관으로부터 제 2 정보 처리 장치(120)에 대한 인증서를 획득할 수 있다.

[0076] 인증서를 획득한 후, 제 2 정보 처리 장치(120)로부터 실행 환경 전자 서명을 수신할 수 있다. 여기서, 실행 환경 전자 서명은 제 2 정보 처리 장치(120)에서 제 1 정보 처리 장치(110)의 정보 요청을 수신함에 따라 제 2 정보 처리 장치(120)에 대한 사용자 정보 및 실행 환경 정보를 포함하는 무결성 정보를 인증서의 비밀키로 전자 서명함으로써 생성될 수 있다.

[0077] 그리하여, 실행 환경 전자 서명을 인증서의 공개키를 이용하여 검증함으로써 제 2 정보 처리 장치에 대한 무결성을 검증할 수 있다. 이 때, 제 2 정보 처리 장치에 대한 무결성 검증에 실패하는 경우에는 제 2 정보 처리 장치의 실행 환경이 안전하지 않다고 판단하여 데이터의 공유를 중단할 수 있다.

[0078] 보안 정책 검증부(113)는 제 2 정보 처리 장치(120)의 실행 환경에 대한 무결성이 검증되면 데이터를 사용하는데 필요한 제 1 정보 처리 장치(110)의 보안 정책 정보를 제 2 정보 처리 장치(120)에 전송하여 적용시키는데 이 때, 제 2 정보 처리 장치(120)에 적용된 제 1 정보 처리 장치(110)의 보안 정책 정보가 훼손되지 않았는지 무결성을 검증할 수 있다.

[0079] 보다 구체적으로, 제 2 정보 처리 장치(120)로부터 보안 정책 전자 서명을 수신할 수 있다. 여기서, 보안 정책 전자 서명은 제 2 정보 처리 장치(120)에 적용된 제 1 정보 처리 장치(110)의 보안 정책 정보에 대한 무결성 정보를 인증서의 비밀키로 전자 서명함으로써 생성될 수 있다.

[0080] 그리하여, 보안 정책 전자 서명을 인증서의 공개키를 이용하여 검증함으로써 제 2 정보 처리 장치에 적용된 제 1 정보 처리 장치의 보안 정책 정보의 무결성을 검증할 수 있다.

[0081] 이 때, 제 1 정보 처리 장치(110)의 보안 정책 정보에 대한 무결성 검증에 실패하는 경우 제 1 정보 처리 장치(110)의 보안 정책 정보가 제 2 정보 처리 장치(120)로 전송되는 동안 훼손되거나 유출되었다고 판단하여 제 2 정보 처리 장치(120)와의 데이터 공유를 중단할 수 있다.

[0082] 데이터 공유부(115)는 제 2 정보 처리 장치(120)에 적용된 제 1 정보 처리 장치(110)의 보안 정책 정보에 대한 무결성이 검증됨에 따라 제 2 정보 처리 장치(120)로부터 수신한 바인딩 키를 이용하여 데이터를 공유할 수 있다.

[0083] 여기서, 바인딩 키는 제 2 정보 처리 장치(120)에서 제 1 정보 처리 장치(110)의 요청을 수신함에 따라 제 2 정보 처리 장치(120)에 대한 사용자 정보, 실행 환경 정보 및 제 1 정보 처리 장치(110)에 대한 보안 정책 정보를 포함하는 바인딩 정보를 기반으로 바인딩 공개키와 바인딩 비밀키의 쌍으로 생성될 수 있다.

[0084] 이 때, 바인딩 공개키는 데이터 키를 암호화하는데 이용되며 바인딩 비밀키는 암호화된 데이터 키를 복호화하는데 이용될 수 있다. 따라서, 제 1 정보 처리 장치(120)에 제공되는 바인딩 키는 바인딩 공개키를 의미할 수 있다.

[0085] 즉, 바인딩 공개키를 이용하여 데이터 키를 암호화하여 제 2 정보 처리 장치(120)에 전송한 후, 제 2 정보 처리 장치(120)에 의해 바인딩 비밀키로 암호화된 데이터 키가 복호화되면 제 2 정보 처리 장치(120)에 데이터 접근 권한을 부여함으로써 데이터를 공유할 수 있다.

[0086] 제 2 정보 처리 장치(120)는 제 1 정보 처리 장치(110)의 요청에 따라 실행 환경 전자 서명, 보안 정책 전자 서

명 및 바인딩 키 중 적어도 하나를 생성하여 제 1 정보 처리 장치(110)에 제공하고, 바인딩 키를 이용하여 제 1 정보 처리 장치(110)의 데이터에 접근함으로써 제 1 정보 처리 장치(110)의 데이터를 제공받을 수 있다.

[0087] 제 2 정보 처리 장치(120)는 바인딩 정보 수집부(121), 바인딩 키 생성부(123) 및 데이터 접근부(125)를 포함할 수 있다. 또한, 도 6에 도시되지는 않았으나 제 1 정보 처리 장치(110)의 요청에 따라 전자 서명을 생성하는 전자 서명 생성부를 더 포함할 수 있다.

[0088] 제 2 정보 처리 장치(120)가 제 1 정보 처리 장치(110)의 데이터 접근하고자 하면 제 1 정보 처리 장치(110)는 제 2 정보 처리 장치(120)에 대한 무결성을 검증할 수 있다.

[0089] 따라서, 전자 서명 생성부는 제 1 정보 처리 장치(110)의 요청에 따라 제 2 정보 처리 장치(120)에 대한 실행 환경 전자 서명을 생성할 수 있다. 여기서, 실행 환경 전자 서명은 제 2 정보 처리 장치(120)에 대한 사용자 정보 및 실행 환경 정보를 포함하는 무결성 정보를 인증서의 비밀키로 전자 서명함으로써 생성될 수 있다.

[0090] 제 1 정보 처리 장치(110)에 의해 제 2 정보 처리 장치(120)의 실행 환경에 대한 무결성이 검증되면 데이터를 사용하는데 필요한 제 1 정보 처리 장치(110)의 보안 정책 정보를 제 2 정보 처리 장치(120)에 적용시킬 수 있다. 이 때, 제 2 정보 처리 장치(120)에 적용된 제 1 정보 처리 장치(110)의 보안 정책 정보가 훼손되지 않았는지 무결성을 검증할 수 있다.

[0091] 따라서, 전자 서명 생성부는 제 2 정보 처리 장치(120)에 적용된 제 1 정보 처리 장치(110)의 보안 정책 정보에 대한 무결성 정보를 인증서의 비밀키로 전자 서명함으로써 생성될 수 있다.

[0092] 제 2 정보 처리 장치(120)에 대한 실행 환경 정보 및 제 2 정보 처리 장치(120)에 적용된 제 1 정보 처리 장치(110)의 보안 정책 정보에 대한 무결성이 검증됨에 따라 바인딩 정보를 기반으로 생성된 바인딩 키를 이용하여 데이터를 공유할 수 있다.

[0093] 바인딩 정보 수집부(121)는 제 2 정보 처리 장치(120)에 대한 사용자 정보, 실행 환경 정보 및 제 1 정보 처리 장치(110)에 대한 보안 정책 정보를 포함하는 바인딩 정보를 수집할 수 있다.

[0094] 이 때, 바인딩 정보 수집부(121)에 의해 수집된 바인딩 정보는 데이터가 실행되는 실행 환경과 독립되는 하드웨어 기반의 보안 칩에 기록됨으로써 바인딩 정보에 대한 무결성을 보장할 수 있다. 여기서, 하드웨어 기반의 보안 칩은 신뢰 플랫폼 모듈(Trusted Platform Module, TPM)을 의미할 수 있으나 이에 한정되지 않고 바인딩 정보에 대한 무결성을 보장할 수 있는 하드웨어 기반의 저장 장치가 포함될 수 있다.

[0095] 바인딩 정보에 제 1 정보 처리 장치(110)에 대한 보안 정책 정보가 포함되어 있는 것은 데이터를 가지는 제 1 정보 처리 장치(110)와 데이터에 접근하는 제 2 정보 처리 장치(120)의 실행 환경 및 보안 정책이 상이하기 때문에 제 2 정보 처리 장치(120)에 데이터 사용시 필요한 제 1 정보 처리 장치(110)의 보안 정책을 적용하기 때문이다.

[0096] 바인딩 키 생성부(123)는 바인딩 정보를 기반으로 바인딩 키를 생성할 수 있다. 특히, 바인딩 키는 바인딩 공개키와 바인딩 비밀키의 쌍으로 생성될 수 있으며 이 때, 바인딩 공개키는 데이터 키를 암호화하는데 이용되며 바인딩 비밀키는 바인딩 공개키로 암호화되어 있는 데이터 키를 복호화하는데 이용될 수 있다.

[0097] 여기서, 바인딩 공개키와 바인딩 비밀키는 바인딩 키 생성 당시의 바인딩 정보에 의해 생성되기 때문에 악의적인 목적으로 실행 환경 및 보안 정책이 훼손되거나 허용되지 않은 사용자에 의한 접근이 시도되는 경우, 바인딩 공개키로 암호화된 데이터 키의 바인딩성을 해제할 수 없으므로 데이터에 접근할 수 없다는 점에서 효율적으로 데이터 또는 데이터 키의 무결성을 보장할 수 있다.

[0098] 데이터 접근부(125)는 제 1 정보 처리 장치(110)로부터 바인딩 공개키로 암호화된 데이터 키를 수신하고, 암호화된 데이터 키를 바인딩 비밀키로 복호화하여 제 1 정보 처리 장치(110)의 데이터에 접근할 수 있다.

[0099] 보다 구체적으로, 암호화된 데이터 키가 바인딩 비밀키로 복호화되면 복호화된 데이터 키를 데이터 접근부(125)로 전송할 수 있다. 그리하여, 제 1 정보 처리 장치(110)의 암호화된 데이터를 복호화함으로써 제 1 정보 처리 장치(110)의 데이터에 접근할 수 있다.

[0100] 이와 같이, 바인딩 키를 이용하여 데이터 키를 보호하면, 허용되지 않은 정보 처리 장치가 제 1 정보 처리 장치(110)의 데이터 키를 가지고 있더라도 바인딩 공개키로 암호화되어 있는 데이터 키에 대한 바인딩성은 복호화할 수 없기 때문에 데이터에 접근할 수 없다는 점에서 데이터에 대한 기밀성을 보장할 수 있다.

[0101] 도 7은 본 발명의 일 실시예에 따른 데이터를 공유하는 정보 처리 장치의 구성을 설명하는 예시도이다.

[0102] 도 7을 참조하면, 데이터를 공유하는 제 1 정보 처리 장치(200)와 제 2 정보 처리 장치(300)는 동일하게 구성될 수 있다.

[0103] 그리하여, 제 1 정보 처리 장치(200)와 제 2 정보 처리 장치(300)는 데이터를 사용하는 프로세스/가상머신(205)이 구동되는 데이터 실행 환경(201), 데이터 실행 환경(201)에서 생성되는 데이터를 암호화하거나 보안 정책을 적용하는 데이터 보호 모듈(203) 및 제 2 정보 처리 장치의 실행 환경 및 보안 정책을 검증하거나 데이터 키 또는 바인딩 키를 관리하는 관리 컴포넌트(210)로 구성될 수 있다.

[0104] 여기서, 관리 컴포넌트(210)는 인텔 TXT(Trustred eXecution Technology), AMD SVM(Secure Virtual Machine), ARM TrustZone, SMM(System Management Mode)과 같은 하드웨어 기반의 보안 기술을 이용하여 구현될 수 있으며 이로써 데이터 실행 환경(201)으로부터 독립되는 최상위 권한을 부여받을 수 있다.

[0105] 관리 컴포넌트(210)는 무결성 정보 저장소(211), 실행 환경 검증 수단(213), 키 관리 수단(215) 및 보안 정책 관리 수단(217)을 포함할 수 있다.

[0106] 무결성 정보 저장소(211)는 각각의 정보 처리 장치에 대한 사용자 정보, 실행 환경 정보, 데이터 보호 모듈(203)에 대한 무결성 정보 및 데이터 보호 모듈(203)에 적용되어 있는 보안 정책 정보 중 적어도 하나를 포함하는 바인딩 정보가 기록될 수 있다.

[0107] 무결성 정보 저장소(211)는 하드웨어 기반의 보안 기술이 구현된 관리 컴포넌트(210) 내의 메모리 또는 하드웨어 보안칩인 신뢰 플랫폼 모듈(TPM: Trusted Platform Module)에 구현됨으로써 바인딩 정보에 대한 무결성을 보장할 수 있다.

[0108] 실행 환경 검증 수단(213)은 무결성 정보 저장소(211)에 저장된 바인딩 정보를 기반으로 데이터가 공유될 사용자 정보 또는 실행 환경을 검증하거나 데이터를 제공하는 정보 처리 장치의 보안 정책이 적용되었는지와 그 무결성을 검증할 수 있다.

[0109] 키 관리 수단(215)은 무결성 정보 저장소(211)에 저장된 바인딩 정보를 기반으로 바인딩 키를 생성하고, 바인딩 키를 이용하여 데이터 키를 보호할 수 있다.

[0110] 특히, 바인딩 키는 바인딩 공개키와 바인딩 비밀키의 쌍으로 생성되며 바인딩 공개키를 이용하여 데이터 키를 암호화하고 바인딩 비밀키를 이용하여 암호화된 데이터 키를 복호화할 수 있다.

[0111] 이 때, 키 관리 수단(215)은 신뢰 컴퓨팅 그룹(TCG: Trusted Computing Group)의 신뢰 플랫폼 모듈(TPM: Trusted Platform Module)의 바인딩 키 기능을 통해 바인딩 키를 생성할 수 있다.

[0112] 보안 정책 관리 수단(217)은 데이터를 사용할 프로세스/가상머신(205)에 적용시킬 보안 정책을 정의하여 데이터 보호 모듈(203)에 적용하거나 데이터에 접근하고자 하는 정보 처리 장치의 데이터 보호 모듈(203)에 적용시킬 수 있다.

[0113] 즉, 데이터 보호 모듈(203)에 적용된 보안 정책에 기반하여 데이터를 관리하되, 바인딩 키로 보호되는 데이터 키로 암호화된 데이터를 로컬 저장소(220) 또는 원격 저장소(230)에 저장할 수 있다.

[0114] 따라서, 데이터에 접근하고자 하는 정보 처리 장치의 사용자 정보가 허용되지 않은 경우, 데이터 보호 모듈(203)에 데이터를 소유하는 정보 처리 장치에서 정의된 보안 정책이 적용되지 않은 경우, 데이터 실행 환경(201)에 대한 무결성이 훼손되었을 경우는 데이터 키를 보호하는 바인딩 키의 사용이 불가능함에 따라 프로세스/가상머신(205) 및 데이터 실행 환경(201)에서의 데이터 접근이 불가능할 수 있다.

[0115] 본 발명에서 제 1 정보 처리 장치(200)는 데이터를 생성하여 기록하는 데이터 소유 장치이고 제 2 정보 처리 장치(300)는 제 1 정보 처리 장치(200)가 소유하는 데이터에 접근하여 데이터를 공유받은 데이터 접근 장치를 의미할 수 있으나, 이러한 구분은 정보 처리 장치 간의 데이터 공유에 있어 용이하게 구분하기 위한 것이므로 한정되는 것은 아니다.

[0116] 상술한 바와 같은 본 발명의 실시예에 따른 데이터 기밀성 보장 방법, 이를 이용하는 데이터 공유 방법 및 시스

템에 따르면, 첫째, 데이터를 가지는 정보 처리 장치에 의해 정의된 실행 환경 및 보안 정책이 적용된 정보 처리 장치에 한하여 데이터에 대한 접근을 허용할 수 있다.

[0117] 둘째, 데이터를 가지는 정보 처리 장치에 의해 정의된 실행 환경 및 보안 정책이 구성되어 있는 정보 처리 장치와는 데이터의 기밀성을 유지함과 동시에 안전한 데이터 공유를 보장할 수 있다.

[0118] 셋째, 데이터에 대한 접근이 허용되지 않은 정보 처리 기기와 실행 환경 또는 보안 정책이 훼손된 정보 처리 장치에서는 데이터 키를 가지고 있더라도 데이터 키에 암호화된 바인딩 키를 복호화할 수 없기 때문에 데이터의 기밀성을 보장할 수 있다.

[0119] 넷째, 바인딩 키를 생성함에 있어 사용자 정보, 실행 환경 및 보안 정책뿐 아니라 정보 처리 장치의 다양한 정보를 부가적으로 바인딩할 수 있으므로 데이터 기밀성에 대한 보장이 필요한 다양한 시스템으로 확장될 수 있다.

[0120] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

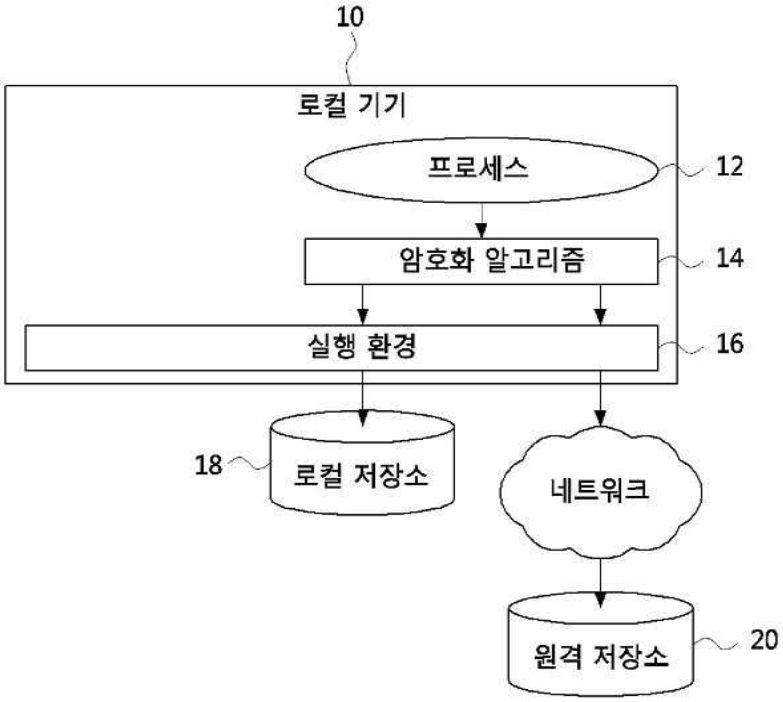
부호의 설명

[0121]

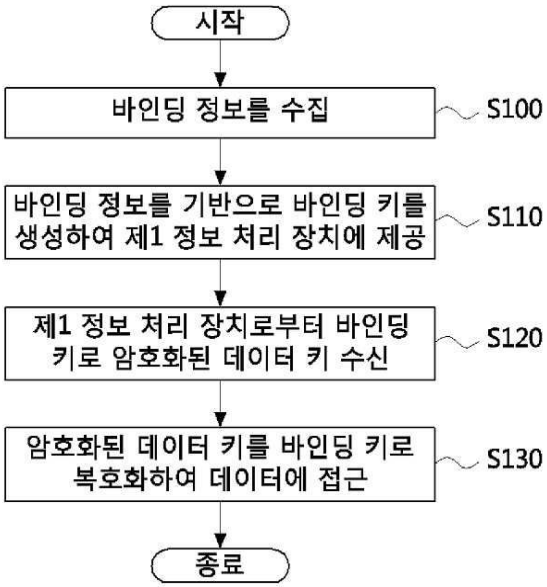
10: 로컬 기기
12: 프로세스
14: 암호화 알고리즘
16: 실행 환경
18: 로컬 저장소
20: 원격 저장소
100: 데이터 공유 시스템
110: 제 1 정보 처리 장치
111: 실행 환경 검증부
113: 보안 정책 검증부
115: 데이터 공유부
117: 로컬 저장부
120: 제 2정보 처리 장치
121: 바인딩 정보 수집부
123: 바인딩 키 생성부
125: 데이터 접근부
130: 원격 저장부
200: 제 1 정보 처리 장치
201: 데이터 실행 환경
203: 데이터 보호 모듈
205: 프로세스/가상머신
210: 관리 컴포넌트
211: 무결성 정보 저장소
213: 실행 환경 검증 수단
215: 키 관리 수단
217: 보안 정책 관리 수단
220: 로컬 저장소
230: 원격 저장소
300: 제 2 정보 처리 장치

도면

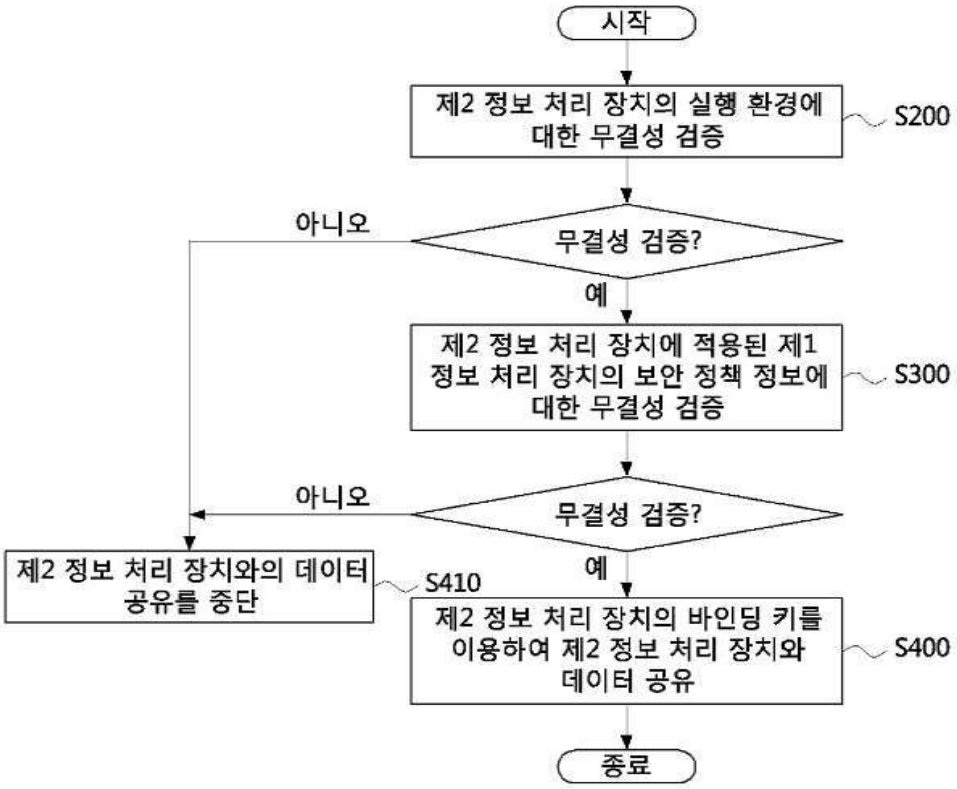
도면1


10
로컬 기기
프로세스
12
암호화 알고리즘
14
실행 환경
16
18
로컬 저장소
네트워크
원격 저장소
20

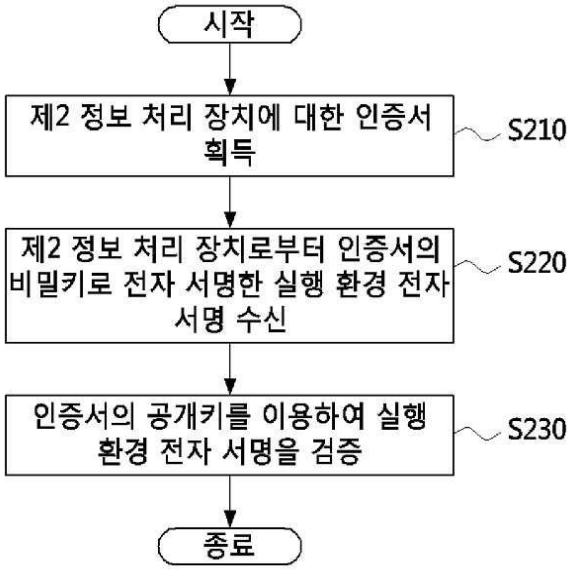
도면2


시작
바인딩 정보를 수집
S100
바인딩 정보를 기반으로 바인딩 키를 생성하여 제1 정보 처리 장치에 제공
S110
제1 정보 처리 장치로부터 바인딩 키로 암호화된 데이터 키 수신
S120
암호화된 데이터 키를 바인딩 키로 복호화하여 데이터에 접근
S130
종료

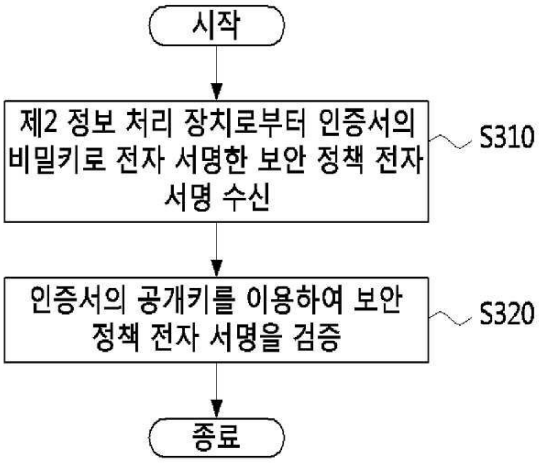
도면3


시작
제2 정보 처리 장치의 실행 환경에 대한 무결성 검증
S200
무결성 검증?
아니오
예
제2 정보 처리 장치에 적용된 제1 정보 처리 장치의 보안 정책 정보에 대한 무결성 검증
S300
무결성 검증?
아니오
예
제2 정보 처리 장치와의 데이터 공유를 중단
S410
제2 정보 처리 장치의 바인딩 키를 이용하여 제2 정보 처리 장치와 데이터 공유
S400
종료

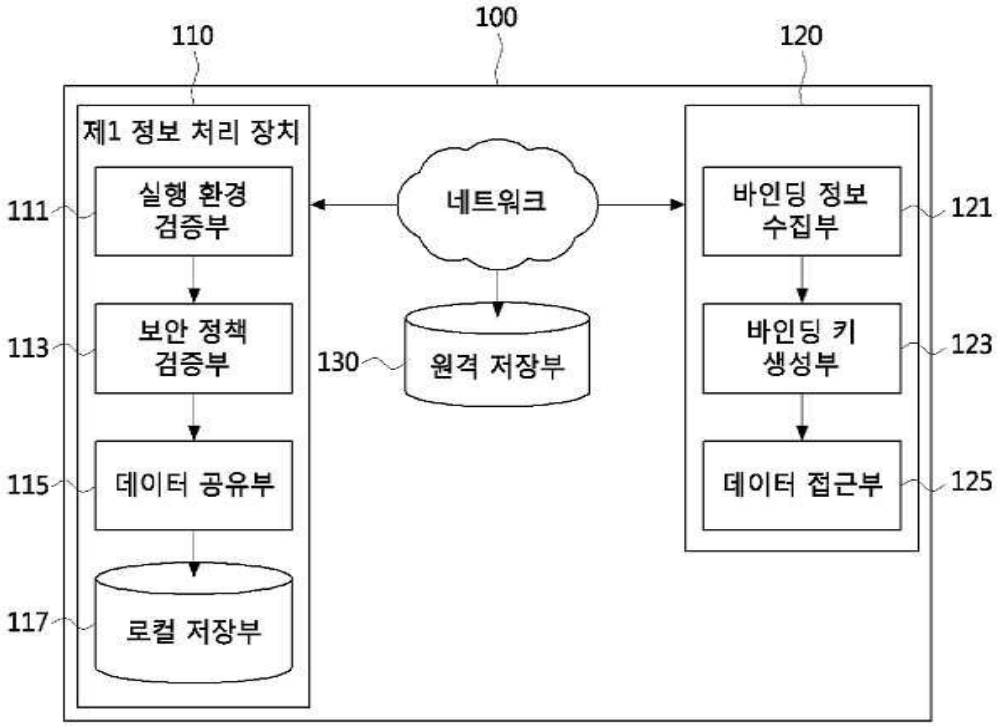
도면4


시작
제2 정보 처리 장치에 대한 인증서 획득
S210
제2 정보 처리 장치로부터 인증서의 비밀키로 전자 서명한 실행 환경 전자 서명 수신
S220
인증서의 공개키를 이용하여 실행 환경 전자 서명을 검증
S230
종료

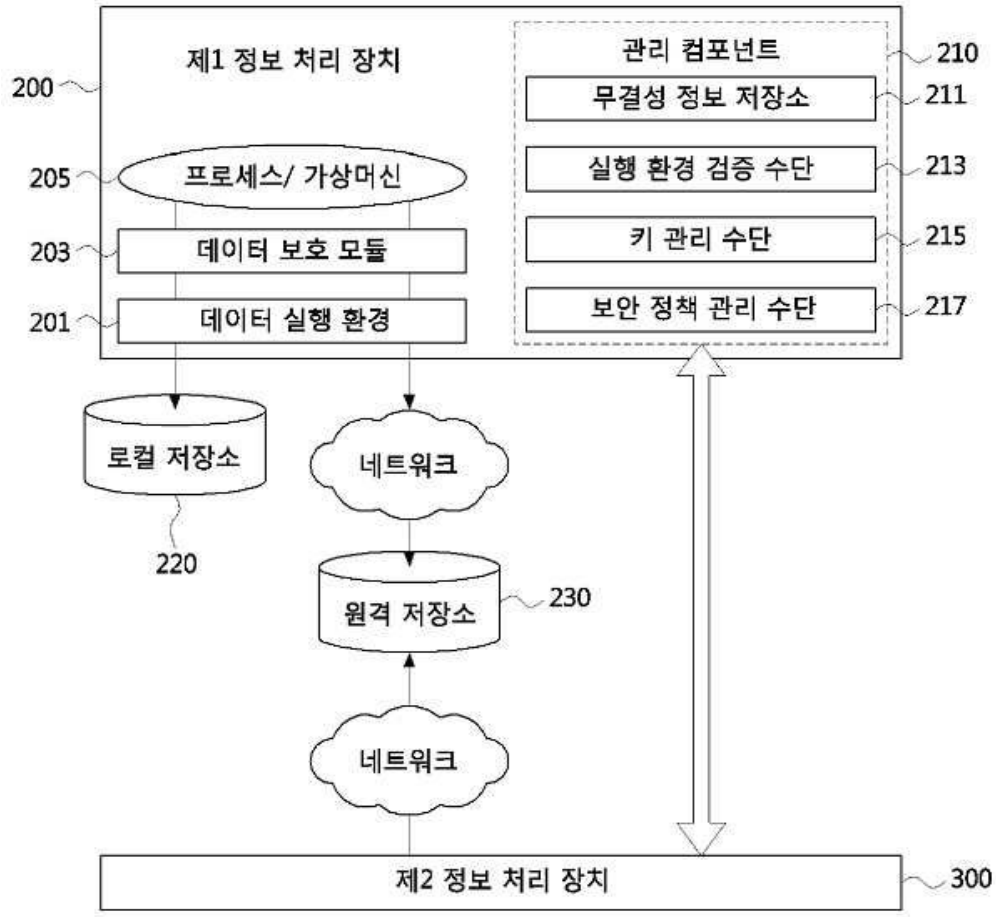
도면5


시작
제2 정보 처리 장치로부터 인증서의 비밀키로 전자 서명한 보안 정책 전자 서명 수신
S310
인증서의 공개키를 이용하여 보안 정책 전자 서명을 검증
S320
종료

도면6


100
110
120
제1 정보 처리 장치
실행 환경 검증부
111
보안 정책 검증부
113
데이터 공유부
115
로컬 저장부
117
네트워크
원격 저장부
130
바인딩 정보 수집부
121
바인딩 키 생성부
123
데이터 접근부
125

도면7


제1 정보 처리 장치
200
관리 컴포넌트
210
무결성 정보 저장소
211
실행 환경 검증 수단
213
키 관리 수단
215
보안 정책 관리 수단
217
205
프로세스/ 가상머신
203
데이터 보호 모듈
201
데이터 실행 환경
로컬 저장소
220
네트워크
원격 저장소
230
네트워크
제2 정보 처리 장치
300