(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0046390
(43) 공개일자 2019년05월07일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
H04L 63/0209 (2013.01)
H04L 63/0227 (2013.01)
(21) 출원번호 10-2017-0140139
(22) 출원일자 2017년10월26일
심사청구일자 2017년10월26일
기술이전 희망 : 기술양도

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
오지수
대전광역시 유성구 신성남로 121
원종진
대전광역시 유성구 어은로 57, 116동 1004호
(뒷면에 계속)
(74) 대리인
한양특허법인

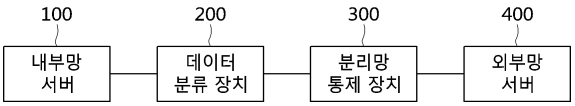
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **데이터 분류 장치, 분리망 통제 장치 및 분리망 간 데이터 통제 방법**

(57) 요 약

데이터 분류 장치, 분리망 통제 장치 및 분리망 간 데이터 통제 방법이 개시된다. 본 발명에 따른 분리망 통제 장치는, 내부망 서버와 연결된 데이터 분류 장치로부터 데이터를 수신하는 내부망 운용부, 상기 데이터 분류 장치에 대한 검증 및 상기 내부망 서버의 데이터에 대한 검증을 수행하고, 검증의 수행 결과를 기반으로 상기 내부망 서버의 데이터가 외부망 서버로 전송되는 것을 통제하는 데이터 통제부, 그리고 상기 검증에 성공한 경우, 상기 내부망 서버의 데이터를 상기 외부망 서버로 전송하는 외부망 운용부를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/12 (2013.01)
H04L 9/0643 (2013.01)
(72) 발명자
박성진
대전광역시 유성구 엑스포로 448, 304동 1602호
안정철
대전광역시 유성구 배울2로 61, 1016동 1003호
강철오
대전광역시 서구 청사로 254, 111동 1004호
오윤근
세종특별자치시 달빛로 80, 1208동 302호
심재화
대전광역시 유성구 죽동로298번길 84, 202호

명 세 서

청구범위

청구항 1

내부망 서버와 연결된 데이터 분류 장치로부터 데이터를 수신하는 내부망 운용부,

상기 데이터 분류 장치에 대한 검증 및 상기 내부망 서버의 데이터에 대한 검증을 수행하고, 검증의 수행 결과를 기반으로 상기 내부망 서버의 데이터가 외부망 서버로 전송되는 것을 통제하는 데이터 통제부, 그리고

상기 검증에 성공한 경우, 상기 내부망 서버의 데이터를 상기 외부망 서버로 전송하는 외부망 운용부

를 포함하는 분리망 통제 장치.

청구항 2

제1항에 있어서,

상기 데이터 통제부는,

상기 데이터 분류 장치에 대한 검증을 수행하는 데이터 분류 장치 검증 모듈,

상기 데이터 분류 장치가 분리망 통제 기능에 대한 검증을 수행하도록, 상기 데이터 분류 장치로 전송할 통제 QUOTE를 생성하는 통제 QUOTE 생성 모듈, 그리고

상기 데이터의 HMAC 값을 기반으로 상기 데이터에 대한 검증을 수행하여, 상기 내부망 서버의 데이터가 상기 외부망 서버로 전송되는 것을 통제하는 데이터 검증 모듈

을 포함하는 것을 특징으로 하는 분리망 통제 장치

청구항 3

제2항에 있어서,

상기 데이터 분류 장치 검증 모듈은,

기 저장된 분류 엔클레이브 정보와 상기 데이터 분류 장치로부터 수신된 분류 QUOTE의 엔클레이브 정보를 비교하여, 상기 데이터 분류 장치에 대한 무결성을 검증하는 것을 특징으로 하는 분리망 통제 장치.

청구항 4

제2항에 있어서,

상기 내부망 운용부는,

생성된 상기 통제 QUOTE를 상기 데이터 분류 장치로 전송하고, 상기 통제 QUOTE를 기반으로 분리망 통제 장치에 대한 검증을 수행한 상기 데이터 분류 장치로부터 상기 데이터 및 상기 HMAC 값을 수신하여, 상기 데이터 통제부로 전달하는 것을 특징으로 하는 분리망 통제 장치.

청구항 5

제2항에 있어서,

상기 데이터 검증 모듈은,

상기 데이터 분류 장치와 디피 헬먼 파라미터를 교환하여 HMAC 키를 생성하고, 상기 HMAC 키를 이용하여 상기 데이터의 HMAC 값에 대한 검증을 수행하는 것을 특징으로 하는 분리망 통제 장치.

청구항 6

제2항에 있어서,

상기 데이터 통제부는,

상기 내부망 운용부로부터 상기 데이터를 전달받는 PIC 통신 모듈, 그리고

상기 외부망 운용부로 상기 데이터를 전달하는 외부망 통신 모듈을 더 포함하는 것을 특징으로 하는 분리망 통제 장치.

청구항 7

제2항에 있어서,

상기 데이터 통제부는,

소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 엔클레이브 상에서 동작하는 것을 특징으로 하는 분리망 통제 장치.

청구항 8

내부망 서버로부터 수신한 데이터가 외부망 서버로 전송 가능한 데이터인지 여부를 검사하여, 상기 데이터를 분류하는 데이터 검사부,

상기 외부망 서버와 연결된 분리망 통제 장치와 디피 헬먼 파라미터를 교환하여 HMAC 키를 생성하고, 상기 HMAC 키를 이용하여 상기 데이터의 HMAC 값을 생성하는 HMAC 생성부,

상기 분리망 통제 장치가 상기 데이터의 분류 기능에 대한 검증을 수행하도록, 상기 분리망 통제 장치로 전송할 분류 QUOTE를 생성하는 분류 QUOTE 생성부,

상기 분리망 통제 장치를 통하여 상기 데이터를 상기 외부망 서버로 전송할지 여부를 결정하기 위하여, 상기 분리망 통제 장치에 대한 검증을 수행하는 분리망 통제 장치 검증부, 그리고

검증이 완료된 상기 분리망 통제 장치로, 분류된 상기 데이터 및 상기 데이터의 HMAC 값을 전송하는 통신부

를 포함하는 데이터 분류 장치.

청구항 9

제8항에 있어서,

상기 데이터 검사부, 상기 HMAC 생성부, 상기 QUOTE 생성부 및 상기 분리망 통제 장치 검증부는,

소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 엔클레이브 상에서 동작하는 것을 특징으로 하는 데이터 분류 장치.

청구항 10

제9항에 있어서,

상기 QUOTE 생성부는,

상기 엔클레이브의 정보를 상기 소프트웨어 가드 확장(SGX) 프로세스의 비밀키로 서명하여, 상기 분류 QUOTE를 생성하는 것을 특징으로 하는 데이터 분류 장치.

청구항 11

제10항에 있어서,

상기 분리망 통제 장치 검증부는,

기 저장된 통제 엔클레이브 정보와 상기 분리망 통제 장치로부터 수신한 통제 QUOTE의 엔클레이브 정보를 비교하여, 상기 분리망 통제 장치에 대한 무결성을 검증하는 것을 특징으로 하는 데이터 분류 장치.

청구항 12

제9항에 있어서,

상기 HMAC 생성부는,

분류 디피 헬먼 파라미터 및 상기 분리망 통제 장치의 통제 디피 헬먼 파라미터를 조합하여 상기 HMAC 키를 생성하고, 상기 HMAC 키를 이용하여 분류가 완료된 상기 데이터에 대한 상기 HMAC 값을 생성하는 것을 특징으로 하는 데이터 분류 장치.

청구항 13

분리망 통제 장치에 의해 수행되는 분리망 간 데이터 통제 방법에 있어서,

내부망 서버와 연결된 데이터 분류 장치에 대한 검증을 수행하는 단계,

상기 데이터 분류 장치에 대한 검증에 성공한 경우, 상기 데이터 분류 장치로부터 수신된 상기 내부망 서버의 데이터에 대한 검증을 수행하는 단계, 그리고

검증의 수행 결과를 기반으로 상기 데이터가 상기 내부망 서버에 대응되는 외부망 서버로 전송되는 것을 통제하여, 상기 내부망 서버의 데이터를 외부망 서버로 전송하는 단계

를 포함하는 분리망 간 데이터 통제 방법.

청구항 14

제13항에 있어서,

상기 데이터 분류 장치에 대한 검증을 수행하는 단계는,

상기 데이터 분류 장치로부터 분류 QUOTE를 수신하는 단계,

수신된 상기 분류 QUOTE의 엔클레이브 정보와 기 저장된 분류 엔클레이브 정보를 비교하는 단계, 그리고

상기 엔클레이브 정보의 비교 결과를 기반으로, 상기 데이터 분류 장치의 무결성을 검증하는 단계

를 포함하는 것을 특징으로 하는 분리망 간 데이터 통제 방법.

청구항 15

제13항에 있어서,

상기 내부망 서버의 데이터에 대한 검증을 수행하는 단계는,

상기 데이터 분류 장치로부터 분류 디피 헬먼 파라미터를 수신하는 단계,

수신된 상기 분류 디피 헬먼 파라미터와, 통제 디피 헬먼 파라미터를 이용하여, HMAC 키를 생성하는 단계, 그리고

생성된 상기 HMAC 키를 이용하여, 상기 데이터의 HMAC 값을 검증하는 단계

를 포함하는 것을 특징으로 하는 분리망 간 데이터 통제 방법.

청구항 16

제15항에 있어서,

상기 데이터 분류 장치로 통제 QUOTE를 전송하여, 상기 데이터 분류 장치가 상기 분리망 통제 장치에 대한 검증을 수행하도록 하는 단계를 더 포함하는 것을 특징으로 하는 분리망 간 데이터 통제 방법.

청구항 17

제16항에 있어서,

상기 통제 QUOTE를 기반으로 상기 분리망 통제 장치에 대한 검증을 수행한 상기 데이터 분류 장치로부터 상기 내부망 서버의 데이터 및 상기 데이터의 HMAC 값을 수신하는 단계를 더 포함하는 것을 특징으로 하는 분리망 간 데이터 통제 방법.

청구항 18

제17항에 있어서,

상기 데이터 분류 장치로부터 수신된 상기 내부망 서버의 데이터는,

상기 데이터 분류 장치가, 상기 내부망 서버로부터 수신한 상기 데이터 중에서 외부망 서버로 전송 가능한 데이터인 것으로 판단하여 분류한 데이터인 것을 특징으로 하는 분리망 간 데이터 통제 방법.

청구항 19

제17항에 있어서,

상기 데이터의 HMAC 값은,

상기 데이터 분류 장치가 상기 분류 디피 헬먼 파라미터 및 상기 통제 디피 헬먼 파라미터를 이용하여 생성한 HMAC 키를 상기 데이터에 적용하여 생성한 것을 특징으로 하는 분리망 간 데이터 통제 방법.

청구항 20

제13항에 있어서,

상기 데이터 분류 장치 및 상기 분리망 통제 장치 각각은,

소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 엔클레이브 상에서 동작을 수행하는 것을 특징으로 하는 분리망 간 데이터 통제 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 분리망 간의 데이터 전송을 통제하는 기술에 관한 것으로, 특히 소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 실행 환경에서 분리망 간 전송 데이터를 통제하고, 안전한 전달 경로를 제공하는 분리망 통제 기술에 관한 것이다.

배 경 기 술

[0002] 정보 공유 및 상호 운용성이 강조되면서, 각각의 독립적인 네트워크상에서 운용되던 응용 서비스들의 망간 연동의 필요성이 요구되고 있다. 독립된 네트워크는 다른 네트워크간의 연동이 요구될 때 자신의 자원을 보호하기 위해 이를 직접 연결하지 않고 두 망간의 접점에 연동을 위한 별도의 시스템을 구축하여 분리망간 연동을 수행하고 있다.

[0003] 이러한 분리망간 연동 시스템은 특정 서비스에 대한 연동을 수행하며, 연동하고자 하는 응용서비스의 특성에 따라 연동 데이터의 통제 및 전달을 판단하고 있다.

[0004] 분리망간 연동 시스템은 기존의 오프라인(Off-line) 방식 또는 관리자에 의한 필터링 수행 후 승인된 자료만 전달하는 방식에 비해, 자동화되었으며, 신속하게 처리할 수 있다. 그러나 분리망간 연동 시스템의 자동화된 통제 기능을 수행하는 시스템이 안전성이 보장되지 않은 실행 영역에서 수행되므로, 해킹 등의 보안 위협으로부터 안전하지 않으며, 이로 인하여 연동 데이터의 신뢰성을 보장할 수 없다.

[0005] 따라서, 분리망 간 공유 자료에 대한 올바른 데이터 통제 과정을 거쳤는지 보장할 수 있는 실행 환경이 요구되고 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국 등록 특허 제10-0554172호, 2006년 02월 22일 공고(명칭: 네트워크 보안성을 강화한 무결성 관리 시스템, 이를구비한 무결성 네트워크 시스템 및 그 방법)

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은 분리망 연동 시스템의 실행 영역에 대한 안전성을 보장하는 것이다.

[0008] 또한, 본 발명의 목적은 분리망 연동 시스템에서 전달되는 데이터에 대한 검증을 수행하여, 변조된 데이터의 전달을 통제하는 것이다.

[0009] 또한, 본 발명의 목적은 분리망 통제 장치 내에 망 간 데이터 전달을 수행하는 소프트웨어 가드 확장(SGX) 기반의 CPU 보드를 별도로 구성하여, 물리적 수준의 데이터 통제를 수행하는 것이다.

과제의 해결 수단

[0010] 상기한 목적을 달성하기 위한 본 발명에 따른 분리망 통제 장치는 내부망 서버와 연결된 데이터 분류 장치로부터 데이터를 수신하는 내부망 운용부, 상기 데이터 분류 장치에 대한 검증 및 상기 내부망 서버의 데이터에 대한 검증을 수행하고, 검증의 수행 결과를 기반으로 상기 내부망 서버의 데이터가 외부망 서버로 전송되는 것을 통제하는 데이터 통제부, 그리고 상기 검증에 성공한 경우, 상기 내부망 서버의 데이터를 상기 외부망 서버로 전송하는 외부망 운용부를 포함한다.

[0011] 이때, 상기 데이터 통제부는, 상기 데이터 분류 장치에 대한 검증을 수행하는 데이터 분류 장치 검증 모듈, 상기 데이터 분류 장치가 분리망 통제 기능에 대한 검증을 수행하도록, 상기 데이터 분류 장치로 전송할 통제 QUOTE를 생성하는 통제 QUOTE 생성 모듈, 그리고 상기 데이터의 HMAC 값을 기반으로 상기 데이터에 대한 검증을 수행하여, 상기 내부망 서버의 데이터가 상기 외부망 서버로 전송되는 것을 통제하는 데이터 검증 모듈을 포함할 수 있다.

[0012] 이때, 상기 데이터 분류 장치 검증 모듈은, 기 저장된 분류 엔클레이브 정보와 상기 데이터 분류 장치로부터 수신된 분류 QUOTE의 엔클레이브 정보를 비교하여, 상기 데이터 분류 장치에 대한 무결성을 검증할 수 있다.

[0013] 이때, 상기 내부망 운용부는, 생성된 상기 통제 QUOTE를 상기 데이터 분류 장치로 전송하고, 상기 통제 QUOTE를 기반으로 분리망 통제 장치에 대한 검증을 수행한 상기 데이터 분류 장치로부터 상기 데이터 및 상기 HMAC 값을 수신하여, 상기 데이터 통제부로 전달할 수 있다.

[0014] 이때, 상기 데이터 검증 모듈은, 상기 데이터 분류 장치와 디피 헬먼 파라미터를 교환하여 HMAC 키를 생성하고, 상기 HMAC 키를 이용하여 상기 데이터의 HMAC 값에 대한 검증을 수행할 수 있다.

[0015] 이때, 상기 데이터 통제부는, 상기 내부망 운용부로부터 상기 데이터를 전달받는 PIC 통신 모듈, 그리고 상기 외부망 운용부로 상기 데이터를 전달하는 외부망 통신 모듈을 더 포함할 수 있다.

[0016] 이때, 상기 데이터 통제부는, 소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 엔클레이브 상에서 동작할 수 있다.

[0017] 또한, 본 발명의 일실시예에 따른 데이터 분류 장치는, 내부망 서버로부터 수신한 데이터가 외부망 서버로 전송 가능한 데이터인지 여부를 검사하여, 상기 데이터를 분류하는 데이터 검사부, 상기 외부망 서버와 연결된 분리망 통제 장치와 디피 헬먼 파라미터를 교환하여 HMAC 키를 생성하고, 상기 HMAC 키를 이용하여 상기 데이터의 HMAC 값을 생성하는 HMAC 생성부, 상기 분리망 통제 장치가 상기 데이터의 분류 기능에 대한 검증을 수행하도록, 상기 분리망 통제 장치로 전송할 분류 QUOTE를 생성하는 분류 QUOTE 생성부, 상기 분리망 통제 장치를 통하여 상기 데이터를 상기 외부망 서버로 전송할지 여부를 결정하기 위하여, 상기 분리망 통제 장치에 대한 검증을 수행하는 분리망 통제 장치 검증부, 그리고 검증이 완료된 상기 분리망 통제 장치로, 분류된 상기 데이터 및 상기 데이터의 HMAC 값을 전송하는 통신부를 포함한다.

[0018] 이때, 상기 데이터 검사부, 상기 HMAC 생성부, 상기 QUOTE 생성부 및 상기 분리망 통제 장치 검증부는, 소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 엔클레이브 상에서 동작할 수 있다.

[0019] 이때, 상기 QUOTE 생성부는, 상기 엔클레이브의 정보를 상기 소프트웨어 가드 확장(SGX) 프로세스의 비밀키로 서명하여, 상기 분류 QUOTE를 생성할 수 있다.

[0020] 이때, 상기 분리망 통제 장치 검증부는, 기 저장된 통제 엔클레이브 정보와 상기 분리망 통제 장치로부터 수신한 통제 QUOTE의 엔클레이브 정보를 비교하여, 상기 분리망 통제 장치에 대한 무결성을 검증할 수 있다.

[0021] 이때, 상기 HMAC 생성부는, 분류 디피 헬먼 파라미터 및 상기 분리망 통제 장치의 통제 디피 헬먼 파라미터를

조합하여 상기 HMAC 키를 생성하고, 상기 HMAC 키를 이용하여 분류가 완료된 상기 데이터에 대한 상기 HMAC 값을 생성할 수 있다.

[0022] 또한, 본 발명의 일 실시예에 따른 분리망 통제 장치에 의해 수행되는 분리망 간 데이터 통제 방법은, 내부망 서버와 연결된 데이터 분류 장치에 대한 검증을 수행하는 단계, 상기 데이터 분류 장치에 대한 검증에 성공한 경우, 상기 데이터 분류 장치로부터 수신된 상기 내부망 서버의 데이터에 대한 검증을 수행하는 단계, 그리고 검증의 수행 결과를 기반으로 상기 데이터가 외부망 서버로 전송되는 것을 통제하여, 상기 내부망 서버의 데이터를 외부망 서버로 전송하는 단계를 포함한다.

[0023] 이때, 상기 데이터 분류 장치에 대한 검증을 수행하는 단계는, 상기 데이터 분류 장치로부터 분류 QUOTE를 수신하는 단계, 수신된 상기 분류 QUOTE의 엔클레이브 정보와 기 저장된 분류 엔클레이브 정보를 비교하는 단계, 그리고 상기 엔클레이브 정보의 비교 결과를 기반으로, 상기 데이터 분류 장치의 무결성을 검증하는 단계를 포함할 수 있다.

[0024] 이때, 상기 내부망 서버의 데이터에 대한 검증을 수행하는 단계는, 상기 데이터 분류 장치로부터 분류 디피 헬먼 파라미터를 수신하는 단계, 수신된 상기 분류 디피 헬먼 파라미터와, 통제 디피 헬먼 파라미터를 이용하여, HMAC 키를 생성하는 단계, 그리고 생성된 상기 HMAC 키를 이용하여, 상기 데이터의 HMAC 값을 검증하는 단계를 포함할 수 있다.

[0025] 이때, 상기 데이터 분류 장치로 통제 QUOTE를 전송하여, 상기 데이터 분류 장치가 상기 분리망 통제 장치에 대한 검증을 수행하도록 하는 단계를 더 포함할 수 있다.

[0026] 이때, 상기 통제 QUOTE를 기반으로 상기 분리망 통제 장치에 대한 검증을 수행한 상기 데이터 분류 장치로부터 상기 내부망 서버의 데이터 및 상기 데이터의 HMAC 값을 수신하는 단계를 더 포함할 수 있다.

[0027] 이때, 상기 데이터 분류 장치로부터 수신된 상기 내부망 서버의 데이터는, 상기 데이터 분류 장치가, 상기 내부망 서버로부터 수신한 상기 데이터 중에서 외부망 서버로 전송 가능한 데이터인 것으로 판단하여 분류한 데이터일 수 있다.

[0028] 이때, 상기 데이터의 HMAC 값은, 상기 데이터 분류 장치가 상기 분류 디피 헬먼 파라미터 및 상기 통제 디피 헬먼 파라미터를 이용하여 생성한 HMAC 키를 상기 데이터에 적용하여 생성한 것일 수 있다.

[0029] 이때, 상기 데이터 분류 장치 및 상기 분리망 통제 장치 각각은, 소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 엔클레이브 상에서 동작을 수행할 수 있다.

발명의 효과

[0030] 본 발명에 따르면, 분리망 연동 시스템의 실행 영역에 대한 안전성을 보장할 수 있다.

[0031] 또한 본 발명에 따르면, 분리망 연동 시스템에서 전달되는 데이터에 대한 검증을 수행하여, 변조된 데이터의 전달을 통제할 수 있다.

[0032] 또한 본 발명에 따르면, 분리망 통제 장치 내에 망 간 데이터 전달을 수행하는 소프트웨어 가드 확장(SGX) 기반의 CPU 보드를 별도로 구성하여, 물리적 수준의 망분리를 제공할 수 있다.

도면의 간단한 설명

[0033] 도 1은 본 발명의 일실시예에 따른 데이터 분류 장치 및 분리망 통제 장치가 적용되는 환경을 개략적으로 나타낸 도면이다.

도 2는 본 발명의 일실시예에 따른 데이터 분류 장치의 구성을 나타낸 블록도이다.

도 3은 본 발명의 일실시예에 따른 분리망 통제 장치의 구성을 나타낸 블록도이다.

도 4는 본 발명의 일실시예에 따른 분리망 통제부의 구성을 나타낸 블록도이다.

도 5는 본 발명의 일실시예에 따른 분리망 통제 장치에 의해 수행되는 분리망 간 데이터 통제 방법을 설명하기 위한 순서도이다.

도 6은 본 발명의 일실시예에 따른 분리망 통제 시스템의 분리망 간 데이터 통제 과정의 흐름을 설명하기 위한 순서도이다.

도 7은 본 발명의 일실시예에 따른 컴퓨터 시스템을 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0034] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시 예들을 도면에 예시하고 상세하게 설명하고자 한다.

[0035] 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.

[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 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0038] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0040] 도 1은 본 발명의 일실시예에 따른 데이터 분류 장치 및 분리망 통제 장치가 적용되는 환경을 개략적으로 나타낸 도면이다.

[0041] 도 1에 도시한 바와 같이, 분리망 간 안전한 데이터 전송을 위한 분리망 통제 시스템은 내부망 서버(100), 데이터 분류 장치(200), 분리망 통제 장치(300) 및 외부망 서버(400)로 구성될 수 있다.

[0042] 분리망 통제 시스템은 데이터를 분류하는 과정, 데이터를 통제하는 과정 및 데이터를 외부망으로 전달하는 과정으로 분류될 수 있다. 종래의 분리망 통제 기술은 각 과정을 수행하는 모듈의 프로세싱 자체에 대한 안정성이 보장되지 않았다. 또한, 종래의 분리망 통제 기술은 각 과정을 수행하는 모듈간의 통신 시, 상호 인증 등을 고려하지 않고, 동일 시스템 내의 통신으로 처리하였다.

[0043] 그러나, 본 발명의 실시예에 따른 분리망 통제 시스템은 각 과정의 프로세싱을 모듈화하여 데이터 분류 장치(200) 및 분리망 통제 장치(300)로 분리하여 구성하였다. 또한, 본 발명의 일실시예에 따른 분리망 통제 시스템은 데이터를 외부망으로 전달하는 과정에서 망분리 안전성을 보장하기 위하여, 분리망 통제 장치(300)는 데이터 통제부와 내부망 운용부가 별도의 하드웨어로 구성되도록, 데이터 통제부를 전용 하드웨어 통제 모듈로 구성하였다.

[0044] 그리고 내부망으로부터 수신된 데이터의 외부망 공유 여부를 결정하기 위하여 데이터를 분류하는 과정을 엔클레이브(enclave)에서 수행하고, 외부망으로 전송하고자 하는 데이터가 분류 과정을 거친 데이터가 맞는지 무결성을 검증하는 과정(데이터를 통제하는 과정)을 적용하여 각각의 분리된 모듈간 통신의 안정성을 보장할 수 있다.

[0045] 내부망 서버(100)의 데이터는 데이터 분류 장치(200) 및 분리망 통제 장치(300)를 거쳐, 검증이 완료된 경우에만 외부망 서버(400)로 전달될 수 있다.

[0046] 데이터 분류 장치(200)는 내부망 서버(100)로부터 수신한 데이터를 분류하여, 데이터를 전송할지 여부를 결정한다. 데이터 분류 장치(200)는 내부망 서버(100)에 탑재되거나, 별도의 시스템에서 동작할 수 있다. 그리고 분리망 통제 장치(300)는 데이터 분류 장치(200)로부터 수신된 데이터를 외부망 서버(400)로 전송한다. 여기서, 분리망 통제 장치(300)는 데이터 분류 장치(200)와 별개의 장치로 구현될 수 있다.

[0047] 또한, 데이터 분류 장치(200)와 분리망 통제 장치(300)는 상호 장치에 대한 검증을 수행하고, 검증에 성공한 경우에만 내부망 서버(100)와 연결된 데이터 분류 장치(200)의 데이터 전송을 승인하고, 내부망 서버(100)의 데이

터를 분리망 통제 장치(300)를 통하여 외부망 서버(400)로 데이터를 전달할 수 있다.

[0048] 설명의 편의를 위하여, 내부망 서버(100)의 데이터가 외부망 서버(400)로 전송되는 경우에 대해서만 설명하였으나 이에 한정하지 않고, 외부망 서버(400)에서 내부망 서버(100)로의 데이터 전송은 필요에 따라 본 발명의 대칭 구조로 구성할 수 있다.

[0049] 또한, 데이터 분류 장치(200)의 핵심 기능 및 분리망 통제 장치(300)의 핵심 기능은 소프트웨어 가드 확장(Software Guard eXtensions, SGX)에 의해 제공되는 안전한 실행 환경에서 수행될 수 있다.

[0050] 인텔사에서 제공하는 소프트웨어 가드 확장(Software Guard eXtensions, SGX)을 이용한 실행 환경을 활용하는 경우, SGX를 지원하는 프로세서에 의해 안전하게 보호되는 보안 메모리 영역에서 엔클레이브(enclave)라는 애플리케이션이 동작할 수 있다. 그리고 엔클레이브는 해킹 등의 보안 위협으로부터 안전하며, 변조 없이 수행됨이 보장된다.

[0052] 이하에서는 도 2를 통하여 본 발명의 일실시예에 따른 데이터 분류 장치에 대하여 더욱 상세하게 설명한다.

[0053] 도 2는 본 발명의 일실시예에 따른 데이터 분류 장치의 구성을 나타낸 블록도이다.

[0054] 데이터 분류 장치(200)는 데이터 분류 엔클레이브(210) 및 통신부(260)를 포함하고, 데이터 분류 엔클레이브(210)는 데이터 검사부(220), HMAC 생성부(230), 분류 QUOTE 생성부(240) 및 분리망 통제 장치 검증부(250)를 포함할 수 있다. 여기서, 데이터 분류 엔클레이브(210)의 모든 동작은 소프트웨어 가드 확장(SGX)에 의해 제공되는 실행환경에서 수행되므로, 무결성이 보장된다.

[0055] 데이터 분류 엔클레이브(210)의 분류 QUOTE 생성부(240)는 분리망 통제 장치(300)로 전송할 분류 QUOTE를 생성한다. 분류 QUOTE 생성부(240)는 데이터 분류 엔클레이브(210)의 무결성 보장을 위하여, SGX 프로세스를 통해 분류 QUOTE를 생성할 수 있다.

[0056] 여기서, 분류 QUOTE는 데이터 분류 엔클레이브(210) 및 SGX에 의한 실행 환경에 대한 정보를 포함할 수 있다. 그리고 통제 QUOTE는 SGX 프로세스로부터 유도되는 비밀키로 서명된 형태일 수 있다. 또한, 생성된 분류 QUOTE는 분리망 통제 장치(300)가 데이터 분류 장치(200)에 대한 검증을 수행할 때 활용된다.

[0057] 그리고 분리망 통제 장치 검증부(250)는 분리망 통제 장치(300)로부터 수신한 통제 QUOTE를 이용하여, 분리망 통제 장치(300)에 대한 검증을 수행한다. 분리망 통제 장치 검증부(250)는 통제 QUOTE에 대한 검증을 수행하여, 분리망 통제 장치(300)의 데이터 통제 엔클레이브가 변조되지 않았음을 검증할 수 있다.

[0058] 분리망 통제 장치(300)에 대한 검증에 성공한 경우, 데이터 분류 엔클레이브(210)의 데이터 검사부(220)는 내부망 서버(100)로부터 수신한 데이터를 분류하고, HMAC 생성부(230)는 분류가 완료된 데이터에 대한 HMAC 값을 생성하며, 통신부(260)를 통하여 분리망 통제 장치(300)로 분류가 완료된 데이터 및 데이터의 HMAC 값을 전송할 수 있다.

[0059] 데이터 분류 장치(200)의 데이터 분류 엔클레이브(210)의 구성에 대하여 더욱 상세하게 설명하면, 다음과 같다. 데이터 검사부(220)는 내부망 서버(100)로부터 수신된 데이터에 대한 분류를 수행한다. 즉, 데이터 검사부(220)는 내부망 서버(100)의 데이터들은 외부망 서버(400)로 전송되기 이전에, 외부망으로 전송 가능한 데이터인지 확인하는 분류 과정을 거친다.

[0060] 데이터 검사부(220)는 해당 네트워크에서 요구하는 기준에 따라 데이터 분류를 수행하고, 해당 데이터가 외부망 서버(400)로 전송 가능한지 확인할 수 있다. 그리고 외부망 서버(400)로의 데이터 전송이 가능한 경우, 즉 데이터 전송이 인가된 경우, 해당 데이터는 데이터의 HMAC 값과 함께 분리망 통제 장치(300)로 전달될 수 있다.

[0061] 다음으로 HMAC 생성부(230)는 분리망 통제 장치(300)와 디피 헬먼 파라미터를 교환하여 HMAC 키를 생성한다. HMAC 생성부(230)는 데이터 분류 장치(200)의 분류 디피 헬먼 파라미터 및 분리망 통제 장치(300)로부터 수신한 통제 디피 헬먼 파라미터를 조합하여 HMAC 키를 생성할 수 있다. 그리고 HMAC 생성부(230)는 생성된 HMAC 키를 이용하여, 데이터 검사부(220)의 분류가 완료된 데이터의 HMAC 값을 생성한다.

[0062] 그리고 분류 QUOTE 생성부(240)는 분리망 통제 장치(300)가 데이터의 분류 기능에 대한 검증을 수행할 수 있도록, 분리망 통제 장치(300)로 전송할 분류 QUOTE를 생성한다.

[0063] 또한, 분리망 통제 장치 검증부(250)는 분리망 통제 장치(300)를 통하여 외부망 서버(400)로 데이터를 전송할지

여부를 결정하기 위하여, 데이터를 전달할 분리망 통제 장치(300)에 대한 검증을 수행한다.

[0064] 이때, 분리망 통제 장치 검증부(250)는 기 저장된 통제 QUOTE 원본과, 분리망 통제 장치(300)로부터 수신한 통제 QUOTE를 비교하여, 분리망 통제 장치(300)에 대한 무결성 검증을 수행할 수 있다. 특히, 분리망 통제 장치 검증부(250)는 통제 엔클레이브 정보(MRENCLAVE)를 사전에 저장하고 있으며, 사전에 저장된 통제 엔클레이브 정보와 수신된 통제 QUOTE의 엔클레이브 정보(MRENCLAVE)를 비교하여 분리망 통제 장치(300)에 대한 무결성을 검증할 수 있다.

[0065] 무결성 검증의 수행 결과, 분리망 통제 장치(300)의 데이터 통제 엔클레이브가 변조되지 않은 것으로 판단된 경우, HMAC 생성부(230)는 디피 헬먼 파라미터를 이용하여 HMAC 키를 생성할 수 있다.

[0066] 마지막으로 데이터 분류 장치(200)의 통신부(260)는 내부망 서버(100)로부터 데이터를 수신하고, 수신한 데이터를 데이터 분류 엔클레이브(210)로 전달하여, 데이터 분류를 수행한다. 그리고 통신부(260)는 데이터 분류 엔클레이브(210)에 의한 분류가 완료된 데이터를 분리망 통제 장치(300)로 전송하여, 외부망 서버(400)로의 데이터 전송을 요청한다.

[0067] 그리고 데이터 분류 장치(200)의 통신부(260)는 내부망 서버(100)로부터 데이터를 수신하고, 분류가 완료된 데이터를 분리망 통제 장치(300)로 전달한다.

[0068] 통신부(260)는 HMAC 생성부(230)가 생성한 분류 디피 헬먼 파라미터 및 분류 QUOTE 생성부(240)가 생성한 데이터 분류 엔클레이브(210)의 분류 QUOTE를 분리망 통제 장치(300)로 전달할 수 있다. 또한, 그에 대한 응답으로 통신부(260)는 분리망 통제 장치(300)로부터 통제 QUOTE를 수신할 수 있다.

[0070] 이하에서는 도 3 및 도 4를 통하여 본 발명의 일실시예에 따른 분리망 통제 장치의 구성에 대하여 더욱 상세하게 설명한다.

[0071] 도 3은 본 발명의 일실시예에 따른 분리망 통제 장치의 구성을 나타낸 블록도이다.

[0072] 도 3과 같이, 분리망 통제 장치(300)는 내부망 운용부(310), 데이터 통제부(320) 및 외부망 운용부(330)를 포함한다.

[0073] 내부망 운용부(310)는 내부망 운용 소프트웨어를 실행하고, 외부망 운용부(330)는 외부망 운용 소프트웨어를 실행하여, 내부망 및 외부망에서 복수의 데이터 전송을 동시에 처리하기 위한 세션 관리 등을 수행할 수 있다.

[0074] 데이터 분류 장치(200)로부터 수신된 데이터는 내부망 운용부(310)를 거쳐 데이터 통제부(320)에서 처리되며, 외부망 운용부(330)로 전달될 수 있다. 그리고 인가된 데이터 이외의 데이터 전송을 차단하기 위하여, 내부망 운용부(310)와 데이터 통제부(320)는 상이한 CPU 및 메모리 내에서 동작하며, 망분리 안전성을 보장하기 위하여, 외부망으로의 데이터 전송은 데이터 통제부(320)에 의해서만 수행될 수 있다.

[0075] 분리망 통제 장치(300)의 데이터 통제부(320)의 구성은 도 4에 도시한 바와 같다.

[0076] 도 4는 본 발명의 일실시예에 따른 분리망 통제부의 구성을 나타낸 블록도이다.

[0077] 도 4와 같이, 데이터 통제부(320)는 데이터 통제 엔클레이브(321), PCI 통신 모듈(328) 및 외부망 통신 모듈(239)을 포함할 수 있다. 그리고 데이터 통제 엔클레이브(321)는 데이터 분류 장치 검증 모듈(323), 통제 QUOTE 생성 모듈(325), 데이터 검증 모듈(327)을 포함할 수 있다.

[0078] PCI 통신 모듈(328)은 내부망 서버(100)가 전송하는 데이터를 수신하며, PCI 통신 모듈(328)이 수신한 데이터는 데이터 통제 엔클레이브(321)로 전달된다. 그리고 내부망 서버(100)의 모든 데이터는 데이터 통제 엔클레이브(321)의 통제 과정을 거친 후에, 외부망 통신 모듈(329)에 의해 외부망 서버(400)로 전달될 수 있으며, 이를 통하여 망분리를 보장할 수 있다.

[0079] PCI 통신 모듈(328)은 데이터 분류 장치(200)와의 통신을 수행하며, 데이터 분류 장치(200)로 통제 디피 헬먼 파라미터 및 통제 QUOTE를 전송하고, 데이터 분류 장치(200)로부터 데이터 및 데이터의 HMAC 값을 수신하여 데이터 통제부(320)의 데이터 통제 엔클레이브(321)로 전달할 수 있다. 그리고 외부망 통신 모듈(329)은 외부망 서버(400)와의 통신을 수행하며, 외부망 서버(400)로 분류 및 검증이 완료된 데이터를 전송할 수 있다.

[0080] 데이터 통제 엔클레이브(321)의 데이터 분류 장치 검증 모듈(323)은 데이터 분류 장치(200)의 분류 QUOTE를 검

증하여, 데이터 분류가 정상적으로 수행되었는지 확인한다.

[0081] 그리고 통제 QUOTE 생성 모듈(325)은 데이터 통제 엔클레이브(321)의 무결성을 데이터 분류 장치(200)에 보장하기 위한 통제 QUOTE를 생성한다. 여기서, 통제 QUOTE는 데이터 통제 엔클레이브(321) 및 SGX에 의한 실행 환경에 대한 정보를 포함할 수 있다. 그리고 통제 QUOTE는 SGX 프로세스로부터 유도되는 비밀키로 서명된 형태일 수 있다.

[0082] 또한, 데이터 검증 모듈(327)은 데이터 분류 엔클레이브와 동일한 HMAC 키를 생성하고, 생성된 키를 이용하여, 데이터 분류 장치(200)로부터 수신한 데이터의 HMAC 값을 검증할 수 있다.

[0083] 그리고 수신된 데이터가 검증이 완료된 데이터 분류 장치(200)로부터 수신된 것이고, 데이터의 HMAC 값에 대한 검증에 성공한 경우, 데이터 통제부(320)는 외부망 서버(400)로 해당 데이터를 전달할 수 있다.

[0085] 이하에서는 도 5를 통하여 본 발명의 일실시예에 따른 분리망 통제 장치에 의해 수행되는 분리망 간 데이터 통제 방법에 대하여 더욱 상세하게 설명한다.

[0086] 도 5는 본 발명의 일실시예에 따른 분리망 통제 장치에 의해 수행되는 분리망 간 데이터 통제 방법을 설명하기 위한 순서도이다.

[0087] 먼저, 분리망 통제 장치(300)는 데이터 분류 장치(200)에 대한 검증을 수행한다(S510).

[0088] 분리망 통제 장치(300)는 데이터 분류 장치(200)로부터 분류 QUOTE 및 분류 디피 헬먼 파라미터를 수신하고, 수신된 분류 QUOTE에 대한 검증을 수행한다.

[0089] 이때, 분리망 통제 장치(300)는 기 저장된 데이터 분류 장치(200)의 분류 엔클레이브 정보와 수신된 분류 QUOTE의 엔클레이브 정보를 비교하여, 데이터 분류 장치(200)에 대한 검증을 수행할 수 있다. 여기서, 데이터 분류 장치(200)에 대한 검증은, 데이터 분류 장치(200)가 데이터 분류를 정상적으로 수행하였는지 여부를 확인하는 과정을 의미할 수 있다.

[0090] 그리고 분리망 통제 장치(300)는 내부망 서버의 데이터에 대한 검증을 수행한다(S520).

[0091] 데이터 분류 장치(200)에 대한 검증에 성공한 경우, 분리망 통제 장치(300)는 데이터 분류 장치(200)로부터 수신한 데이터에 대한 검증을 수행할 수 있다. 이때, 분리망 통제 장치(300)는 데이터 분류 장치(200)로부터 데이터 및 데이터의 HMAC 값을 수신하고, 수신된 HAMC 값에 대한 검증을 수행하여 해당 데이터에 대한 검증을 수행할 수 있다.

[0092] 분리망 통제 장치(300)는 데이터 분류 장치(200)의 데이터 분류 엔클레이브(210)와 동일한 방식으로 HMAC 키를 생성한다. 이때, 분리망 통제 장치(300)는 데이터 분류 장치(200)와 교환한 디피 헬먼 파라미터를 이용하여 HMAC 키를 생성할 수 있다. 그리고 분리망 통제 장치(300)는 생성된 HMAC 키를 이용하여 HMAC 값에 대한 검증을 수행할 수 있다.

[0093] 검증을 수행한 결과(S530) 검증에 성공한 것으로 판단된 경우, 분리망 통제 장치(300)는 데이터 분류 장치(200)를 통하여 내부망 서버(100)로부터 수신된 데이터를 외부망 서버(400)로 전송한다(S540).

[0094] S510 단계에서 데이터 분류 장치(200)에 대한 검증에 성공하고, S520 단계에서 내부망 서버의 데이터에 대한 검증에 성공한 경우, S530 단계에서 분리망 통제 장치(300)는 검증에 성공한 것으로 판단한다. 그리고 분리망 통제 장치(300)는 검증이 완료된 내부망 서버의 데이터를 외부망 서버로 전송한다.

[0095] 반면, 검증에 실패한 경우, 데이터 분류 장치(200)는 내부망 서버(100)의 데이터를 폐기하거나, 데이터 전송 과정의 수행을 종료할 수 있다. 즉, S510 단계에서 데이터 분류 장치(200)에 대한 검증에 실패하거나, S520 단계에서 내부망 서버(100)의 데이터에 대한 검증에 실패한 경우, 분리망 통제 장치(300)는 내부망 데이터를 외부망으로 전송하는 과정의 수행을 종료할 수 있다.

[0096] 도 5에서 분리망 통제 장치(300)가 데이터를 통제하는 과정 및 데이터를 외부망으로 전달하는 과정은 도 4의 분리망 통제 장치(300)에 의해 수행되며, 설명의 편의를 위하여 중복되는 설명은 생략한다.

[0098] 이하에서는 도 6을 통하여 본 발명의 일실시예에 따른 분리망 간 안전한 데이터 전송을 위한 분리망 통제 시스

템의 분리망 통제 과정에 대하여 더욱 상세하게 설명한다.

[0099] 도 6은 본 발명의 일실시예에 따른 분리망 통제 시스템의 분리망 간 데이터 통제 과정의 흐름을 설명하기 위한 순서도이다.

[0100] 도 6에 도시한 바와 같이, 내부망 서버(100)는 데이터 분류 장치(200)로 데이터를 전송하고(S610), 데이터 분류 장치(200)는 분리망 통제 장치(300)로 데이터 전송을 요청한다(S615).

[0101] 그리고 데이터 전송 요청을 수신한 분리망 통제 장치(300)는 데이터 분류 장치(200)로 분류 QUOTE를 요청하고, 통제 DH 파라미터를 전송한다(S620).

[0102] 다음으로 데이터 분류 장치(200)는 분류 QUOTE를 생성하고(S625), 생성된 분류 QUOTE 및 분류 DH 파라미터를 분리망 통제 장치(300)로 전송한다(S630).

[0103] 데이터 분류 장치(200) 및 분리망 통제 장치(300)는 S620 단계 및 S630 단계를 통하여 디피 헬먼 파라미터(통제 DH 파라미터, 분류 DH 파라미터)를 교환한다. 분리망 통제 장치(300)는 후술할 S645 단계에서, 데이터 분류 장치(200)는 후술할 S660 단계에서 교환된 DH 파라미터를 이용하여 HMAC 키를 생성할 수 있다.

[0104] 또한, 분리망 통제 장치(300)는 수신한 분류 QUOTE에 대한 검증을 수행하고(S635), 통제 QUOTE를 생성한다(S640).

[0105] 분리망 통제 장치(300)와 데이터 분류 장치(200)는 QUOTE의 검증을 위하여 엔클레이브에 대한 정보(MRENCLAVE)를 보유하고 있어야 하며, 상대 엔클레이브의 무결성을 검증하기 위하여 사전에 상대의 엔클레이브 정보(MRENCLAVE)를 저장하고 있다.

[0106] 그리고 분리망 통제 장치(300)는 S630 단계에서 수신한 분류 QUOTE의 엔클레이브 정보와 기 저장된 분류 엔클레이브 정보를 비교하여, 분류 QUOTE에 대한 검증을 수행할 수 있다. 그리고 분류 QUOTE의 검증에 성공한 경우, 분리망 통제 장치(300)는 통제 QUOTE를 생성할 수 있따.

[0107] 다음으로 분리망 통제 장치(300)는 HMAC 키를 생성한다(S645).

[0108] 분리망 통제 장치(300)는 데이터 분류 장치(200)와 교환한 DH 파라미터를 이용하여, HMAC 키를 생성할 수 있다.

[0109] 그리고 분리망 통제 장치(300)는 생성한 통제 QUOTE를 데이터 분류 장치(200)로 전송하고, 데이터 전송 승인 메시지를 데이터 분류 장치(200)로 전송할 수 있다(S650).

[0110] 또한, 데이터 분류 장치(200)는 통제 QUOTE에 대한 검증을 수행하고(S655), HMAC 키를 생성하여(S660), 내부망 서버(100)로부터 수신된 데이터를 검사한다(S665).

[0111] 여기서, 데이터 분류 장치(200)가 HMAC 키를 생성하는 과정은 S645 단계에서 분리망 통제 장치(300)가 HMAC 키를 생성하는 과정과 실질적으로 동일할 수 있다.

[0112] 그리고 수신된 데이터를 검사한 결과, 해당 데이터가 외부망 서버(400)로의 전송이 인가된 데이터인 경우, 데이터 분류 장치(200)는 데이터의 HMAC 값을 생성하고(S670), 내부망 서버(100)의 데이터 및 데이터의 HMAC 값을 분리망 통제 장치(300)로 전송한다(S675).

[0113] 마지막으로, 분리망 통제 장치(300)는 수신된 HMAC 값에 대한 검증을 수행하고(S680), 검증에 성공한 경우, 내부망 서버(100)의 데이터를 외부망 서버(400)로 전송한다(S685).

[0115] 도 7은 본 발명의 일실시예에 따른 컴퓨터 시스템을 나타낸 블록도이다.

[0116] 도 7을 참조하면, 본 발명의 실시예는 컴퓨터로 읽을 수 있는 기록매체와 같은 컴퓨터 시스템(700)에서 구현될 수 있다. 도 7에 도시된 바와 같이, 컴퓨터 시스템(700)은 버스(720)를 통하여 서로 통신하는 하나 이상의 프로세서(710), 메모리(730), 사용자 인터페이스 입력 장치(740), 사용자 인터페이스 출력 장치(750) 및 스토리지(760)를 포함할 수 있다. 또한, 컴퓨터 시스템(700)은 네트워크(780)에 연결되는 네트워크 인터페이스(770)를 더 포함할 수 있다. 프로세서(710)는 중앙 처리 장치 또는 메모리(730)나 스토리지(760)에 저장된 프로세싱 인스트럭션들을 실행하는 반도체 장치일 수 있다. 메모리(730) 및 스토리지(760)는 다양한 형태의 휘발성 또는 비휘발성 저장 매체일 수 있다. 예를 들어, 메모리는 ROM(731)이나 RAM(732)을 포함할 수 있다.

[0117] 따라서, 본 발명의 실시예는 컴퓨터로 구현된 방법이나 컴퓨터에서 실행 가능한 명령어들이 기록된 비일시적인

컴퓨터에서 읽을 수 있는 매체로 구현될 수 있다. 컴퓨터에서 읽을 수 있는 명령어들이 프로세서에 의해서 수행될 때, 컴퓨터에서 읽을 수 있는 명령어들은 본 발명의 적어도 한 가지 태양에 따른 방법을 수행할 수 있다.

[0119] 이상에서와 같이 본 발명에 따른 데이터 분류 장치, 분리망 통제 장치 및 분리망 간 데이터 통제 방법은 상기한 바와 같이 설명된 실시예들의 구성과 방법이 한정되게 적용될 수 있는 것이 아니라, 상기 실시예들은 다양한 변형이 이루어질 수 있도록 각 실시예들의 전부 또는 일부가 선택적으로 조합되어 구성될 수도 있다.

부호의 설명

[0120] 100: 내부망 서버

200: 데이터 분류 장치

210: 데이터 분류 엔클레이브

220: 데이터 검사부

230: HMAC 생성부

240: 분류 QUOTE 생성부

250: 분리망 통제 장치 검증부

260: 통신부

300: 분리망 통제 장치

310: 내부망 운용부

320: 데이터 통제부

321: 데이터 통제 엔클레이브

323: 데이터 분류 장치 검증 모듈

325: 통제 QUOTE 생성 모듈

327: 데이터 검증 모듈

328: PCI 통신 모듈

329: 외부망 통신 모듈

330: 외부망 운용부

400: 외부망 서버

700: 컴퓨터 시스템

710: 프로세서

720: 버스

730: 메모리

731: 롬

732: 램

740: 사용자 인터페이스 입력 장치

750: 사용자 인터페이스 출력 장치

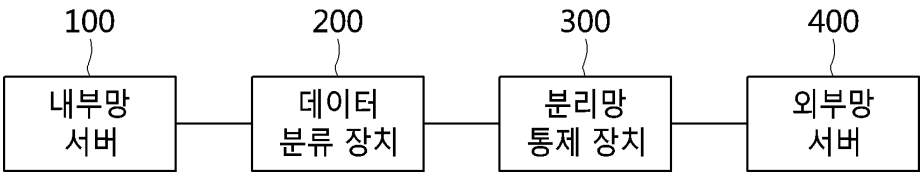
760: 스토리지

770: 네트워크 인터페이스

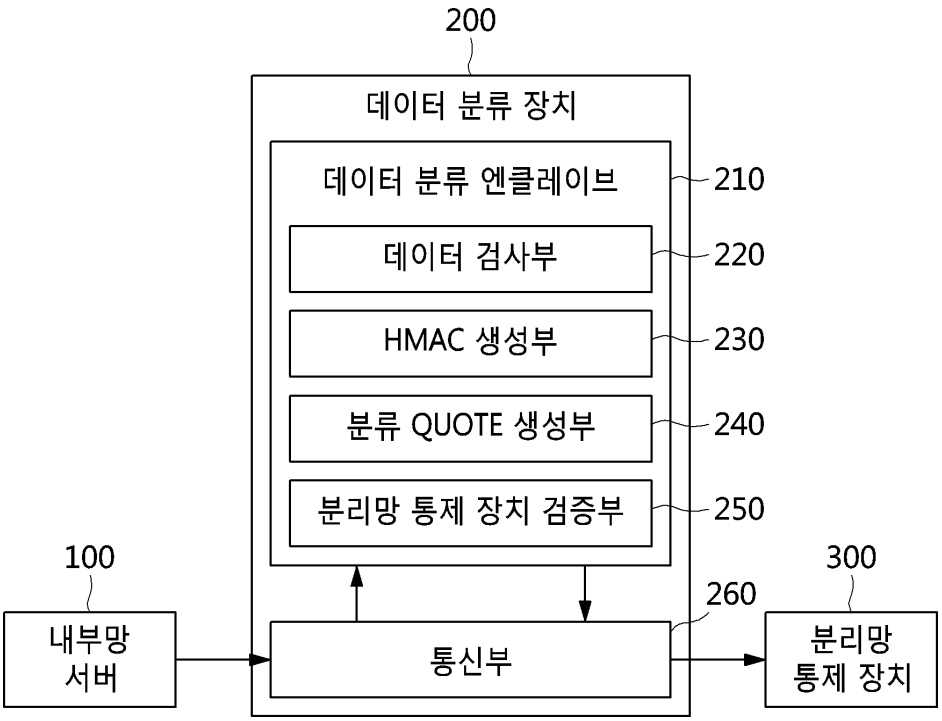
780: 네트워크

도면

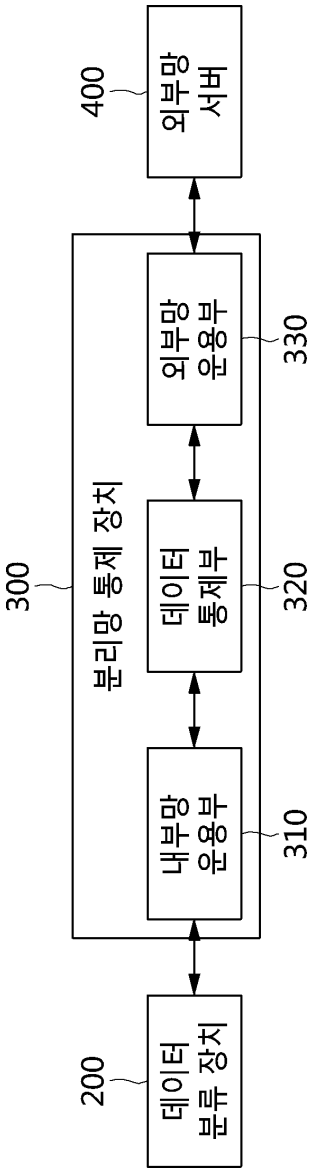
도면1



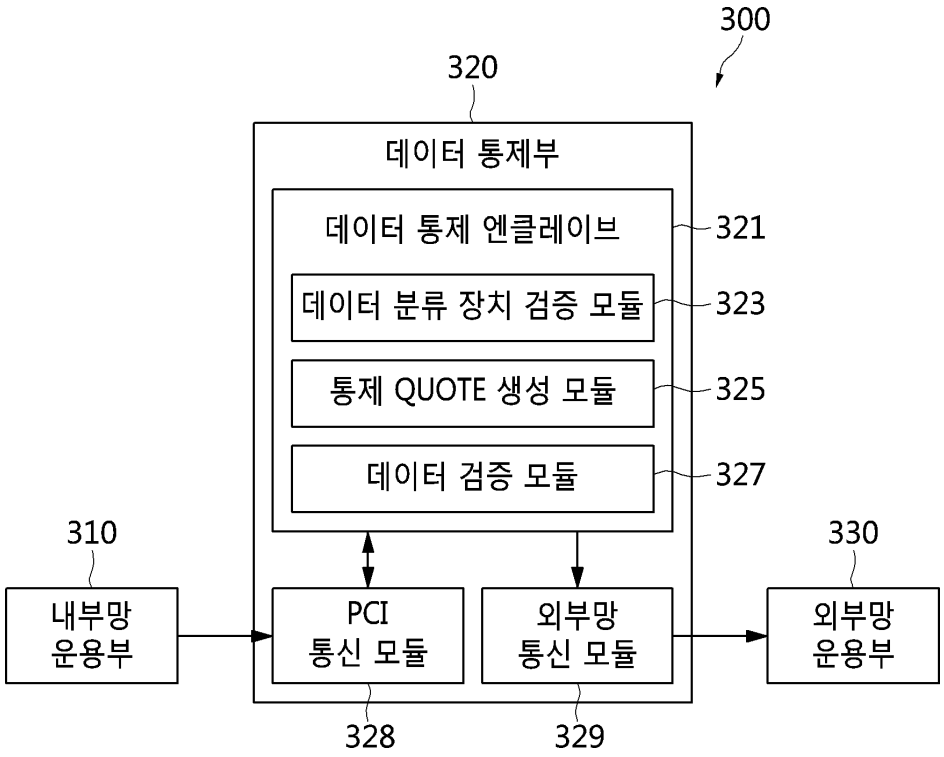
도면2



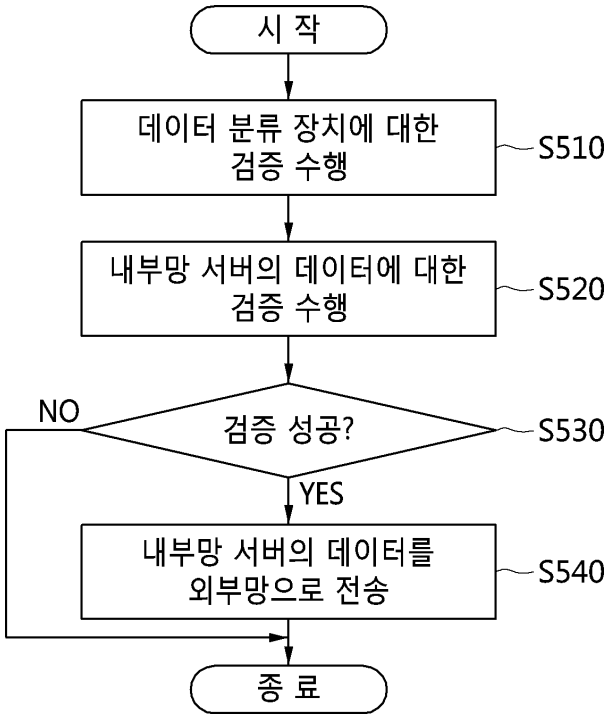
도면3


400
외부망 서버
300
분리망 통제 장치
외부망 운용부
330
데이터 통제부
320
내부망 운용부
310
200
데이터 분류 장치

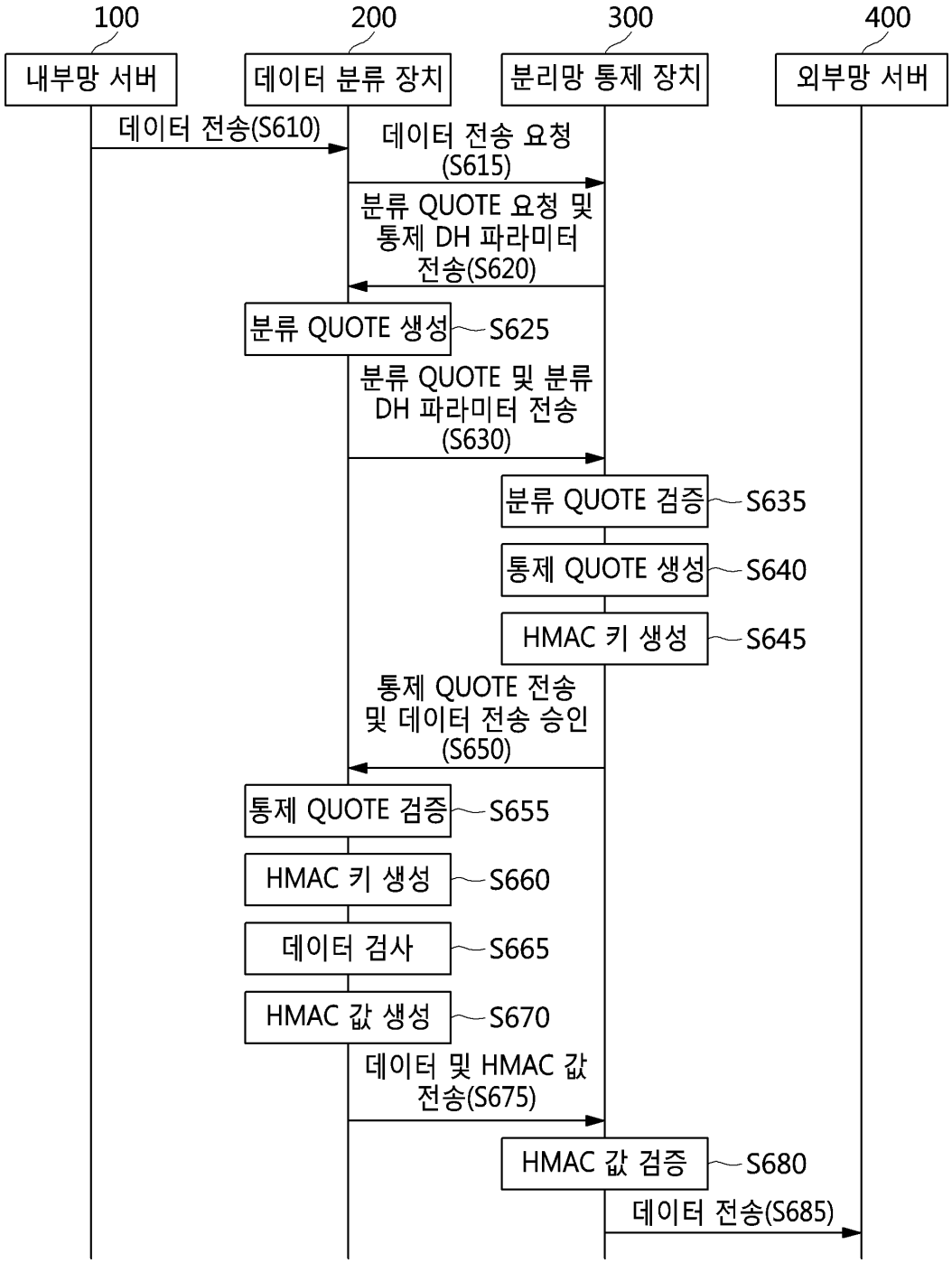
도면4


300
320
데이터 통제부
데이터 통제 엔클레이브
321
데이터 분류 장치 검증 모듈
323
통제 QUOTE 생성 모듈
325
데이터 검증 모듈
327
310
330
내부망 운용부
PCI 통신 모듈
외부망 통신 모듈
외부망 운용부
328
329

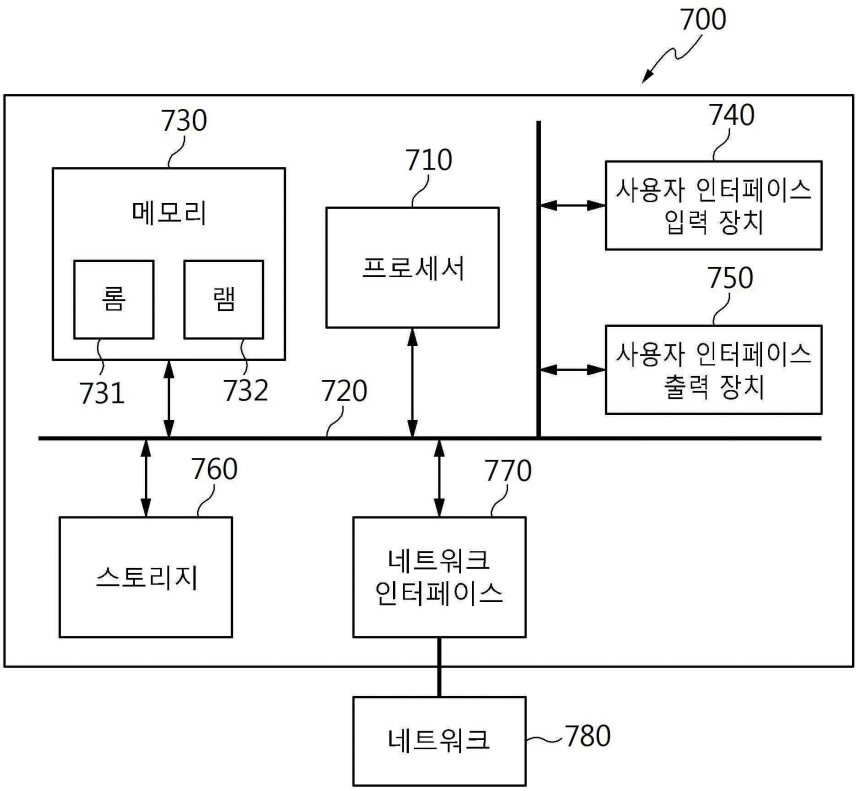
도면5


시 작
데이터 분류 장치에 대한 검증 수행
S510
내부망 서버의 데이터에 대한 검증 수행
S520
NO
검증 성공?
S530
YES
내부망 서버의 데이터를 외부망으로 전송
S540
종 료

도면6


100
200
300
400
내부망 서버
데이터 분류 장치
분리망 통제 장치
외부망 서버
데이터 전송(S610)
데이터 전송 요청 (S615)
분류 QUOTE 요청 및 통제 DH 파라미터 전송(S620)
분류 QUOTE 생성
S625
분류 QUOTE 및 분류 DH 파라미터 전송 (S630)
분류 QUOTE 검증
S635
통제 QUOTE 생성
S640
HMAC 키 생성
S645
통제 QUOTE 전송 및 데이터 전송 승인 (S650)
통제 QUOTE 검증
S655
HMAC 키 생성
S660
데이터 검사
S665
HMAC 값 생성
S670
데이터 및 HMAC 값 전송(S675)
HMAC 값 검증
S680
데이터 전송(S685)

도면7


700
730
메모리
롬
램
731
732
710
프로세서
720
740
사용자 인터페이스
입력 장치
750
사용자 인터페이스
출력 장치
760
스토리지
770
네트워크
인터페이스
네트워크
780