Article

Utilizing a Lightweight PKI Mechanism to Guarantee a Secure Service in a Cloud Environment

Sangho Park [1], Hyunjin Kim [2], Jaehyung Park[3] and Jaecheol Ryou [4]*

[1] JiranSoft Researh Center, 87, Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea ; shpark@jiran.com
[2] Department of Computer Engineering, Chungnam National University, 99, Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea ; be.successor@gmail.com
[3] School of Electronics and Computer Engineering, Chonnam National University,77 Yongbong-ro, Buk-gu, Gwangju, 61186, Republic of Korea ; hyeoung@chonnam.ac.kr
[4] Department of Computer Engineering, Chungnam National University, 99, Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea ; jcryou@cnu.ac.kr
* Correspondence: jcryou@cnu.ac.kr; Tel.: +82-10-4410-4292

Abstract: Recently, cloud technology has become popular for smart societies. The Cloud technology has made dynamical network changes by enabling the construction of a logical network without building a physical network. Despite recent research on the cloud, it is necessary to study security functions for the identification of fake VNFs and the encryption of communication between entities. In this paper, we proposed an LW_PKI mechanism that detects a fake VNF and guarantees data security through mutual authentication between VNFs. To evaluate the LW_PKI, we built a MANO environment to test the performance of authentication and key generation for data security. In addition, we applied the artificial intelligence algorithm to detect abnormal behavior by using real attack data in the MANO environment. The LW_PKI guaranteed the reliability of a smart service by enhancing the security of the cloud environment.

Keywords: Energy-efficient communications; Green and cloud computing; Network Function Virtualization; Lightweight PKI; Authentication; DDOS; Artificial Intelligence

---

1. Introduction

Recently, cloud technology has been used to solve energy shortage problems caused by climate change and population growth because cloud technology reduces CAPEX and OPEX by building a logical network without building a physical network. In particular, cloud technology has increased interest in using virtualization technology to provide effective control of services and escape hardware constraints. Because virtualization technology creates a logical network without building a physical network, changing service environments can be rapidly adapted to. The interest in virtualization technology has led to a lot of research on NFV (Network Functions Virtualization) and MANO (Management and Orchestration). In particular, NFV is a core technology for next generation networks and 5G. NFV is a technology that separates software functions from hardware-dependent network devices and provides services through infrastructure based on a general-purpose server. On the other hand, MANO is a core module of NFV that manages different platform layers and configures network services [1-2]. With the spread of cloud computing-based virtual service platforms, various services are increasing. Besides, new application services are emerging to satisfy user requirements. Despite recent research, it is necessary to study security mechanisms against fake VNFs and data leakages, and abnormal behavior. That is, mutual authentication between entities and encryption of communication are not guaranteed in the cloud environment. Through the threats, attackers can access shared resources, and services can be disabled through an attacker's abnormal behavior. Thus, a security mechanism to ensure reliability in a cloud environment is essential.

There are three main security threats in an NFV environment. The first security threat is that there is no mutual authentication between VNFs or a VNF and an EM(Element Management). Mutual

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 February 2018 doi:10.20944/preprints201802.0132.v1

authentication guarantees secure communication between a VNF and a VNF, and between a VNF and an EM against a man-in-the middle attack in a multi-tenant environment. The second security threat is VNF services data leakages. Data security between VNFs can prevent data theft by fake VNFs and contaminated VNFs. The last security threat is a resource consumption attack due to the contamination of a VNF. The abnormal behavior of contaminated VNFs affects the overall service in a virtualized network. In this paper, we propose a lightweight PKI (LW_PKI) that performs mutual authentication between VNFs in a virtual environment and generates secure communication by using a security key for data security. The LW_PKI blocks fake VNFs through the mutual authentication and data security between VNFs.

In addition, in this paper, the performance of various AI (Artificial Intelligence) algorithms used for abnormal behavior detection is measured. To test abnormal behavior detection by the AI algorithms, we used 7.7 DDoS attack data which occurred in 2009 [3].

The subsequent sections of this paper are organized as follows: In Section II, we discuss the concept of PKI, abnormal behavior detection, and various artificial intelligence techniques. In Section III, we describe the LW_PKI developed in this study, and in Section IV, the LW_PKI is tested for performance of mutual authentication, and security key sharing and abnormal behavior detection. Finally, this paper is concluded in Section V.

2. Related Work

2.1. PKI : Public Key Infrastructure

PKI is the framework that guarantees secure data exchanges using a private key and a public key which users receive from a trusted authority in an insecure public network [4]. A PKI is constructed with a CA (Certificate Authority), an RA (Registration Authority) and a VA (Validation Authority) [5]. Each entity in a PKI has a public key for CA and a certificate which includes its private key and public key. The authentication begins when an initiator requests authentication by transmitting a certificate signed with its own private key. A CA that receives a certificate signed with a private key can decrypt the certificate with its own public key, and authenticate the initiator using the received public key from an authentication request message. Besides CAs, PKIs have RAs that carry out registration procedures, and a VA that validates certificates. Finally, the other party's public key, obtained in the authentication process of the entity, is used as an encryption key in data communication because data encrypted by a public key can be decrypted using a private key by the other party [6]. Even if a PKI authenticates with the other party via the trusted certification authority, and guarantees secure communication with the other party, when the PKI components RA, CA, and VA install in a virtual environment, a large amount of resource is required, and overhead occurs [7]. Therefore, the LW_PKI is considered with the overhead of a PKI in a virtual environment. In this paper, we propose an LW_PKI (Lightweight PKI) which is suitable for a MANO based virtual environment. The LW_PKI can guarantee mutual authentication and encrypted data communication without changing existing MANO functions.

2.2. Abnormal Behavior

DoS (denial of service) affects services because system resources are exhausted by an attack. In other words, a DDoS (distributed DoS) attack against internet services is difficult to prevent due to the vulnerability of protocols. In addition, The smart service is more vulnerable to DDoS attacks because they are located in distributed locations and attack targets at the same time [8-9]. Furthermore a DDoS attack uses multiple botnets to attack the cloud system, consuming shared resources more rapidly than a DoS attack, and lowering the efficiency of computing energy.

Bandwidth consuming attacks, resource consuming attacks, and application attacks are representative DDoS attacks [10]. In a bandwidth consuming attack, an attacker controls many zombies to generate a large number of packets to exceed the network bandwidth capacity. In particular, a bandwidth consuming attack can cause a connection failure to other systems in the same network. UDP flooding, which transmits a large number of UDP packets, and ICMP flooding, which

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 February 2018 doi:10.20944/preprints201802.0132.v1

uses a large number of ICMP packets, are examples of bandwidth consuming attacks [11]. In a resource consuming attack, an attacker increases the CPU load of a system by increasing the packet throughput using TCP. Although a resource consuming attack does not increase the bps, it generates system overhead due to an increase in pps (packets per second). SYN flooding attack using a SYN packet is an example of a resource consuming attack [12]. Finally, in an application attack, an attacker generates a disorder of system services through excessive application access. The Slowloris DDoS attack, incidents of which have recently increased, is an application attack. In the Slowloris DDoS attack, an attacker uses two methods. One is the HCCP CC method through which an attacker interrupts the use of cache by a system, and the other is HTTP GET flooding through which an attacker uses an abundance of HTTP GET messages for attacks [13]. Since the NFV environment is a virtual environment, an attacker can load multiple VNFs in a tenant. Therefore, an attacker can cause a bandwidth exhaustion attack that depletes a virtual network bandwidth using a large number of packets in the network, resulting in great damage that paralyzes a whole network. In other words, if an attacker makes a botnet with a VNF in a tenant, the botnet can infect all VNFs in the tenant, and cause the paralysis of services. However, DDoS attacks can be prevented by communication after verifying the identity of a VNF using a PKI certificate. Therefore, it is possible to block abnormal behavior through authentication of the traffic sender and white list-based communication.

2.3. Artificial Intelligence

AI (Artificial intelligence) requires a long learning time; however, we can determine whether various input traffic is an attack or not. Among AI techniques, a clustering algorithm can be used for abnormal behavior detection [14] because a clustering algorithm can detect a pattern in a large amount of data and identify an attack by the pattern. Representative clustering algorithms are Farthest First, Hierarchical Cluster, and LVQ [15]. Using the Farthest First algorithm, observed data is clustered by selecting specific data and classified the data while searching for data in order of data having a large difference from the designated data. The Farthest First algorithm uses a method for discriminating the similarity of data by using differences between the data [16]. Using the Hierarchical algorithm, observed data can be clustered into groups without specifying the number of groups. The Hierarchical cluster algorithm uses an agglomerative method which specifies data and merges the data with the closest group, and a division method which divides a large group into smaller groups according to criteria [17]. The LVQ algorithm is a supervised learning algorithm for clustering input vectors according to initial weights using a competitive learning method. The similarity between the data on input layers and the data on output layers is calculated, and the reference data is updated according to the similarity. The observed data is clustered while repeating the process of calculation and updating [18]. Using these clustering algorithms, we can determine whether traffic between VNFs in a virtual environment is abnormal or not. Therefore, if a VNF infected by an attacker performs an abnormal behavior, we can detect the DDoS attack using an AI algorithm, and protect VNFs by blocking traffic from the source.

3. The Lightweight PKI

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 February 2018 doi:10.20944/preprints201802.0132.v1

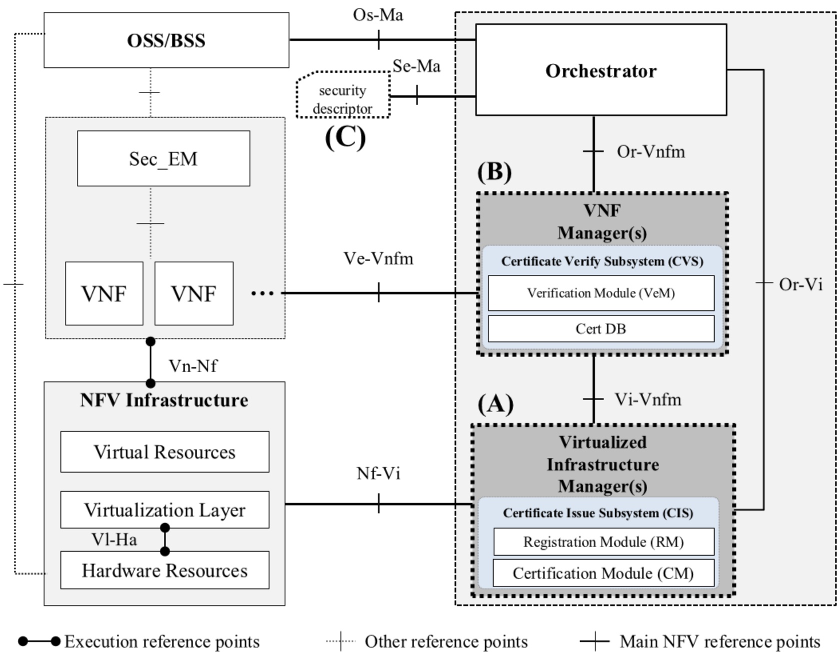

Figure 1. The architecture of the LW_PKI.

The LW_PKI consisted of a CIS (Certificate Issue Subsystem) and a CVS (Certificate Verify Subsystem). (A) was a CIS for registering a certificate and issuing a certificate in the VIM, and (B) was a CVS for verifying a VNF issued certificate. (C) was a security descriptor that contained information for generating a certificate. A certificate was issued by the LW_PKI when a VNF or an EM was installed in the virtual machine. Each VNF and EM use issued certificates for mutual authentication and data security.

3.1. LW_PKI:Lightweight Public Key Infrastructure

The CIS of the LW_PKI consisted of an RM (Registration Module), which was a certificate registration module, and a CM (Certificate Module), which was a certificate issue module. In addition, the CVS was composed of a VeM (Verification Module) for verifying certificates, and a CertDB for storing certificates. The SeC_EM included its own certificate when a tenant was created, and a VNF certificate was issued from the CM in the CIS during a VNF instantiation process. We defined a security descriptor for information about issuing certificates. Table 1 shows the contents of the security descriptor.

Table 1. Contents of the security descriptor.

Field	Contents
Serial	Unique ID for certificate
Signature Algorithm	Algorithm for digital signature
Validity Period	Certificiate validity period
Subject Public Key Info.	Information about public key subjects
Issuer Unique Identifier	ID for certificate issuer
Subject Unique Identifier	EM ID(or VNF ID) for Certificate owner
Extensions	Reserved fields

Serial was a serial number for identifying a certificate, and the signature algorithm was the signature algorithm to be used for the certificate. Validity Period was the term of validity for a certificate, and this value was input giving consideration to the security policy according to the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 February 2018 doi:10.20944/preprints201802.0132.v1

purpose of the Sec_EM and VNF. Subject Public Key Info. was the information of the public key for subjects, and Issuer Unique Identifier was an ID for the subject of a certificate such as Sec_EM's ID (ID_{Sec_EM}) and VNF's ID (ID_{VNF}). Finally, the Subject Unique Identifier was the ID (ID_{VNF} or ID_{Sec_EM}) of a certificate subject. Figure 2 shows the VNF instantiation process.

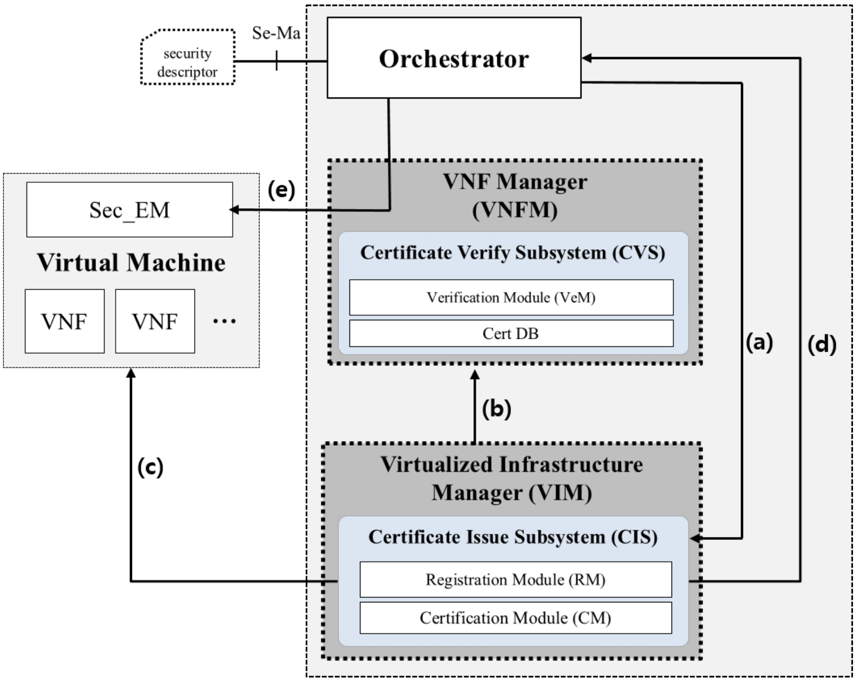

Figure 2. The VNF Instantiation process.

In process (a), the Orchestrator transmits the VNFD (VNF descriptor), the resource information, and the security descriptor for issuing a certificate to the VIM. (b) is the process in which the VIM generates a certificate based on security descriptor information, and stores it in the Cert_DB. In process (c), the VIM installs a certificate in the virtual machine where a VNF will be placed. In process (d), the VIM transmits a VNF_ID and a Tenant_ID to the Orchestrator. In case of tenant creation, instantiation of the Sec_EM is required. The Sec_EM starts with its own certificate in process (e). The RM identifies the VNF requesting certificate issuance using information such as Tenant_ID, VNF_ID or EM_ID, and VNFD, and requests the CM to issue a certificate. Identification of a VNF is implemented using equation:

$$Secret_{vnf} = Tenant\_ID \oplus VNF\_ID \quad (1)$$

The CM creates a key pair (Public key and Private Key) and issues a certificate, and stores the certificate in the Cert DB.

3.2. Mutual Authentication

In general, a VNF service is started by a VNFM or a Sec_EM. To start a VNF, mutual authentication was needed between a VNF and a Sec_EM in the LW_PKI. In Table 2, the parameters for mutual authentication can be seen.

Table 2. Parameters in authentication between VNF and Sec_EM.

Parameter	Information
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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 February 2018 doi:10.20944/preprints201802.0132.v1

The mutual authentication process is shown in Figure 3.

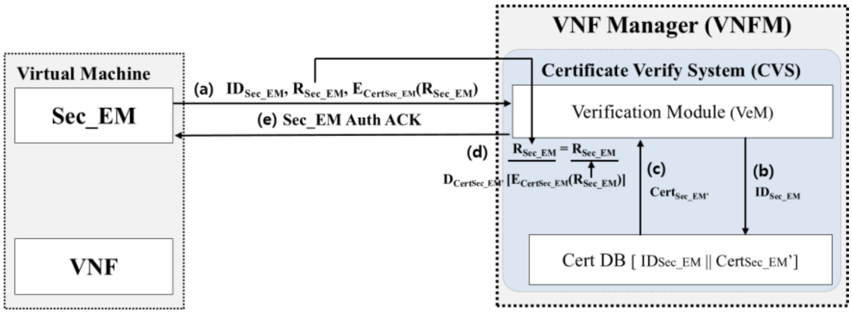

Figure 3. The authentication process between a Sec_EM and a VNF.

(a) is the process through which the Sec_EM requests authentication. During the authentication process, the Sec_EM transmits its own ID (ID_{Sec_EM}), Random value R_{SEC_EM}, and $E_{CertSec\_EM}$ (R_{Sec_EM}) which is encrypted with its own private key for digital signatures. In process (b), the VNFM searches the $Cert_{Sec\_EM}'$ with a received ID_{Sec_EM} in the Cert DB to decrypt a received $E_{CertSec\_EM}$ (R_{Sec_EM}). (c) is the process of searching the $Cert_{Sec\_EM}'$ corresponding to the IDSec_EM. In process (d), the VeM compares the R_{Sec_EM} with R_{Sec_EM}' after the decryption of the $E_{CertSec\_EM}$ ($R_{Sec\_EM'}$) by the $Cert_{Sec\_EM}$ to authenticate the Sec_EM and verify the integrity of the R_{Sec_EM}. In process (e), the VNFM transmits the VNF Auth ACK message to the Sec_EM. Similarly, the VNF to VNF authentication process is shown in Figure 4.

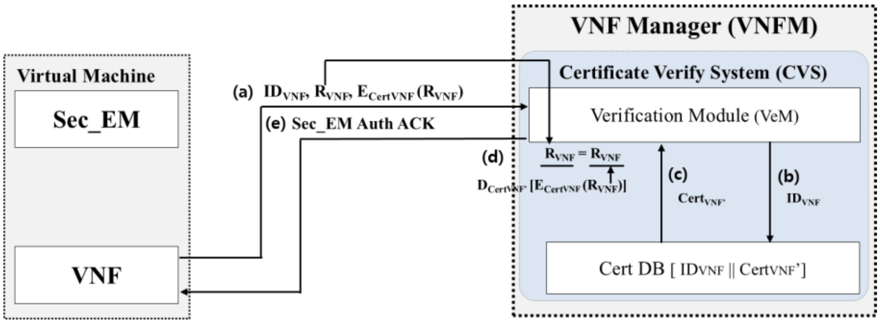

Figure 4. The authentication process between VNFs.

In process (a), the VNF transmits an ID_{VNF}, an R_{VNF}, and an $E_{CertVNF}$ (R_{VNF}) to the CVS in the VNFM. In process (b), the VNFM transmits the ID_{VNF} to the Cert DB for comparing the $Cert_{VNF}$ with the $Cert_{VNF}'$ in the Cert DB. In process (c), the Cert DB relays the $Cert_{VNF}'$ corresponding ID_{VNF} to the VeM. In process (d), the VeM compares the R_{VNF} with the R_{VNF}' after decrypting the $E_{CertSec\_EM}$ ($R_{VNF'}$) to authenticate the VNF and verify the integrity of the R_{VNF}. In process (e), the VNFM transmits a VNF ACK message to complete the mutual authentication between the Sec_EM and VNFs. Authentication between VNFs is performed by a CVS in a VNFM like the above process.

3.3. Secure Communication

The process of achieving secure communication between VNFs in the same tenant is as follows. In Table 3, the parameters to create the data encryption key are shown.

Table 3. Parameters in secure communication between VNFs.

Parameter	Information
$R_{A\ or\ B}$	Random Number for authentication about VNF
$Cert_{A\ or\ B}$	VNF certificate
$Cert_{A'\ or\ B}$	VNF certificate in Cert_DB

 doi:10.20944/preprints201802.0132.v1

DEK	Data Encryption Key

After the authentication between a Sec_EM and a VNF, or between a VNF and a VNF, a symmetric key DEK (data encryption key) for encrypting a communication is generated using ID_{VNF} ID_{Sec_EM}, and Nonce. The VNFM transmits a DEK to a VNF, as shown in Figure 5.

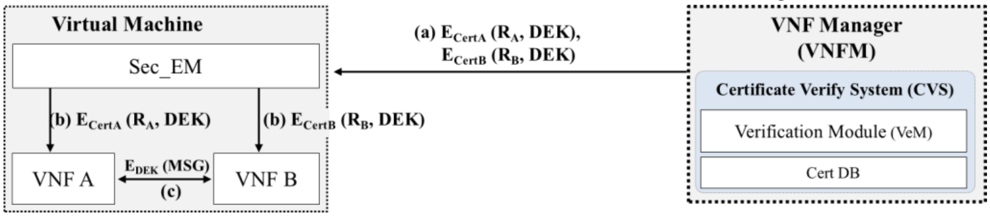

Figure 5. The secure communication between VNFs.

The generation process for a DEK is shown in equation:

$$DEK = ID_{VNF} \oplus ID_{Sec\_EM} \oplus Nonce \qquad (2)$$

The VNFM encrypts a generated DEK with a $Cert_A$ or a $Cert_B$ stored in the Cert DB, and transmits it with parameters to all VNFs. Each VNF obtains a DEK after decrypting an E_{CertA} (R_A, DEK) and E_{CertB} (R_B, DEK) using the private key of the certificate. In other words, a VNF A and B encrypt messages and communicate securely with each other.

4. Implementation and Performance

In this chapter, we analyze the performance of the LW_PKI. Regarding the performance of the LW_PKI, we performed two tests. The first test analyzed the time and system resources required for VNF authentication when the LW_PKI was applied in an NFV environment. The second test compared the detection rate of a DDoS using various artificial intelligence algorithms in a virtual environment. There were three tenants used in the test, and there were ten VMs in each tenant. We set one VNF for each VM, and allocated 1 CPU and 2 GB of memory.

4.1. Implemenatation and Performance

In a tenant, mutual authentication was performed between a Sec_EM and a VNF, or between VNFs. We used PKI certificate based authentication, and the time required for authentication is shown in Figure 6.

 doi:10.20944/preprints201802.0132.v1

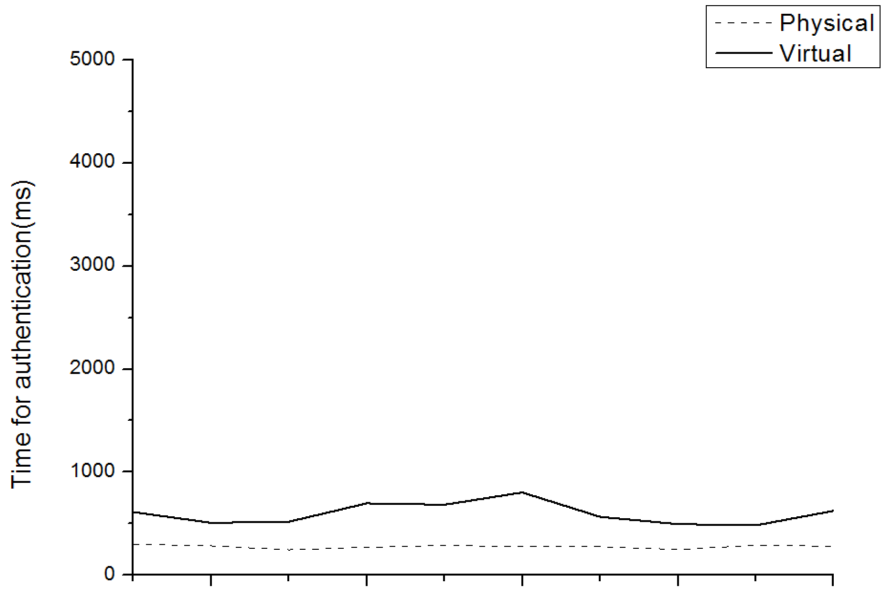

Figure 6. Authentication time in LW_PKI.

Figure 6 shows that the average authentication in the physical environment is 0.28 seconds and 0.59 seconds is required in the virtual environment. The average authentication time in the virtual environment takes about 47% more time than the physical environment. Figure 7 shows the system resource requirements for certificate-based authentication.

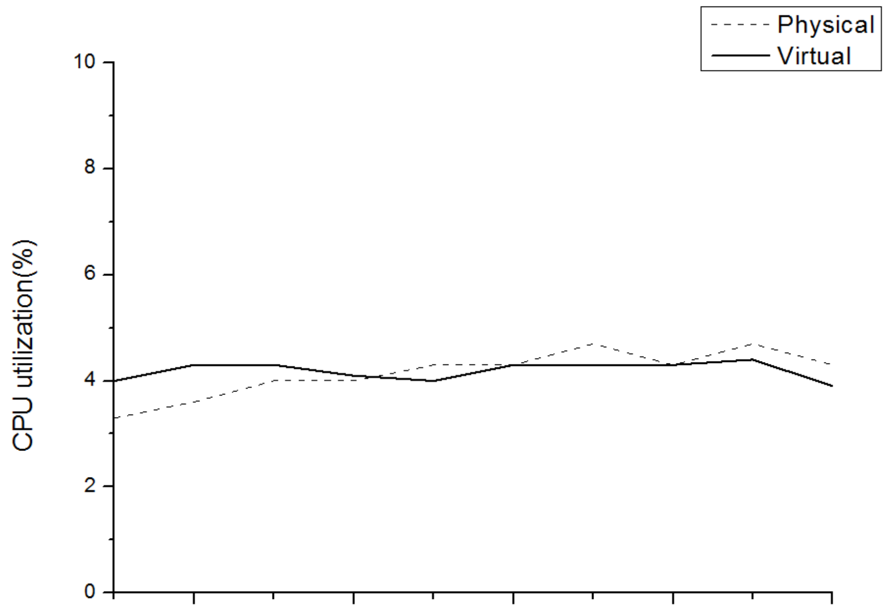

Figure 7. CPU utilization for authentication.

We compared the CPU utilization when the LW-PKI was operating in an actual and a virtual environment. On average, the CPU utilization on the physical machine was 4.2%, and also 4.2% on the virtual machine. The system resource showed that the virtual environment and the physical environment used the same amount of resources. Therefore, the LW-PKI in a virtual environment took 0.31 seconds longer than in a physical environment, and system resource had no overhead.

4.2. DDoS Attack Detection Using AIs

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 February 2018 doi:10.20944/preprints201802.0132.v1

To test for abnormal behavior contaminating VNFs in the same tenant, various artificial intelligence algorithms were used. We used ICMP flooding, SYN flooding, and UDP flooding for DDoS attacks, and compared the performance of each algorithm. The AI algorithms used in the test were Farthest First, Hierarchical Cluster and LVQ (Learning Vector Quantization). The attack traffic used in the test is shown in Table 4.

Table 4. Input Traffic.

ICMP Traffic	SYN Traffic	UDP Traffic
74 byte – 1000 byte	1500 byte	74 byte – 1000 byte

On July 4, 2009, important sites in the world such as the White House and the NASDAQ in the USA, and in South Korea, the Blue House and the Ministry of National Defense on July 7 of the same year were targets for attack. These attacks have been called the 7.7 DDoS attacks. The attack traffic for the tests in this study was obtained from the 7.7 DDoS attacks [3]. The protocols of the attack traffic were ICMP, SYN, and UDP, and bps (bits per second) was up to 200Kbps, and pps (packets per second) was up to 3Kpps. The detection rates of the DDoS attacks were calculated by comparing whether the test results were the same as the actual results or not. Increasing the number of datasets, we compared the detection rate and the actual attack rate for each algorithm. The detection rate for each algorithm is shown in Figure 8.

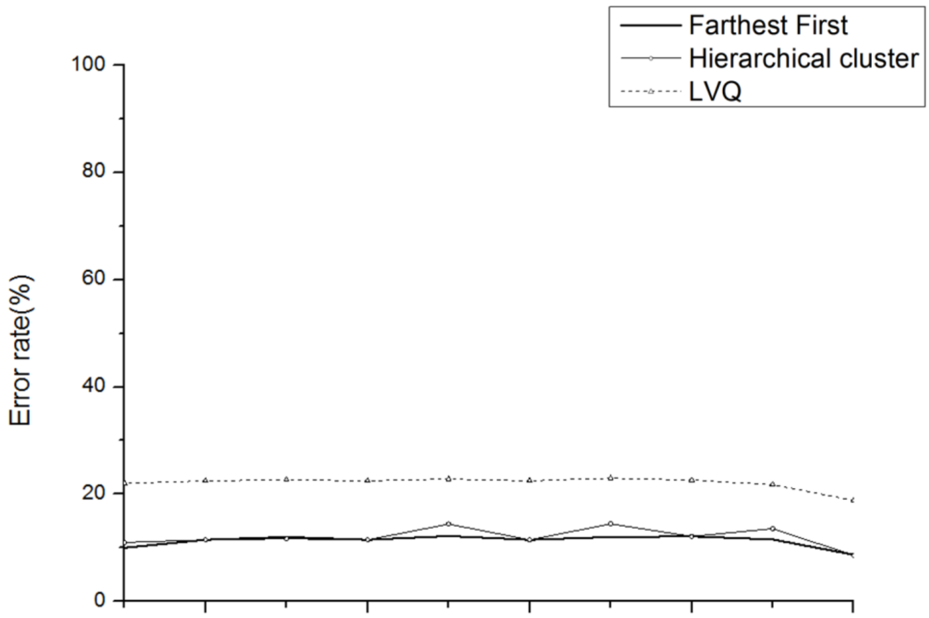

Figure 8. Error rate for AI algorithms.

When the number of datasets was 100, the false positive was 10%. When the number of datasets was 1000, the false positive was 8%. As the number of datasets increased, the detection error decreased. The average detection error rates for each algorithm were as follows: For the Farthest First algorithm, it was 11.3%, 12.0% for the Hierarchical cluster algorithm, and 22.1% for the LVQ algorithm. We discovered that the detection rate of the Farthest First algorithm was 0.7% better than the Hierarchical cluster algorithm, and 10.8% better than the LVQ algorithm. The resource requirements for operating each algorithm were as follows.

 doi:10.20944/preprints201802.0132.v1

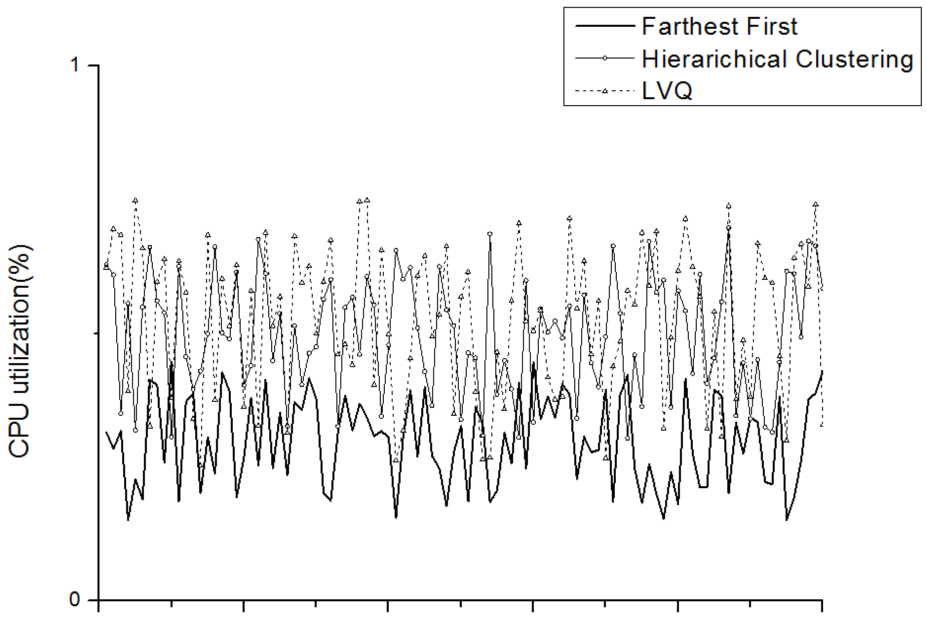

Figure 9. CPU utilization for AI algorithms

All algorithms consumed 1% or less of the CPU resources during operation, respectively. The CPU utilization used for each algorithm was 0.30% for the Farthest First algorithm, 0.49% for the Hierarchical cluster algorithm, and 0.52% for the LVQ algorithm. In other words, the Farthest First algorithm consumed 0.19% less than the Hierarchical cluster algorithm, and 0.22% less system resources than the LVQ algorithm. Therefore, the Farthest First algorithm had a higher DDoS attack detection rate than the Hierarchical algorithm and the LVQ algorithm, and consumed less system resources.

5. Conclusion

Since NFV is employed by organizations in order to reduce management costs, and to manage network environments efficiently, research on NFV is being undertaken. Despite the popularity of NFV, there is still a lack of research on the security threats between VNFs.

In this paper, we proposed an LW_PKI for VNF authentication and as a security mechanism to guarantee a secure NFV environment. The LW_PKI is a PKI for virtual environments that performs certificate-based mutual authentication and prevents data leakages by using security keys. We compared the performances of various AI algorithms detecting abnormal behavior of contaminated VNFs in NFV. When the LW_PKI was enabled in a virtual environment, it took 0.31 seconds longer to operate than in a physical environment. Therefore, the LW_PKI is an efficient secure mechanism in a virtual environment, and authentication can be performed without overhead affecting system performance. In addition, we confirmed that DDoS attacks can be detected by executing the Farthest First algorithm in a virtual environment. The proposals for the mutual authentication between entities and encryption of communication can be used to verify the stability of the cloud environment, and improve energy efficiency.

Acknowledgments: This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT)(R0190-17-2009,Development of endpoint protection technology using white list and context-aware).

Author Contributions: Sangho Park conceived and designed the research, performed the system simulations and wrote the paper, Hyunjin Kim analyzed the data and improved the system simulations; and Jaehyung Park made suggestions for this research. Jaecheol Ryou supervised the paperwork, review, comments, and assessment. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. ETSI Std. DGS/NFV-MAN001 Network Functions Virtualisation (NFV); Management and Orchestration, The European Telecommunications Standards Institute (ETSI), Sophia Antipolis, Valbonne, France, 2014
2. D.R. Lopez. Network functions virtualization: Beyond carrier-grade clouds. *Optical Fiber Communications Conference and Exhibition (OFC)* **2014**, DOI 10.1109/OFC.2014.6887145.
3. Sin-seok Seo; Young J. Won; James Won-Ki Hong. Witnessing Distributed Denial-of-Service traffic from an attacker's network. *Network and Service Management(CNSM) 2011*, France; pp. 241-247, ISBN 978-1-4577-1588-4.
4. Sanjeet Kumar Nayak; Sujata Mohanty; Banshidhar Majhi. CLB-ECC: Certificateless Blind Signature Using ECC. *Journal of Information Processing Systems(JIPS)* **2017**, Volume 13, pp. 392-397, DOI 10.3745/JIPS.03.0029.
5. R. L. Rivest; A. Shamir; L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM 1978*, Volume 21, No. 2, pp. 120–126, DOI 10.1145/359340.359342.
6. Mihir Bellare; Anand Desai; David Pointcheval; Phillip Rogaway. *Lecture Notes in Computer Science*, CRYPTO: Annual International Cryptology Conference, USA, 1998; Volume 1462, pp. 26-45, ISBN 978-3-540-64892-5.
7. Ki-Woong Park; Jaesun Han; JaeWoong Chun; Kyu Ho Park. THEMIS: A mutually Verifiable Billing System for the Cloud Computing Environment. *IEEE Transactions on Services Computing* **2013**, Volume 6, Issue 3, pp. 300-313, DOI 10.1109/TSC.2012.1.
8. Saket Acharya; Namita Tiwari. Survey Of DDoS Attacks Based On TCP/IP Protocol Vulnerabilities. *IOSR Journal of Computer Engineering (IOSR-JCE)* **2016**, Volume 18, Issue 3, pp. 68-76, DOI 10.9790/0661-1803046876.
9. Won Min Kang; Seo Yeon Moon; Jong Hyuk Park. An enhanced security framework for home applicances in smart home. *Human-centric Computing and Information Sciences(HCIS)* **2017**, 7:6, DOI 10.1186/s13673-017-0087-4.
10. Resul Das; Abubakar Karabade; Gurkan Tuna. Common network attack types and defense mechanisms. *Signal Processing and Communications Applications Conference (SIU)*, Turkey, 2015; pp. 658-661, ISBN 978-1-4673-7386-9.
11. Neha Gupta; Ankur Jain; Pranav Saini; Vaibhav Gupta. DDoS attack algorithm using ICMP flood. Computing for Sustainable Global Development(INDIACom), India, 2016; pp. 4082-4084, ISBN 978-1-4673-9417-8.
12. Wei Chen; Dit-Yan Yeung. Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing. *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, USA, 2006; ISBN 0-7695-2552-0.
13. Jelena Mirkovic; Peter Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review **2004**, Volume 34, Issue 2, pp. 39-53, DOI 10.1145/997150.997156.
14. Nathan Keegan; Soo-Yeon Ji; Aastha Chaudhary; Claude Concolate; Byunggu Yu. A survey of cloud-based network intrusion detection analysis. *Human-centric Computing and Information Sciences* **2016**, 6:19, DOI 10.1186/s13673-016-0076-z.
15. U. Maulik; S. Bandyopadhyay. Performance evaluation of some clustering algorithms and validity indices. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **2002**, Volume 24, Issue 12, pp.1650-1654, DOI 10.1109/TPAMI.2002.1114856.
16. Sharmila; Mukesh Kumar. An optimized farthest first clustering algorithm. *Nirma University International Conference on Engineering (NUiCONE)*, India, 2013; ISBN 978-1-4799-0725-0.
17. Seema Bandyopadhyay; E. J. Coyle. An energy efficient hierarchical clustering algorithm for wireless sensor networks. *INFOCOM* **2003**, Volume 3, pp.1713-1723, DOI 10.1109/INFOCOM.2003.1209194.
18. R. Inokuchi; S. Miyamoto. LVQ clustering and SOM using a kernel function. *International Conference on Fuzzy System*, Hungary, 2004; Volume 3, pp.1497-1500, ISBN 0-7803-8353-2.