



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0075491
(43) 공개일자 2020년06월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 63/0869 (2013.01)
(21) 출원번호 10-2018-0164235
(22) 출원일자 2018년12월18일
심사청구일자 2018년12월18일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57, 132동 801호
김현진
대전광역시 유성구 온천북로 7, 102동 1092호
(74) 대리인
홍성욱, 심경식

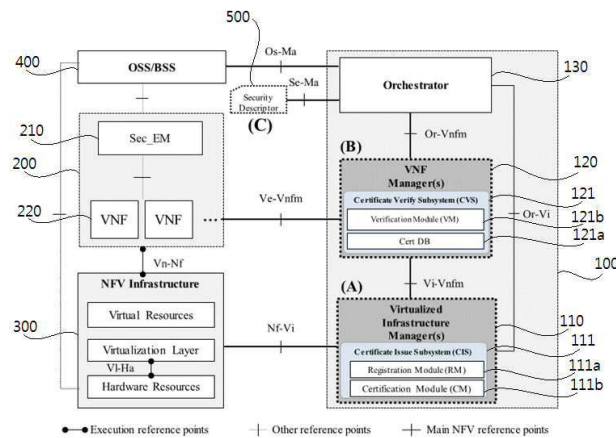
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 NFV 환경을 위한 LW_PKI 시스템 및 그 시스템을 이용한 통신방법.

(57) 요약

본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법은 (a) LW_PKI가 테넌트 내의 VNF 또는 Sec_EM의 인증서를 발행하는 단계; (b) 상기 LW_PKI가 상기 VNF의 구동을 위해 상기 Sec_EM과 VNF 간, 또는 상기 VNF간을 인증하는 단계; 및 (c) 상기 Sec_EM과 VNF 간, 또는 상기 VNF간 통신을 위해 통신 메시지를 암호화하여 통신하는 단계;를 포함하여 VNF 간의 상호인증 및 데이터 보안을 이용하여 Fake VNF를 차단하고 AI(Artificial Intelligence) 기반의 비정상 행위 탐지 기법을 이용하여 VNF 간 전송되는 악성 트래픽을 차단할 수 있는 효과가 있다.

대표도 - 도1



(52) CPC특허분류

H04L 63/1441 (2013.01)

H04L 9/0861 (2013.01)

H04L 9/3247 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711070437

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 대학ICT연구센터육성지원사업

연구과제명 지능정보기술을 활용한 금융서비스 보호 기술 연구

기 여 율 1/1

주관기관 충남대학교 산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

- (a) LW_PKI가 테넌트 내의 VNF 또는 Sec_EM의 인증서를 발행하는 단계;
- (b) 상기 LW_PKI가 상기 VNF의 구동을 위해 상기 Sec_EM과 VNF 간, 또는 상기 VNF간을 인증하는 단계; 및
- (c) 상기 Sec_EM과 VNF 간, 또는 상기 VNF간 통신을 위해 통신 메시지를 암호화하여 통신하는 단계;를 포함하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 2

제 1항에 있어서,

상기 (a)단계는

- (a-1) 상기 LW_PKI의 오케스트레이터(Orchestrator)가 상기 VNF에서 사용할 자원정보, VNFD(VNF Descriptor) 및 인증서 발급을 위한 씨큐리티 디스크립터 정보를 상기 LW_PKI의 가상화 인프라 관리부에 전달하는 단계;
- (a-2) 상기 가상화 인프라 관리부가 상기 씨큐리티 디스크립터 정보를 기반으로 인증서를 생성하여 Cert_DB에 저장하는 단계;
- (a-3) 상기 가상화 인프라 관리부가 상기 (a-2)단계에서 생성된 인증서를 상기 VNF가 설치되는 가상머신에 설치하여 컴퓨팅 노드에 로드(Placement)하는 단계; 및
- (a-4) 상기 가상화 인프라 관리부가 VNF_ID 및 Tenant_ID를 상기 오케스트레이터에 응답하는 단계;를 포함하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 3

제 2항에 있어서,

상기 (a-2) 단계는

- (a-2-1) 상기 인증서 발행 서버 시스템 내의 등록 모듈은 상기 가상화 인프라 관리부의 발급 요청 메시지 내의 Tenant_ID, VNFD, VNF_ID 또는 Sec_EM_ID정보를 이용하여 인증서 발급을 요청한 VNF를 식별하고, 상기 인증서 발급 모듈에 상기 VNF의 인증서 발급을 요청하는 단계;를 더 포함하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 4

제 3항에 있어서,

상기 등록 모듈은

$Secret_{vnf} = Tenant_ID \oplus VNF_ID$ 를 이용하여 인증서 발급을 요청한 VNF를 식별하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 5

제 4항에 있어서,

상기 테넌트가 처음 생성되는 경우 상기 Sec_EM이 Instantiation 될 때, 상기 Sec_EM을 위한 인증서가 발급되어 상기 Sec_EM을 구동시키는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 6

제 5항에 있어서,

상기 (b)단계는

(b-1) 상기 Sec_EM이 자신의 ID_{Sec_EM}와 임의의 난스(Nonce) R_{SEC_EM}를 생성하여 전송하고 자신의 개인키로 암호화한 E_{CertSec_EM}(R_{Sec_EM})을 전송하여 전자서명하는 단계;

(b-2) 상기 가상 네트워크 함수 관리부가 수신한 상기 E_{CertSec_EM}(R_{Sec_EM})를 복호화하기 위해서 상기 ID_{Sec_EM}을 이용하여 Cert DB 내 Cert_{Sec_EM}'를 검색하는 단계;

(b-3) 상기 가상 네트워크 함수 관리부가 검색된 ID_{Sec_EM}에 해당하는 Cert_{Sec_EM}'을 인증서 검증 모듈로 전송하는 단계; 및

(b-4) 상기 인증서 검증 모듈이 전송된 R_{Sec_EM}과 Cert_{Sec_EM}으로 E_{CertSec_EM}(R_{Sec_EM})을 복호화하여 얻은 R_{Sec_EM}'과 비교하여 R_{Sec_EM}의 무결성과 Sec_EM을 인증하는 단계;를 포함하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 7

제 6항에 있어서,

상기 (b)단계는

(b-1) 상기 VNF가 ID_{VNF}, R_{VNF}과 R_{VNF}의 무결성 검증을 위해 E_{CertVNF}(R_{VNF})을 상기 가상 네트워크 함수 관리부의 인증서 검증 서버 시스템에 전송하는 단계;

(b-2) 상기 가상 네트워크 함수 관리부가 Cert_{VNF}과 상기 Cert DB 내 Cert_{VNF}'을 비교하기 위해 ID_{VNF}을 Cert DB로 전송하는 단계;

(b-3) 상기 가상 네트워크 함수 관리부가 ID_{VNF}에 해당하는 Cert_{VNF}'을 인증서 검증 모듈로 전송하는 단계; 및

(b-4) 상기 인증서 검증 모듈이 전송된 R_{VNF}과 Cert_{VNF}으로 E_{CertVNF}(R_{VNF})을 복호화하여 얻은 R_{VNF}'과 비교하여 R_{VNF}의 무결성과 상기 VNF를 인증하는 단계;를 포함하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 8

제 7항에 있어서,

상기 (c)단계는

(c-1) 상기 가상 네트워크 함수 관리부가 ID_{VNF}, ID_{Sec_EM}, and 난스(Nonce)를 이용하여 암호화 통신에 사용될 대칭키인(Symmetric key) DEK(Data Encryption Key)를 생성하는 단계;

(c-2) 상기 가상 네트워크 함수 관리부가 생성된 상기 DEK를 상기 VNF에 전달하는 단계;

(c-3) 상기 가상 네트워크 함수 관리부가 인증서 검증 서버 시스템의 Cert DB에 보관된 Cert_A, Cert_B로 각각 암호화하여 상기 Sec_EM 또는 VNF에 해당되는 각 엔티티들에 전달하는 단계; 및

(c-4) 상기 엔티티들이 자신이 가지고 있는 인증서의 개인키를 이용하여 $E_{\text{CertA}}(R_A, \text{DEK})$, $E_{\text{CertB}}(R_B, \text{DEK})$ 을 복호화하여 얻은 DEK를 이용하여 메시지를 암호화하여 안전한 통신을 수행하는 단계;를 포함하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

청구항 9

제 8항에 있어서,

상기 가상 네트워크 함수 관리부는

$\text{DEK} = \text{ID}_{\text{VNF}} \oplus \text{ID}_{\text{Sec_EM}} \oplus \text{Nonce}$ 을 이용하여 DEK(Data Encryption Key)를 생성하는 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법.

발명의 설명

기술 분야

[0001] 본 발명은 NFV 환경을 위한 LW_PKI 시스템 및 그 시스템을 이용한 통신방법에 관한 것으로서, 더욱 상세하게는 PKI기반으로 테넌트 내 VNF간의 인증을 수행하고, 인증서를 이용하여 공개키 기반의 암호화를 통해서 트래픽에 대한 보안성을 향상시킬 수 있는 NFV 환경을 위한 LW_PKI 시스템 및 그 시스템을 이용한 통신방법에 관한 것이다.

배경 기술

[0003] 최근 세계 네트워크 동향은 하드웨어에 의존적이 않고, 자원을 보다 효율적으로 활용하기 위해서 가상화 기술을 도입하고 있다. 조직 및 기업이 가상화 기술을 도입함으로써 효율적인 자원활용과 인프라의 구축 및 관리의 간소화에 따라서 비용 절감 효과를 얻을 수 있기 때문이다.

[0004] NFV(Network Function Virtualization) 기술은 이러한 요구를 반영하기 위한 차세대 네트워크 가상화 기술이다. NFV는 네트워크 장비내 여러 기능을 분리시켜, 소프트웨어적으로 제어 및 관리가 가능한 가상시스템인 VNF(Virtual Network Function)를 서버의 운영체제에 업로드시켜 활용한다.

[0005] 물리적인 네트워크 장비의 기능을 가상화하여 가상머신 서버 혹은 범용 프로세서를 탑재한 하드웨어에서 실행하는 방식을 사용한다.

[0006] NFV 기술을 이용하면 논리적으로 네트워크를 구축할 수 있기 때문에 기존의 네트워크 변화에 유연하게 대응하는 것이 가능하다.

[0007] 하지만 가상화된 기기의 수가 증가함에 따라서 테넌트 내에 Fake VNF를 판별하지 못하면 전송 데이터 간의 유출될 가능성뿐만 아니라 CAPEX(Capital Expenditure) 및 OPEX(Operating Expense) 등의 소요 비용이 크다.

[0008] 따라서, VNF간 상호인증을 통해 정당한 VNF임을 판단하고, 전송 데이터의 보안성을 향상시킬 수 있는 기능이 필요하다.

[0009] 또한, 테넌트 내에 로드되는 VNF에 별도의 인증 과정을 거치지 않으면 악의적인 악성 VNF가 로드되어, 테넌트 내에 존재하는 VNF 간의 상호인증 및 데이터 보안을 보장하고, VNF 운영과정을 학습하여 각 VNF의 비정상행위를 탐지할 수 있는 메커니즘이 필요한 실정이다.

[0010]

선행기술문헌

특허문헌

[0011] (특허문헌 0001) 대한민국 등록특허공보 제10-1357074호(2014. 01. 23)

발명의 내용

해결하려는 과제

[0012] 상술한 바와 같은 필요에 따라 본 발명은 PKI(Public Key Infrastructure: 공개키 기반구조) 기반으로 테넌트 내 VNF간의 인증을 수행하고, 인증서를 이용하여 공개키 기반의 암호화를 통해서 트래픽에 대한 보안성을 향상시키고, 더불어 기존 인공지능 알고리즘을 이용하여 VNF의 비정상 행위를 탐지하는 NFV 환경을 위한 PKI 시스템의 제공을 목적으로 한다.

과제의 해결 수단

[0014] 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법은 (a) LW_PKI가 테넌트 내의 VNF 또는 Sec_EM의 인증서를 발행하는 단계; (b) 상기 LW_PKI가 상기 VNF의 구동을 위해 상기 Sec_EM과 VNF 간, 또는 상기 VNF간을 인증하는 단계; 및 (c) 상기 Sec_EM과 VNF 간, 또는 상기 VNF간 통신을 위해 통신 메시지를 암호화하여 통신하는 단계;를 포함하는 것을 특징으로 한다.

[0015] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법의 (a)단계는 (a-1) 상기 LW_PKI의 오케스트레이터(Orchestrator)가 상기 VNF에서 사용할 자원정보, VNFD(VNF Descriptor) 및 인증서 발급을 위한 씨큐리티 디스크립터 정보를 상기 LW_PKI의 가상화 인프라 관리부에 전달하는 단계; (a-2) 상기 가상화 인프라 관리부가 상기 씨큐리티 디스크립터 정보를 기반으로 인증서를 생성하여 Cert_DB에 저장하는 단계; (a-3) 상기 가상화 인프라 관리부가 상기 (a-2)단계에서 생성된 인증서를 상기 VNF가 설치되는 가상머신에 설치하여 컴퓨팅 노드에 로드(Placement)하는 단계; 및 (a-4) 상기 가상화 인프라 관리부가 VNF_ID 및 Tenant_ID를 상기 오케스트레이터에 응답하는 단계;를 포함하는 것을 특징으로 한다.

[0016] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법의 (a-2)단계는 (a-2-1) 상기 인증서 발행 서버 시스템 내의 등록 모듈은 상기 가상화 인프라 관리부의 발급 요청 메시지 내의 Tenant_ID, VNFD, VNF_ID 또는 Sec_EM_ID정보를 이용하여 인증서 발급을 요청한 VNF를 식별하고, 상기 인증서 발급 모듈에 상기 VNF의 인증서 발급을 요청하는 단계;를 더 포함하는 것을 특징으로 한다.

[0017] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법은 등록 모듈이 $Secret_{vni} = Tenant_ID \oplus VNF_ID$ 를 이용하여 인증서 발급을 요청한 VNF를 식별하는 것을 특징으로 한다.

[0018] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법은 테넌트가 처음 생성되는 경우 상기 Sec_EM이 Instantiation 될 때, 상기 Sec_EM을 위한 인증서가 발급되어 상기 Sec_EM을 구동시키는 것을 특징으로 한다.

[0019] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법의 (b)단계는 (b-1) 상기 Sec_EM이 자신의 ID_{Sec_EM}와 임의의 난스(Nonce) R_{SEC_EM}를 생성하여 전송하고 자신의 개인키로 암호화한 E_{CertSec_EM}(R_{Sec_EM})을 전송하여 전자서명하는 단계; (b-2) 상기 가상 네트워크 함수 관리부가 수신한 상기 E_{CertSec_EM}(R_{Sec_EM})를 복호화하기 위해서 상기 ID_{Sec_EM}을 이용하여 Cert DB 내 Cert_{Sec_EM}'를 검색하는 단계; (b-3) 상기 가상 네트워크 함수 관리부가 검색된 ID_{Sec_EM}에 해당하는 Cert_{Sec_EM}'을 인증서 검증 모듈로 전송하는 단계; 및 (b-4) 상기 인증서 검증 모듈이 전송된 R_{Sec_EM}과 Cert_{Sec_EM}으로 E_{CertSec_EM}(R_{Sec_EM})을 복호화하여 얻은 R_{Sec_EM}'과 비교하여 R_{Sec_EM}의 무결성과 Sec_EM을 인증하는 단계;를 포함하는 것을 특징으로 한다.

[0020] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법의 (b)단계는 (b-1)' 상기 VNF가 ID_{VNF}, R_{VNF}와 R_{VNF}의 무결성 검증을 위해 E_{CertVNF}(R_{VNF})을 상기 가상 네트워크 함수 관리부의 인증서 검증 서버 시스템에 전송하는 단계; (b-2)' 상기 가상 네트워크 함수 관리부가 Cert_{VNF}과 상기 Cert

DB 내 $Cert_{VNF}$ '을 비교하기 위해 ID_{VNF} 을 Cert DB로 전송하는 단계; (b-3)` 상기 가상 네트워크 함수 관리부가  $ID_{VNF}$ 에 해당하는  $Cert_{VNF}$ '을 인증서 검증 모듈로 전송하는 단계; 및 (b-4)` 상기 인증서 검증 모듈이 전송된 R_{VNF} 과 $Cert_{VNF}$ 으로 $E_{Cert_{VNF}}(R_{VNF})$ 을 복호화하여 얻은 R_{VNF} '과 비교하여 R_{VNF} 의 무결성과 상기 VNF를 인증하는 단계;를 포함하는 것을 특징으로 한다.

[0021] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법의 (c)단계는 (c-1) 상기 가상 네트워크 함수 관리부가 ID_{VNF} , ID_{Sec_EM} , and 난스(Nonce)를 이용하여 암호화 통신에 사용될 대칭키인(Symmetric key) DEK(Data Encryption Key)를 생성하는 단계; (c-2) 상기 가상 네트워크 함수 관리부가 생성된 상기 DEK를 상기 VNF에 전달하는 단계; (c-3) 상기 가상 네트워크 함수 관리부가 인증서 검증 서비스 시스템의 Cert DB에 보관된 $Cert_A$, $Cert_B$ 로 각각 암호화하여 상기 Sec_EM 또는 VNF에 해당되는 각 엔티티들에 전달하는 단계; 및 (c-4) 상기 엔티티들이 자신이 가지고 있는 인증서의 개인키를 이용하여 $E_{Cert_A}(R_A, DEK)$, $E_{Cert_B}(R_B, DEK)$ 을 복호화하여 얻은 DEK를 이용하여 메시지를 암호화하여 안전한 통신을 수행하는 단계;를 포함하는 것을 특징으로 한다.

[0022] 또한, 상술한 목적을 달성하기 위한 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법은 $DEK = ID_{VNF} \oplus ID_{Sec_EM} \oplus Nonce$ 을 이용하여 상기 가상 네트워크 함수 관리부가 DEK(Data Encryption Key)를 생성하는 것을 특징으로 한다.

발명의 효과

[0024] 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템을 이용한 통신방법은 VNF 간의 상호인증 및 데이터 보안을 이용하여 Fake VNF를 차단하고 AI(Artificial Intelligence) 기반의 비정상 행위 탐지 기법을 이용하여 VNF 간 전송되는 악성 트래픽을 차단할 수 있는 효과가 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템의 블록 구조도 이다.
 도 2는 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템의 Instantiation 과정을 설명하기 위한 도면이다.
 도 3은 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템의 Sec_EM과 VNF의 인증과정을 설명하기 위한 도면이다.
 도 4는 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템의 VNF간의 인증과정을 설명하기 위한 도면이다.
 도 5는 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템의 VNF간 암호화 통신 과정에 대해 설명하기 위한 도면이다.
 도 6은 인증서 기반 인증에 소요되는 시간의 그래프 도면이다.
 도 7은 인증서 기반 인증에 소요되는 System Resource의 그래프 도면이다.
 도 8은 데이터 셋의 개수를 증가시키면서 각 알고리즘 별로 계산된 탐지율에 대한 그래프 도면이다.
 도 9는 각 알고리즘을 동작시켰을 때의 리소스 점유율에 대한 그래프 도면이다.

발명을 실시하기 위한 구체적인 내용

[0027] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면을 참조하여 상세하게 설명하도록 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.

[0028] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만

사용된다. 예를 들어, 본 발명의 권리범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재 항목들의 조합 또는 복수의 관련된 기재 항목들 중의 어느 항목을 포함한다.

- [0029] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급될 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 언급될 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.
- [0030] 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.
- [0031] 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.
- [0032] 명세서 및 청구범위 전체에서, 어떤 부분이 어떤 구성 요소를 포함한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있다는 것을 의미한다.
- [0033] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0034] 도 1은 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템의 블록 구조도 이다.
- [0035] 도 1에 도시된 바와 같이 본 발명에 따른 NFV 환경을 위한 LW_PKI 시스템은 LW_PKI(100:LightWeight Public Key Infrastructure), 테넌트(200:Tenant) 네트워크 기능 가상화 시설(300:NFVI<Network Function Virtualization Infrastructure>), 운용/업무 지원시스템(400:OSS<Operation Support System>/BSS<Business Support System>) 및 씨큐리티 디스크립터(500: Security descriptor)를 포함한다.
- [0036] 상기 LW_PKI(100)는 두 개의 서브 시스템인 인증서 발생 서브 시스템(111:CIS<Certificate Issue Subsystem>)과 인증서 검증 서브 시스템(121:CVS<Certificate Verify Subsystem>)이 각각 가상화 인프라 관리부(110:VIM<Virtualized Infrastructure Managers>) 가상 네트워크 함수 관리부(120:VNFM<(Virtual Network Function Managers>))에 포함된다.
- [0037] 상기 인증서 발생 서브 시스템(111)은 인증서 발급 신청을 위한 등록 모듈(111a:RM<Registration Module>)과 상기 인증서의 발급신청에 따라 해당 인증서를 발급하는 인증서 발급 모듈(111b:CM<Certificate Module>)를 포함한다.
- [0038] 상기 인증서 검증 서브 시스템(121)은 상기 인증서 발급 모듈(111b)에서 발급된 인증서를 저장관리하는 Cert DB(121a)와 상기 Cert DB(121a)에 저장된 인증서를 검증하는 인증서 검증 모듈(121b:VM<Verification Module>)을 포함한다.
- [0039] 상기 테넌트(200)는 SeC_EM(210)과 복수의 VNF(220)을 포함하는데, 상기 SeC_EM(210)은 테넌트(200) 생성시 생성되고 인증서를 포함한다.
- [0040] 상기 VNF(220)의 인증서는 상기 VNF 인스턴스 생성과정에서 상기 인증서 발생 서브 시스템(111)의 인증서 발급 모듈(111b)에서 발급된다.
- [0041] 상기 씨큐리티 디스크립터(500)는 아래 표와 같이 정의되는 파라미터와 같은 인증서 생성을 위한 정보를 포함한다.

표 1

[0042]	Serial	Unique ID for certificate
	Signature Algorithm	Algorithm for digital signature
	Validity Period	Certificate validity period

Subject Public Key info	Information about public key subjects
Issuer Unique Identifier	ID for certificate issue
Subject Unique Identifier	ID(EM or VNF ID) for Certificate owner
Extensions	Reserved fields

- [0043] <parameter in security descriptor>
- [0044] 상기 씨큐리티 디스크립터(500)의 Serial은 인증서 식별을 위한 일련번호가 기입되며, Signature Algorithm은 인증서에 사용될 서명 알고리즘의 종류가 기입된다.
- [0045] Validity Period는 인증서의 유효 기간으로 Sec_EM과 VNF 이용 목적에 따른 보안 정책을 고려하여 기입한다.
- [0046] Subject Public Key info.에는 인증서 주체의 공개키에 대한 설명이 기입되고, Issuer Unique Identifier는 Sec_EM(210)과 VNF(220)의 ID(ID_{EM} , ID_{VNF})와 같이 인증서 발급 주체의 ID가 기입된다. 마지막으로 Subject Unique Identifier는 인증서주체의 ID(ID_{VNF} or ID_{Sec_EM})가 기입된다.
- [0047] 상술한 바와 같은 구성을 갖는 본 발명에 따른 NFV 환경을 위한 PKI 시스템 구성에 의한 VNF간 인증서 발급과정을 도 2를 참조하여 설명한다.
- [0048] 도 2에 도시된 바와 같이 (a)과정에서 상기 LW_PKI(100)의 오케스트레이터(130:Orchestrator)는 상기 VNF(220)가 사용할 자원정보, VNFD(VNF Descriptor) 및 인증서 발급을 위한 씨큐리티 디스크립터(500) 정보를 상기 가상화 인프라 관리부(110)에 전달한다.
- [0049] (b)과정에서 상기 가상화 인프라 관리부(110)는 상기 씨큐리티 디스크립터(500) 정보를 기반으로 인증서를 생성하여 상기 Cert_DB(121a)에 저장한다.
- [0050] (c)과정에서 상기 가상화 인프라 관리부(110)는 생성된 인증서를 상기 VNF(220)가 설치되는 가상머신에 설치하여 컴퓨팅 노드에 로드(Placement)한다.
- [0051] (d)과정에서 상기 가상화 인프라 관리부(110)는 VNF_ID 및 Tenant_ID를 상기 오케스트레이터(130)에 응답하게 된다.
- [0052] 만약, 처음 상기 테넌트(200)가 생성되는 경우 상기 Sec_EM(210)이 Instantiation 되는데, 이때 (e)과정에서 상기 Sec_EM(210)을 위한 인증서가 발급되어 Sec_EM(210)를 구동시킨다.
- [0053] 상기 인증서 발행 서버 시스템(111) 내의 등록 모듈(111a)은 상기 가상화 인프라 관리부(110)의 발급 요청 메시지 내의 Tenant_ID, VNFD, VNF_ID 또는 Sec_EM_ID정보를 이용하여 인증서 발급을 요청한 VNF(220)를 아래의 [수학식 1]을 이용하여 식별하고, 상기 인증서 발급 모듈(111b)에 상기 VNF인증서 발급을 요청한다.

수학식 1

[0054] $Secret_{vnf} = Tenant_ID \oplus VNF_ID$

- [0055] 상기 인증서 발급 모듈(111b)은 공개키/개인키 쌍을 생성하고 공개키 인증서를 발급하여 상기 가상화 인프라 관리부(110) 내의 Cert_DB(121a)에 보관한다.
- [0056] 도 3을 참조하여 인증서 기반의 Sec_EM 인증 과정에 대해 설명한다.
- [0057] VNF(220) 서비스 시작은 일반적으로 가상 네트워크 함수 관리부(120:VNFM) 혹은 EM(210)에 의해 시작된다. 상기 LW_PKI(100)에서는 상기 VNF(220)가 구동되기 위해 VNF(220)와 Sec_EM(210)과 상호인증과정이 필요하다.
- [0058] 다음의 표 2는 LW_PKI의 상호인증을 위한 파라메타이다.

표 2

[0059]

R_{Sec_EM} or R_{VNF}	Random Number for authentication about Sec_EM or VNF
$Cert_{Sec_EM}$ or $Cert_{VNF}$	Sec_EM or VNF certificate

Cert _{Sec_EM} ' or Cert _{VNF} '	Sec_EM or VNF certificate in Cert_DB
---	--------------------------------------

- [0060] (a) 과정에서 상기 Sec_EM(210)이 인증을 요청하는 단계이다. 이때 자신의 ID_{Sec_EM}와 임의의 난스(Nonce) R_{Sec_EM}를 생성하여 전송하고 자신의 개인키로 암호화한 E_{CertSec_EM}(R_{Sec_EM})을 전송하여 전자서명을 한다.
- [0061] (b) 과정에서 상기 가상 네트워크 함수 관리부(120:VNFM)는 수신한 E_{CertSec_EM}(R_{Sec_EM})를 복호화하기 위해서 ID_{Sec_EM}을 이용하여 Cert DB(121a) 내 Cert_{Sec_EM}'를 검색한다.
- [0062] (c) 과정에서 ID_{Sec_EM}에 해당하는 Cert_{Sec_EM}'을 상기 인증서 검증 모듈(121b:VM)로 전송한다.
- [0063] (d) 과정에서 상기 인증서 검증 모듈(121b:VM)은 전송된 R_{Sec_EM}과 Cert_{Sec_EM}으로 E_{CertSec_EM}(R_{Sec_EM})을 복호화하여 얻은 R_{Sec_EM}'과 비교하여 R_{Sec_EM}의 무결성과 Sec_EM을 인증한다. (e) 과정에서 VNF Auth ACK를 Sec_EM으로 전송한다.
- [0064] 마찬가지로 VNF 간 인증 과정은 도 4에 도시된 바와 같다.
- [0065] (a) 과정에서 상기 VNF(220)는 ID_{VNF}, R_{VNF}과 R_{VNF}의 무결성 검증을 위해 E_{CertVNF}(R_{VNF})을 상기 가상 네트워크 함수 관리부(120:VNFM)의 인증서 검증 서버 시스템(121:CVS)에 전송한다.
- [0066] (b) 과정에서 상기 가상 네트워크 함수 관리부(120:VNFM)은 Cert_{VNF}과 상기 Cert DB(121a) 내 Cert_{VNF}'을 비교하기 위해 ID_{VNF}을 Cert DB(121a)로 전송한다.
- [0067] (c) 과정에서는 ID_{VNF}에 해당하는 Cert_{VNF}'을 인증서 검증 모듈(121b:VM)으로 전송한다.
- [0068] (d) 과정에서 상기 인증서 검증 모듈(121b:VM)은 전송된 R_{VNF}과 Cert_{VNF}으로 E_{CertVNF}(R_{VNF})을 복호화하여 얻은 R_{VNF}'과 비교하여 R_{VNF}의 무결성과 VNF를 인증한다.
- [0069] (e) 과정에서 VNF Auth ACK를 상기 VNF(220)로 전송하여 Sec_EM(210)과 VNF(220) 간 상호 인증을 완료한다. 상기 VNF(220) 간 인증도 위와 동일한 과정으로 상기 가상 네트워크 함수 관리부(120:VNFM)의 인증서 검증 서버 시스템(121:CVS)에서 수행된다.
- [0070] 도 5를 참조하여 VNF간 암호화 통신 과정에 대해 설명한다.
- [0071] 상기 테넌트(200) 내의 VNF(220) 간 안전한 통신을 위해 통신 메시지를 암호화하는 과정을 설명한다. 아래의 [표 3]은 데이터 보안 키 생성을 위한 파라메타이다.

표 3

R _{A or B}	Random Number for authentication about VNF
Cert _{A or B}	VNF certificate
Cert _{A' or B'}	VNF certificate in Cert_DB
DEK	Data Encryption Key

- [0073] 상기 Sec_EM(210)과 VNF(220) 간 또는 VNF(200)간의 인증 과정을 거친 후에 ID_{VNF}, ID_{Sec_EM}, and 난스(Nonce)를 이용하여 아래의 [수학식 2]와 같이 암호화 통신에 사용될 대칭키인(Symmetric key) DEK(Data Encryption Key)를 생성한다. 그리고 도 5에 도시된 바와 같이 상기 가상 네트워크 함수 관리부(120:VNFM)는 생성된 상기 DEK를 상기 VNF(220)에 전달한다.

수학식 2

- [0074]
$$DEK = ID_{VNF} \oplus ID_{Sec_EM} \oplus Nonce$$

- [0075] 생성된 상기 DEK는 인증서 검증 서버 시스템(121:CVS)의 Cert DB(121a)에 보관된 Cert_A, Cert_B 로 각각 암호화하여 각 엔티티들에 전달한다.
- [0076] 각 엔티티는 자신이 가지고 있는 인증서의 개인키를 이용하여 E_{CertA}(R_A, DEK), E_{CertB}(R_B, DEK)을 복호화하여 DEK를 얻는다. VNF A와 VNF B는 DEK를 이용하여 메시지를 암호화하여 안전한 통신을 수행한다.
- [0077] 기존의 NFV 환경에서 EM과 VNF의 신뢰 여부를 검증하지 않기 때문에 터너트 내에 Fake VNF가 로드되어 전체 네트워크가 위협할 수 있다. 따라서 본 발명은 인증되지 않은 VNF를 식별하고, VNF간 암호화 통신을 이용하여 안전한 NFV 환경을 보장한다.
- [0078] 이하에서 본 발명에 따른 NFV 환경을 위한 LW-PKI 시스템의 성능을 살펴본다.
- [0079] 기존 NFV 환경과 LW-PKI가 적용 중인 NFV 환경에서 가상머신의 System Resource와 인증에 소요시간을 분석하여 성능을 비교한다. 그리고 여러가지 인공지능 알고리즘을 이용하여 VNF간 전송되는 트래픽을 정보를 기반으로 DDos 공격의 탐지 성공률 비교한다. 실험에 사용되는 테넌트(200)는 3개이며, 각 테넌트(200) 내에는 10개의 인증서 검증 모듈(121b:VM)이 존재한다. 그리고 각 인증서 검증 모듈(121b:VM)마다 VNF(220) 1개를 설정했으며, CPU 1개, 2GB의 메모리를 할당했다.
- [0080] 상기 테넌트(200) 내 인증은 Sec_EM(210)과 VNF(220)간(authentication between Sec_EM and VNF), VNF들간(authentication between VNFs)에 수행된다. 총 10번의 시험을 진행하였다. 인증 수단으로는 PKI 인증서를 이용하였으며, 인증서 기반 인증에 소요되는 시간은 도 6과 같다.
- [0081] 실제 환경에서 상기 LW-PKI(100)를 적용했을 때와 가상 환경에서 LW-PKI(100)를 적용했을 때의 인증에 소요되는 시간을 비교했을 때, 실제 환경에서는 평균 0.28s가 소요되었으며, Virtual 환경에서는 평균 0.59s가 소요된 것을 확인할 수 있다. 가상 환경에서는 실제 환경에 비해 0.31s 가량 시간이 더 소요된다. 인증서 기반 인증에 소요되는 System Resource는 도 7에 도시된 바와 같다.
- [0082] 상기 LW-PKI(100)가 실제 환경과 가상환경에서 동작 중일 때의 System resource를 비교했다. 실제 환경에서는 평균적으로 4.2%가 소요되었으며, 가상 환경에서는 4.2%가 소요된 것을 확인할 수 있다.
- [0083] 가상 환경에서는 실제 환경에 비해서 평균적으로 동일한 system resource가 소요된 것을 확인할 수 있다. 따라서 상기 LW-PKI(100)는 가상환경에서 실제 환경에 비해 0.31s가 소요되었으며, system resource는 별도의 오버헤드가 없다.
- [0084] 상기 테넌트(200) 내 VNF(220) 간 전송되는 트래픽의 통계 정보를 이용하고, 인공지능 알고리즘을 적용하여 VNF 간 대표적인 DDos 공격인 ICMP Flooding, SYN Flooding, UDP Flooding 공격의 탐지율을 측정했다.
- [0085] 실험에 사용되는 알고리즘은 FarthestFirst, HierarchicalCluster, LVQ(Learning Vector Quantization)이며, 실험에 사용되는 트래픽은 아래의 [표 4]와 같다.

표 4

ICMP Traffic	SYS Traffic	UDP Traffic
74 byte-1000 byte	1500 byte	74 byte ~ 1000 byte

- [0087] 실험 트래픽은 한국에서 2009년에 발생한 7.7 DDos 공격 트래픽 정보를 기반으로 실험에 사용할 트래픽에 대한 Data set을 작성하였다. 트래픽에 포함된 프로토콜은 ICMP, SYN, UDP이며, bps는 최대 200Kbps, pps는 최대 3K pps이다.
- [0088] 실험 트래픽의 DDos 여부를 판별하고, 판별 결과가 실제 결과와 동일한지를 비교하여 탐지율을 계산한다. 실험에 사용된 데이터 셋의 개수를 증가시키면서 각 알고리즘 별로 계산된 탐지율과 실제 공격 비율을 비교하였다. 각 알고리즘 별로 탐지율은 도 8에 도시된 바와 같다.
- [0089] 각 알고리즘을 적용했을 때 탐지율과 실제 공격 트래픽의 비율을 비교했을 때, 데이터 셋의 수가 많아질수록 탐지 정확도가 상승된 것을 확인할 수 있다. 그리고 알고리즘 별 DDos 탐지 오차의 평균은 Farthest First 알고리즘은 11.3%, Hierarchical cluster 알고리즘은 12.0%, LVQ 알고리즘은 22.1%로 측정되었다.
- [0090] Farthest First 알고리즘이 Hierarchical cluster 알고리즘과 LVQ 알고리즘의 탐지율 오차보다 0.7%, 10.8% 우

수한 것을 확인할 수 있다. 각 알고리즘을 동작시켰을 때의 리소스 점유율은 도 9에 도시된 바와 같다.

[0091] 세가지 알고리즘은 동작 중에, 각각 CPU 자원의 1% 이내를 소모한다. 각 알고리즘 별로 동작에 사용되는 System resource는 Farthest First 알고리즘은 0.30%, Hierarichical clustering 알고리즘은 0.49%, LVQ 알고리즘은 0.52%로 측정되었다.

[0092] Farthest First이 Hierarichical Clustering보다 0.19%, LVQ보다 0.22%로 CPU 자원을 더 적게 소모하는 것을 확인할 수 있다.

[0093] 따라서 종합적으로 세가지 인공지능 알고리즘 중 Farthest First 알고리즘이 Hierarichical clustering 알고리즘, LVQ 알고리즘보다 높은 탐지율을 가지고, 더 적은 CPU 자원을 소모한다.

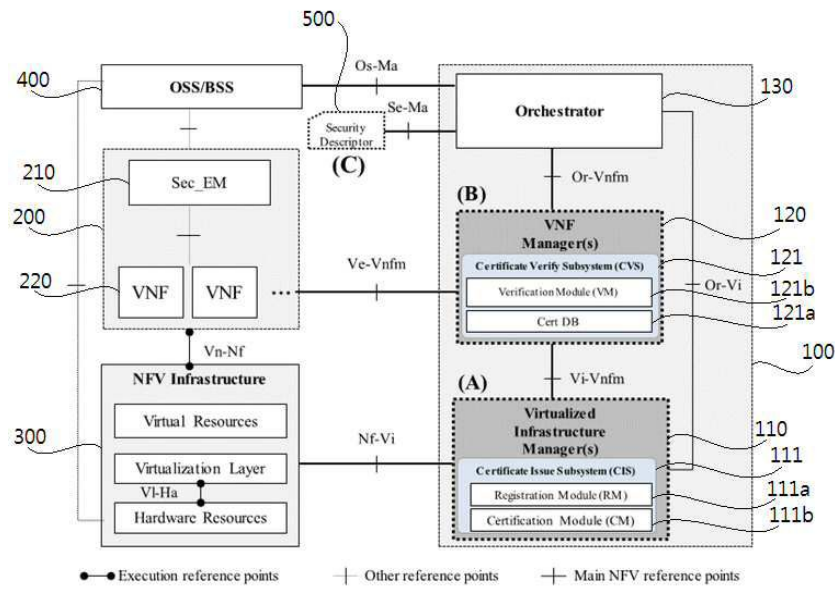
[0094] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 사람이라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

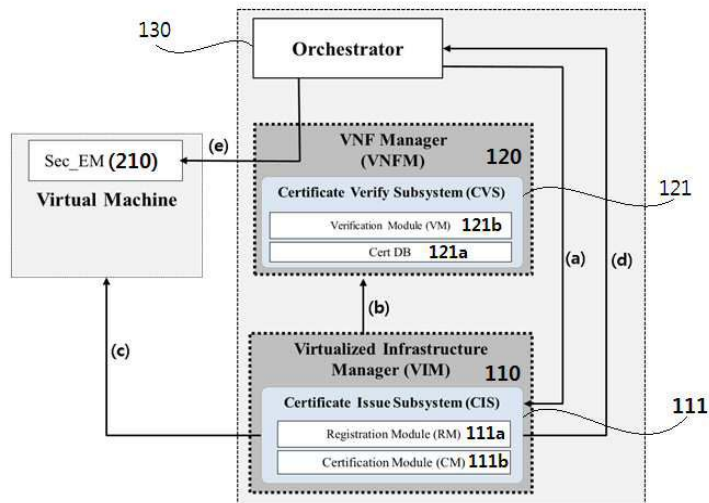
[0095] 100 : LW_PKI(LightWeight_Public Key Infrastructure),
 110 : 가상화 인프라 관리부(VIM:Virtualized Infrastructure Managers)
 111 : 인증서 발행 서브 시스템(CIS:Certificate Issue Subsystem)
 111a : 등록 모듈(RM:Registration Module)
 111b : 인증서 발급 모듈(CM:Certificate Module)
 120 : 가상 네트워크 함수 관리부(VNFM:Virtual Network Function Managers)
 121 : 인증서 검증 서브 시스템(CVS:Certificate Verify Subsystem)
 121a : Cert DB
 121b : 인증서 검증 모듈(VM:Verification Module)
 200 : 테넌트(Tenant)
 210 : SeC_EM
 220 : VNF
 300 : 네트워크 기능 가상화 시설(NFVI<Network Function Virtualization Infrastructure>)
 400 : 운용/업무 지원시스템(OSS<Operation Support System>/BSS<Business Support System>)
 500 : 씨큐리티 디스크립터

도면

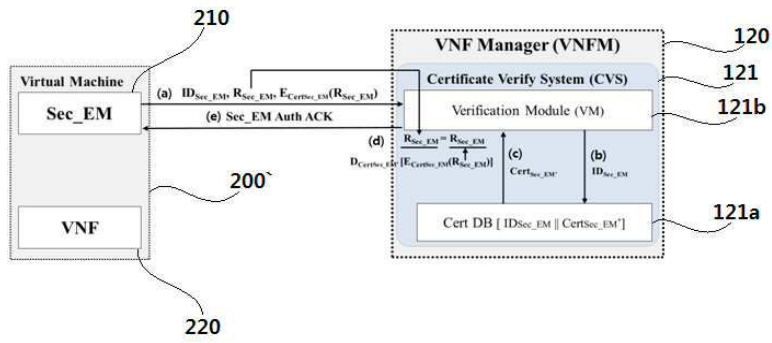
도면1



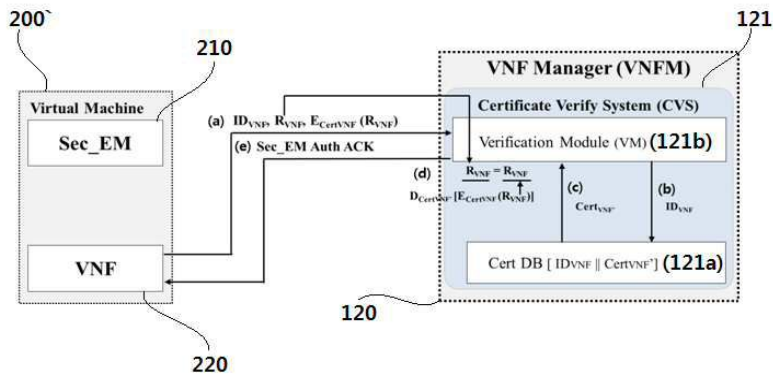
도면2



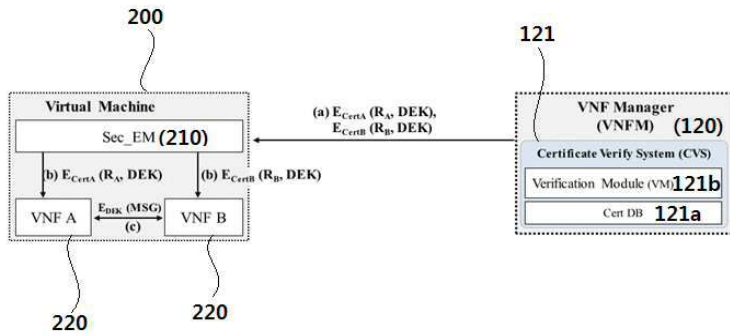
도면3



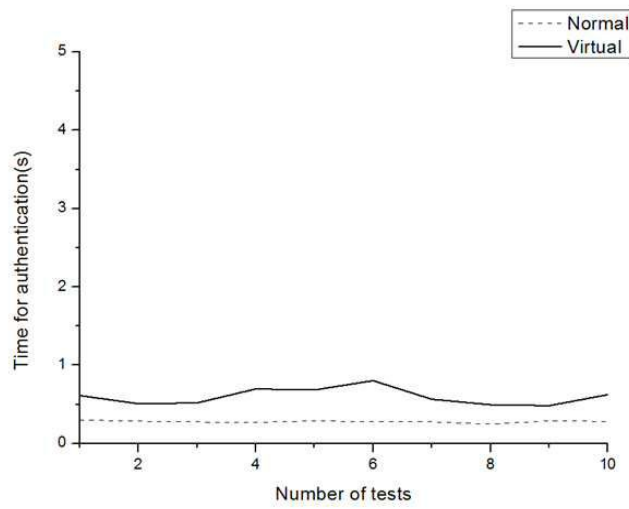
도면4



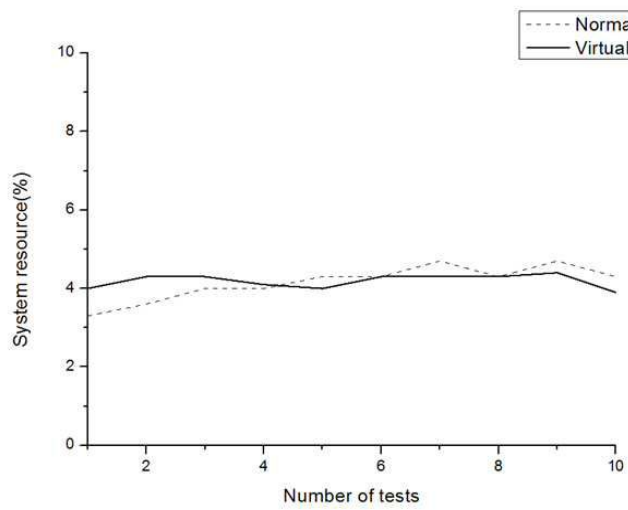
도면5



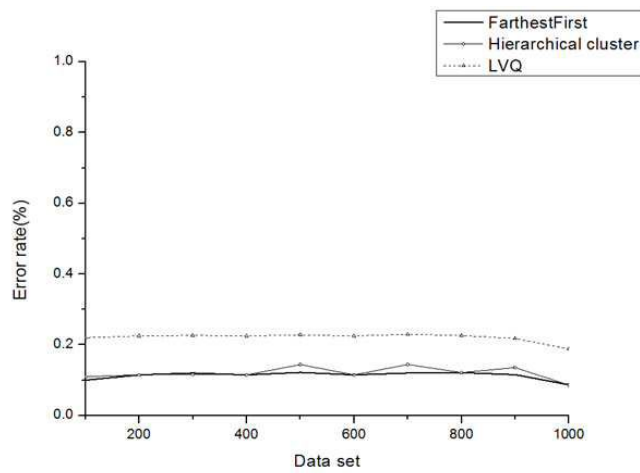
도면6



도면7



도면8



도면9

