Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

The Security Threats and Solutions of Network Functions Virtualization: A Review

Alaa Noori Mazher [a], *Jumana Waleed* [b] *and Abeer Tariq MaoLood* [c]

[a] *Department of Computer Science, University of Technology, Baghdad-Iraq, Email : 110027@uotechnology.edu.iq*

[b] *Department of Computer Science, College of Science, University of Diyala, Diyala -Iraq, Email: jumanawaleed@sciences.uodiyala.edu.iq*

[c] *Department of Computer Science, University of Technology, Baghdad-Iraq, Email: 110032@uotechnology.edu.iq*

ARTICLE INFO

Article history:
Received: 06/12/2020
Rrevised form: 15/12/2020
Accepted :24 /12/2020
Available online: 25 /12/2020

Keywords:

Network Functions Virtualization (NFV); security threats; virtual machines (VMs).

ABSTRACT

The appearance of Network Functions Virtualization (NFV) has provided a revolution in various network-based applications owing to its different advantages like manageability, flexibility, security, and scalability. The users of NFV are provided with a framework that supplies different flexible network services in a dynamic way via the software-based virtualization of network functions in a single infrastructure. Nevertheless, NFV confront various challenges of security which make it vulnerable to several cybersecurity threats. In this paper, a review of NFV has been provided by introducing many related works, discussing serious and potential security attacks on the NFV, and presenting the efficient countermeasures for mitigating these attacks. Finally, several practical solutions are suggested for providing a reliable platform for NFV

MSC : 30C45 , 30C50

DOI : https://doi.org/10.29304/jqcm.2020.12.4.720

1. Introduction

Generally, in order to deploy a new platform or network service, it is essential to include a diversity of hardware appliances that work on increasing the cost of purchasing new resources and employing new engineers for managing these network resources. Nevertheless, the technology over quick changes has caused a shorter product life cycle in the industry of network. Network Functions Virtualization (NFV) is an essential technology to avoid fundamental alterations in the actual physical components of network systems via supplying network functions by implementing pure software instead of hardware resources. Within the environment of virtualization, it is possible to emulate the hardware, and multi-virtual functions

Corresponding author : *Jumana Waleed*

Email address: *jumanawaleed@sciences.uodiyala.edu.iq*

Communicated by : *Alaa Hussein Hamadi*

are capable of sharing the available resources and nning concurrently on infrastructure via virtualization [1].

Recently, NFV has appeared as one of the main leading forces technologies that substantially speed up the nowadays development of computer and communication networks [2]. Although the NFV has many advantages such as; optimizing the consumption of resources, saving the cost of investment, increasing operational efficiency, and facilitating the lifecycle management of network service, several vulnerabilities and security threats will be presented, thus inhibiting their expansion and utilization in practice. In this subject review, the main threats on NFV have been analyzed, and the corresponding security necessities have been identified.

2. NFV Framework and Major Components

According to the framework presented via the European Telecommunications Standards Institute (ETSI), NFV is constructed of four essential components; The first component is NFV Infrastructure (NFVI) which indicates all the software and hardware resources that provide the environment of virtualization on the deployed Virtual Network Functions (VNFs) [3]. As an instance, physical computing, networking, and storage can be virtualized so as to be shared among various network functions. The second component indicates VNFs / Element Management System (EMS), where VNFs represent a set of network functions which are executed in software (for example, firewall, deep packet inspection, balancing the load) for running on a virtualized environment, besides a set of EMSs which implement configurations and fundamental management functions to one or many VNFs. The third component indicates NFV Management and Orchestration (MANO). This component works on managing and orchestrating the whole resources in the environment of NFV, involving computing, networking, and storage. The final component indicates the Operating Support System/Business Support System (OSS/BSS). These are performed via the providers of VNF service for meeting various business objectives like the billing process [4].

Because the software and hardware of NFV are mostly expanded via various vendors, the concept of interoperability is still representing an essential challenge for deploying the services of NFV. For instance, it is possible to effectively implement MANO, only when VNFs and the appliances of the network are accessible and manageable via standard interfaces that conceal as much as possible of heterogeneity in physical resources. For providing standard and open interfaces to the physical resources, Figure 1 illustrates the proposition of ETSI NFV for the

architectural framework of NFV involving the essential functional blocks and the points of reference. The infrastructure of NFV involves a virtualization layer. The virtualization layer works on logically partitioning physical resources and providing a fulcrum between VNF and the underlying layer of virtualized infrastructure. The fundamental tools for implementing this layer are called hypervisors. These tools provide a host with an environment of virtualization which is functionally similar to the environment of the original machine. In practice, the hypervisor works on monitoring the operations of virtual machines (VMs) and managing access to resources, as well as providing failure recovery for the needed Quality of Serves (QoS). In the security view, hypervisors must supply a separated space to serve VMs and the mechanisms of right access control for preventing unauthorized access to the shared resources among VMs. Nevertheless, practically, it is not plain for securing isolation between them [5].

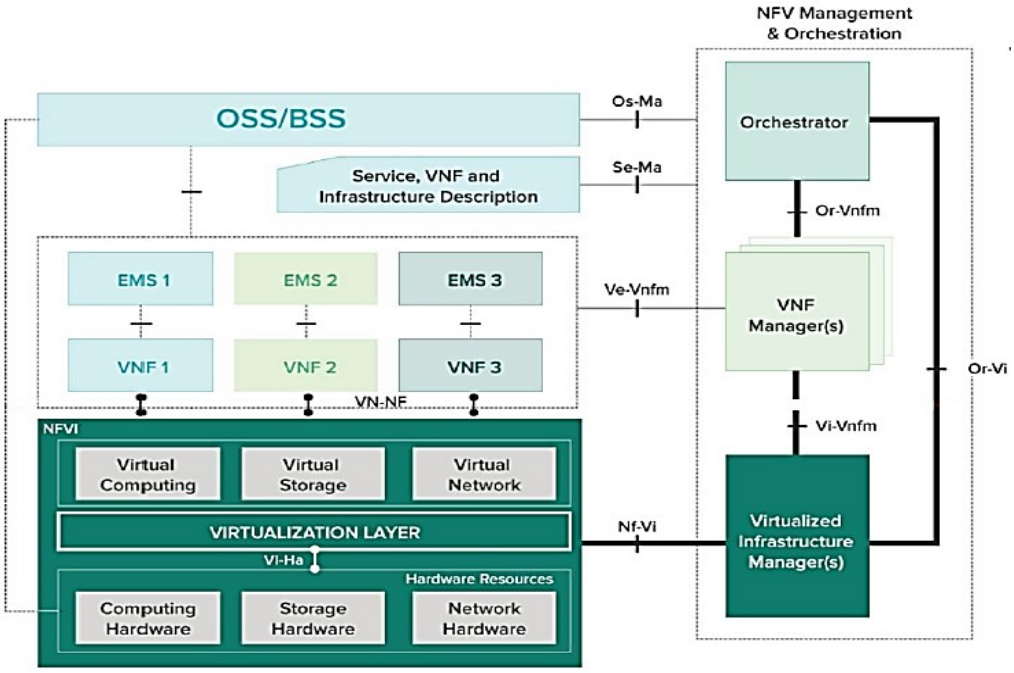

Figure 1. The proposition of ETSI NFV for the architectural framework of NFV involving the essential functional blocks and the points of reference [5].

3. NFV Security Threats and Solutions

In theoretic, NFV represents a typical solution to deploy new network services and equipment since network functions can be updated dynamically using the downloads of software rather than substituting physical hardware. But, several issues of robustness and security still require to be handled for completely attaining the interest of utilizing NFV. In practice, the main

security challenges that should be addressed: firstly, Network function-specific threats, and secondly, Generic virtualization threats, as illustrated in Figure 2 [6].

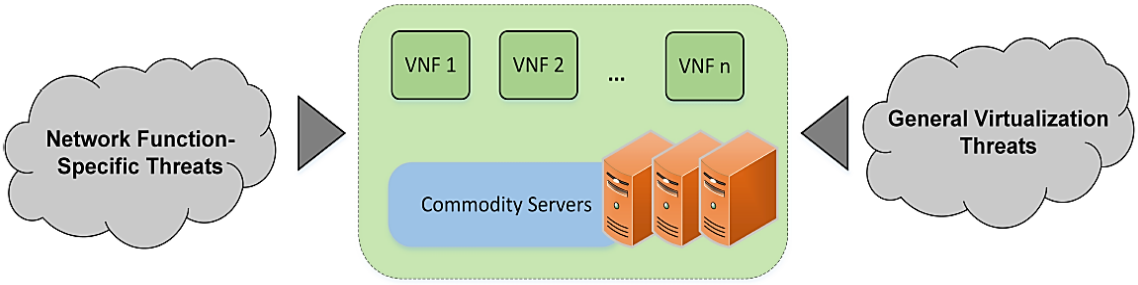

Figure 2. NFV challenges [6].

Network function-specific attacks indicate the threats on network functions/resources, for example, denial of service (DoS), sniffing, and spoofing. Not surprisingly, these kinds of attacks are concerned with the abilities of attackers and the targeted topology of the network.

The NFV foundation is firmed on network virtualization. In this environment of NFV, multiple VNFs can logically share a single physical infrastructure. In these VNFs, offering a hosted and shared network infrastructure presents new vulnerabilities of security. As shown in Figure 3, the generic network virtualization platform includes several elements; the network infrastructure providers, the providers of VNF, and users. Because the system includes various operators, certainly, the cooperation of these operators can be imperfect and every element may conduct in a greedy or uncooperative manner for gaining benefits. The NFV virtualization attacks can be originated from each element and may target part or all of the system [5].

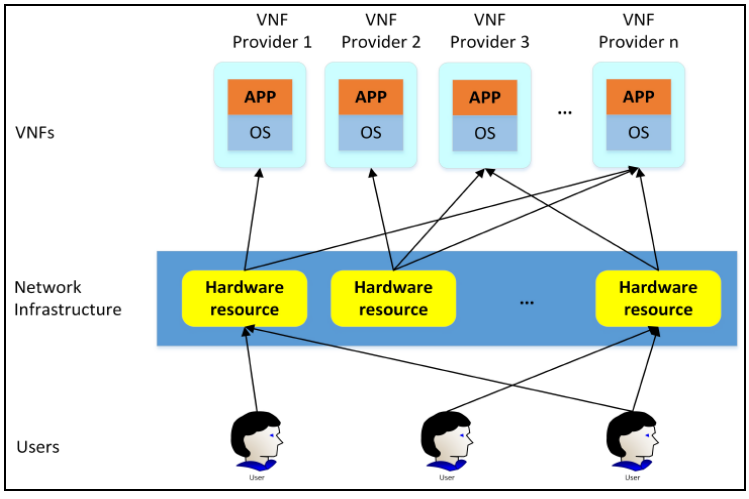

Figure 3. Participating entities in virtualization threats [5].

3.1. Infrastructure-targeted attacks

There are several infrastructure-targeted attacks [7], as summarized in Table 1:

1. Operational interference: Owing to the concerted infrastructure accessibility, a compromised provider or a malicious user of VNF can interfere with the infrastructure operations via changing network traffic or inserting malware.
2. The chance of cooperating with malicious providers: Through access to the network infrastructure resources, the providers of VNF are capable of taking participation in the operations of the network, for a good example Network-as-a-Service (NaaS), which the providers of VNF utilize for supporting the decisions of customized forwarding depends on every application's requirements in cloud computing. Though this model possibly offers effective services in-network like stream processing, data aggregation, protocols of redundancy elimination, and caching, it allows the providers of VNF to carry out subversive activities against the network infrastructure or their competitors. The hypervisor is capable of preventing this issue to happen via detecting the excessive consumption of resource by a virtual network.
3. Misuse of shared resources: The abuse of the infrastructure shared resources, in such a way that the victim cannot benefit from the dedicated or shared resources, is the principle of these threats. To find solutions to these attacks, devoted instances for users can be created and malicious demands regarding IP addresses blacklist can be verified.

3.2. VNF- targeted attacks

There are several VNF- targeted attacks [8]:

1- Outsourcing challenges: NFV permits outsourcing the core software and computing abilities for the network's third-parties. A considerable issue of security in NFV maybe rise via releasing the cloud resources and transmitting the workload to an off-device network for managing the possible workload.

2- Logical isolation: It works on improving the manageability and control of a shared infrastructure system. This isolation can be implemented at various levels as in the SDN virtualization system. In the modern virtualization systems, it is not sufficient to rely only upon the conventional mechanisms of access and control (for example, programming isolated slices or virtual LAN) for performing logical isolation of VMs. Therefore, depending on this insufficiency, several attacks of cross virtual network side-channel can

threaten co-hosted VNFs in the shared infrastructure. Practically, as the attack of a side-channel, the attack of a covert channel evades mandatory auditing and access controls for violating resource isolation. For reducing the opportunity of side-channel threats, several arrangements are necessary, like the utilization of secure database interfaces, the concealment of access management, the obfuscation of service structures, and the dedication of resource instances. The technologies of virtualization depend on a trusted platform module (TPM) that provide the conditions of protection against the attacks of side-channel.

3- VM Live migration: It is considered a significant feature of virtualization since it works on relocating VMs with no interruption in NFV services. The usefulness of migration is considerably obvious in the system management and balancing of workload. But, it might be vulnerable to some threats, like Man-in-the-Middle attack has risen via traffic sniffing, DDoS flooding attack when the protection for the migration is un-carefully designed, and a replay attack. Usually, the migration of VM is implemented via copying its pages of memory from the source to the destination hypervisors whilst a VM is running within the source hypervisor. The initialization of unauthorized migration to the network of the attacker, which results in taking control of a victim's VM, or the initialization of migration to a considerable number of VMs to a victim's network for breaking down, represents the potential results of these attacks. There are several protection solutions which rely on the methods of cryptography, for preparing a secure environment for live migration. Under this consideration, the virtual trusted platform module is capable of using the protocol of TLS for providing authentication and confidentiality. Substantially, these solutions result in a computational overhead of cryptography which is undesirable for having an agile NFV. To prevent this overhead, several solutions are available for safe migration, such as live migration defense framework or Intel's trusted execution technology defines un-cryptographic techniques. In spite of bypassing the overhead, the presented solutions still have their own restrictions.

3.3. User- target attacks

There are several User- target attacks [8]:

1- Confidentiality and privacy of user: A user is a network end-point which represents the most convenient target to other NFV malicious elements. The traffic of the user is

subjected to a VNF provider monitoring and sniffing for a suitable quality of service (QoS). Providing services of virtualized networks, like intrusion detection, firewall, detection of DDoS, etc. allow the providers of services a full dominance on the information of the user. It is leading to a new relationship of confidence in such a way that users should trust their providers of VNF regarding users' data privacy and computations integrity. On another side, the users' confidentiality and privacy are open to the provider of network infrastructure. For controlling the network access and congestion, the traffic of the network is subjected to the monitoring of the infrastructure provider. For examples related to this vulnerability, annoying peer-to-peer connections, and sniffing protocol headers in the excuse of traffic forming. Additionally, the infrastructure can introduce non-evident attacks to other users owing to the subtlety of how physical resources are capable of transparently sharing among VMs.

2- Malicious cases: The NFV user may be attacked with attacks originated via malicious users who use the VNFs flaws or the infrastructure. For example, as a malware injection attack on a cloud, on Amazon EC2 public IaaS Cloud, a malicious user via modifying the image permission (Amazon Machine Image) of its VM are capable of making this malicious image be public in the cloud. This image is becoming visible to other users, therefore, they can launch the instance of VM depend on the malicious image, which creates several attacks like the victims' information leakage. As a result, for providing a secure environment to the users, it is significant to the infrastructure for detecting and preventing all malicious cases. In order to achieve this requirement, the attacker should be incapable of determining where within infrastructure, an instance is located or co-located with its own instance.

Table 1 The Summarization of the main security attacks and counterattacks facing the NFV.

Security attacks	Counterattacks
Outsourcing of task: Eavesdropping, injection of Malwares, Confidentiality compromising, and Functional violation	Secure services of outsourcing, validation of integrity, Over-encryption connection
Multiple tenancies: Side channel threats among co-hosted VNFs	secure database interfaces, the concealment of access management, the obfuscation of service structures, and the dedication of resource instances
VM Live migration: Man-in-the-Middle attack has risen via traffic sniffing, DDoS flooding attack when the protection for the migration is un-carefully designed, and a replay attack	The authentication of source and destination, The detection of malicious activity, Authorized access to the interface.

Compromise provider of infrastructure: Interfering the hosted VNF function, Privilege information threat, and operation violation	Mechanism of monitoring for detecting abnormal behavior, Techniques of traffic validation
Compromise provider of infrastructure and VNF provider: The violation of confidentiality and privacy	The management of trust for ensuring the provision of information integrity
Malicious user: The violation of service, and the leakage of information	Concealing co-serving instance, and the techniques of cryptographic

4. The Presented Efforts for Finding Security Solutions

Security represents a significant issue in NFV environments, however, the architecture ETSI NFV didn't include much about security. Therefore, there are several efforts have been presents by different researchers for finding suitable solutions for common security attacks on NFV.

Basically, NFV permits VNFs to be outsourced via a third party since it works on separating the functions of network from their locations. The outsourcing of VNF puts up considerable challenges for network service chains that represents a significant technology for realizing NFV. H. Jeon and B. Lee [6], discussed the network service chains challenges under the consideration of VNF outsourcing. The detected technical challenges are presented in maintaining multi-subdivided network service chains for each flow of traffic, managing the dependency between these service chains, identifying an outgoing point per service chain, and establishing the data plane among domains supplying network service chains implement to the same flow of traffic.

H. Jang et al. [9], presented the activities that lots of Internet service providers and security vendors are working to specify general interfaces for NFV security services via analyzing the utilized cases and relevant techniques.

P. Patel et al. [10] described NFV, SDN, and the integration of these technologies in Openstack cloud for minimizing the surface of network attacks, and improving network service, as well as providing the salient SDN advantages. In cloud computing, the integration of NFV and SDN gives strength of virtualization and enhance the network service and security.

Y. Liu et al. [11], discussed the conventional manner for implementing service chain, and worked on finding a suitable manner to supply security service chain. In this work, an architecture based on ETSI NFV integrated with SDN has been proposed for implementing security service chain.

M. Pattaranantakul et al. [12], proposed a security-oriented MANO framework which addresses the main requirements to have built in mechanisms of security for NFV based platforms and infrastructure, at the same time, dynamically manages the whole lifecycle of different security functions in NFV context. This proposed architecture includes two fundamental concepts. The first one is the engagement of a security trust model and the validation of security features of services and resources (secure by design). The first second one is providing a set of security functions (security as a service), fo example, IDS/IPS, protection of data, identity and access management, network isolation, that can be utilized for preventing massive threats.

W. Yang and C. Fung [13], presented a theoretical background about NFV and highlighted the main issues of security, and briefly described the security challenges of NFV, and provided solutions for addressing these security issues.

A. Kalliola et al. [14], presented a security orchestration testbed in the environment of NFV. Within a certain scenario, this testbed implementation works on mitigating the DDoS and different types of targeted attacks Through implementing the defense in OpenStack with SDN enabled network environment and showing its efficiency with various kinds of attack traffic. Also, L. Zhou and H. Guo [15], presented a framework for DDoS attack mitigation. This framework includes three levels; application, control, and data levels. In the first level, the module of abnormality detection is in charge of collecting and analyzing data and triggering suitable mitigation mechanisms of DDoS attacks from the application level. The module of NFV works on virtualizing, allocating, instantiating, and managing VMs for the specific mitigation needs of DDoS attacks. The module of SDN with the controller of SDN works on implementing and enabling the allocated physical or virtual resources.

I. P. Bolodurina et al. [16], developed a model based on genetic algorithm and neural network to form an optimized list of rules for providing network security. This developed model was implemented as a firewall, implemented as a VNF for SDN.

A. K. Alnaim et al. [17], utilized an architectural model for analyzing several potential attacks in the VM Environment of NFV using misuse patterns. These misuse patterns cannot be validated in practice since there are no incidents of attack known, therefore, their validation is dependent on logical arguments.

A. M. Alwakeel et al. [18], analyzed several NFV use cases for enumerating their attacks and analyzing their activities of misuse. The obtained results of the analysis improve NFV security and suggest some security policies to enhance system security. Moreover, based on the analysis we can find misuse patterns that provide possible countermeasures to stop them.

Uxia Cheng et al. [19], proposed an effective and intelligent multivariate Hidden Markov Model-based abnormality detection system for protecting online VNF services in the cloud. This model is presented for profiling the normal VNF behavior patterns. The utilization of the VNF behavior model trained with normal sequences of observation enables the system to effectively detect abnormal behaviors online. Two kinds of VNF models, virtual firewall and virtual router are trained utilizing real network traffics in the valuation process.

Uxia Cheng et al. [20], modeled co-residency and cross-level attacks in the stack of NFV and formulated the optimal placement issue of VNF/VM for mitigating the security threats via a standard algorithm of optimization. The obtained simulation results illustrate that the solutions could decrease the security threat level in NFV.

Table 2 Summarizes the main NFV security challenges and the provided security solutions presented by recently existing researches.

Table 2. Comparison of several researchers' efforts in finding NFV security solutions.

Authors Name, Ref. No., Year	Security Challenges	The Provided Security Solution
H. Jeon and B. Lee, [6], 2015	Discussing the network service chains challenges under the consideration of VNF outsourcing	Maintaining multi-subdivided network service chains for each flow of traffic, managing the dependency between these service chains, identifying an outgoing point per service chain, and establishing the data plane among domains supplying network service chains.
H. Jang et al., [9], 2015	Specifying common interfaces for NFV security services	The standardization of interfaces to the functions of network security.
P. Patel et al., [10], 2016	Minimizing the surface of network attacks, and improving network service	The integration of NFV and SDN gives strength of virtualization and enhance the network service and security.
Y. Liu et al., [11], 2016	Finding a suitable manner to supply security service chain	The integration of NFV and SDN provides an efficient security service chain.
M. Pattaranantakul et al., [12], 2016	Handling the requirements to have built in mechanisms of security for NFV based platforms and infrastructure, and managing the whole lifecycle of different security functions in the NFV context.	Secure by design, and security as a service.
W. Yang and C. Fung, [13], 2016	- The domain of hypervisor: data leakage, and unauthorized access. - The domain of computing: shared computing resources. - The domain of Network: shared the virtual switches, and shared physical network interface controllers.	- VMs are only available for authentication controls. - Data can be accessed and encrypted only via the VNFs. - The techniques of secure networking must be adopted.
A. Kalliola et al., [14], 2017	Finding an intelligent response to mitigate DDoS and targeted attack.	Implementing the defense in OpenStack with SDN enabled network environment
L. Zhou and H. Guo, [15], 2017	Mitigating DDoS attack.	Employing the technology of NFV/SDN and applying it to defend the systems of critical industry against DDoS.
I. P. Bolodurina et al., [16], 2018	Providing security in the corporate network.	Developing a model based on genetic algorithm and neural network to form an optimized list of rules for providing security.
A. K. Alnaim et al., [17], 2019	Analyzing several potential attacks in the VM Environment of NFV.	Using misuse patterns depend on logical arguments.
A. M. Alwakeel et al., [18], 2019	Enhancing the NFV security	Depend on analyzing several NFV use cases for enumerating their attacks and analyzing their activities of misuse, several potential countermeasures are provided.
Uxia Cheng et al., [19], 2019	Detecting abnormality behavior in the environment of NFV cloud.	Utilizing the Hidden Markov Model for protecting online VNF services.
Alhebaishi N. et al., [20], 2020	Mitigating and modeling NFV security threats (co-residency and cross-layer attacks).	The mitigation was accomplished for these attacks by optimizing the placement of VM regarding the specified limitations. The obtained simulations results show the efficiency of the solutions.

5. Conclusions

As a new technology, NFV has considerable abilities and can supply several advantages for the providers of telecommunication service via decreasing the setting up a network cost, enhancing it, and dynamically deploying several services for users. But, the NFV technology must be secured from outsider and insider threats, tacking in the consideration that this service holds its own infrastructure with various elements that require to be analyzed seriously for understanding potential attacks and vulnerabilities. NFV provides cost-effective and agile deployment of various services of network for multi-tenants at the same physical infrastructure. Since it depends on virtualization, and since it's stack generally includes various abstraction levels and multi-tenants, this technology inevitably is leading to various security attacks. In this paper, a review of several security threats that faces the NFV has been presented. Additionally, many countermeasures for prevalent threats could alleviate the severity of NFV attacks. However, NFV security remains a field under consideration with different security challenges that require to be studied. Furthermore, recently, NFV is lacking the experimental implementation for understanding its weak points and disadvantages. Finally, NFV has unlimited abilities and represents the networking future. Through integrating several features of security, NFV will provide a secure future of networking as well.

References

[1] ETSI. Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance. Technical report, ETSI GS NFV-SEC 003 V1.1.1, (2014).

[2] A. Aljuhani and T. Alharbi, "Virtualized Network Functions security attacks and vulnerabilities," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, (2017), 1-4.

[3] X. Wu et al., "State of the Art and Research Challenges in the Security Technologies of Network Function Virtualization," in IEEE Internet Computing, vol. 24, no. 1, (2020), 25-35.

[4] Zonghua Zhang, Ahmed Meddahi, Chapter1 - NFV Management and Orchestration, Security in Network Functions Virtualization, Elsevier, (2017), 1-43.

[5] M. De Benedictis and A. Lioy, "A proposal for trust monitoring in a Network Functions Virtualisation Infrastructure," 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, (2019), 1-9.

[6] H. Jeon and B. Lee, "Network service chaining challenges for VNF outsourcing in network function virtualization," 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, (2015), 819-821.

[7] Yan Luo, Eric Murray Timothy, L. Ficarra, "Accelerated Virtual Switching with Programmable NICs for Scalable Data Center Networking". The Second ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures, (2010), 65-72.

[8] Saeed Shafieian, Mohammad Zulkernine, Anwar Haque, "Attacks in Public Clouds: Can They Hinder the Rise of the Cloud", Cloud Computing: Challenges, Limitations and R & D Solutions, Springer, (2014), 3–22.

[9] H. Jang, J. Jeong, H. Kim and J. Park, "A Survey on Interfaces to Network Security Functions in Network Virtualization," 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, (2015), 160-163.

[10] P. Patel, V. Tiwari and M. K. Abhishek, "SDN and NFV integration in openstack cloud to improve network services and security," 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, (2016), 655-660.

[11] Y. Liu, Z. Guo, G. Shou and Y. Hu, "To Achieve a Security Service Chain by Integration of NFV and SDN," 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, (2016), 974-977.

[12] M. Pattaranantakul, R. He, A. Meddahi and Z. Zhang, "SecMANO: Towards Network Functions Virtualization (NFV) Based Security MANagement and Orchestration," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, (2016), 598-605.

[13] W. Yang and C. Fung, "A survey on security in network functions virtualization," 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, (2016), 15-19.

[14] A. Kalliola, S. Lal, K. Ahola, I. Oliver, Y. Miche and S. Holtmanns, "Testbed for security orchestration in a network function virtualization environment," 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, (2017), 1-4.

[15] L. Zhou and H. Guo, "Applying NFV/SDN in mitigating DDoS attacks," TENCON 2017 - 2017 IEEE Region 10 Conference, Penang, (2017), 2061-2066.

[16] I. P. Bolodurina, D. I. Parfenov, V. A. Torchin, L. V. Legashev and V. M. Shardakov, "Development of Prototype of Autonomous Self-organizing System for Ensuring Network

Security in Enterprise based on Technology of Virtualization Network Functions," 2018 Global Smart Industry Conference, Chelyabinsk, (2018), 1-8.

[17] A. K. Alnaim, A. M. Alwakeel and E. B. Fernandez, "Threats Against the Virtual Machine Environment of NFV," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, (2019), 1-5.

[18] A. M. Alwakeel, A. K. Alnaim and E. B. Fernandez, "Analysis of threats and countermeasures in NFV use cases," 2019 IEEE International Systems Conference (SysCon), Orlando, FL, USA, (2019), 1-6.

[19] Uxia Cheng, Huijuan Yao, Yu Wang, Yang Xiang, Hongpei Li, Protecting VNF services with smart online behavior anomaly detection method, Future Generation Computer Systems, Volume 95, (2019), 265-276.

[20] Alhebaishi N., Wang L., Jajodia S., "Modeling and Mitigating Security Threats in Network Functions Virtualization (NFV)", Data and Applications Security and Privacy XXXIV, DBSec 2020, Lecture Notes in Computer Science, vol. 12122, Springer, Cham, (2020).