Security and Privacy Issues in Network Function Virtualization: A Review from Architectural Perspective

Bilal Zahran[1], Naveed Ahmed[2], Abdel Rahman Alzoubaidi[3], Md Asri Ngadi[4]
Engineering and AI Dept., Al Balqa Applied University, Jordan[1]
Faculty of Engineering, University Teknologi Malaysia, Malaysia[2, 4]
Electrical Engineering Dept., Al Balqa Applied University, Jordan[3]

***Abstract*—Network Function Virtualization (NFV) delivers numerous benefits to customers since it is a cost-effective evolution of legacy networks, allowing for rapid network augmentation and extension at a low cost as network functions are virtualized. However, on the other hand, there is a big security concern for NFV users because of shared infrastructure. There are many studies in the literature that report various NFV security threats. In this paper, we categorize these threats according to the alignment of NFV architecture and delineate a taxonomy for NFV security threats. This work provides detailed information about security threats, causes, and countermeasures to reduce the security vulnerabilities of NFV. We believe that the study of NFV security threats from an architectural perspective is a step forward for better insight into these threats since the roots of many NFV threats are connected to their architecture. We also present how NFV design should be revamped to mitigate NFV security threats, something that is a recent trend in this area. Finally, we highlight future research directions to provide enhanced security for future NFV-based networks.**

Keywords*—Network functions virtualization; virtualized network function; network security, security threat; cloud computing

I. INTRODUCTION

In general, it is important to provide a variety of hardware equipment when deploying a new network service, since this increases the expense of buying new resources and hiring new engineers to manage these network resources. Nonetheless, in the network sector, technology's rapid advances have resulted in a shorter product life cycle. Network Functions Virtualization (NFV) is a new trend for avoiding significant changes to network systems hardware elements while providing network functions with pure software rather than hardware tools. It is possible to replicate hardware inside the virtualization setting, and multi-virtual functions are prepared to share available resources and running simultaneously on infrastructure through virtualization [1-5].

NFV is expected to provide the several benefits by implementation networks functions in software. 1) Independence: since network functions are decoupled from hardware, as a result, their evolution will be self-contained. 2) Flexibility: It is possible to reassign and share the same infrastructure resources, enabling different network functions at different times depending on the customer's demand. 3) Scalability: finer granularity of resources in software leads to better scalability. 4) Lower energy consumption: since resource provisioning can be scaled up and down in NFV, telecommunication service providers will be able to lower the OPEX required to run network devices, which could be as much as 10% of current power consumption [1].

Although NFV has several benefits, it faces many internal and external security risks, which indeed limit its extension and use in application. In NFV, multiple network functions which may belong to different customers are sharing the same virtualized computer system, in this scenario, if a part of virtualized system is compromised it can affect the entire system since all network functions are co-located. Securing NFV demands rigorous security review as well as the use of security methods to counter the dangers. In this paper [2], we examine the security risks associated with NFV technology and how the technology's unique properties pose additional security risks. Then we present the counter measures which can be taken to address these security challenges.

There are many survey studies in the literature which highlight several security threats and mitigation strategies related to NFV security [3]. However, in our work, we have discussed security concerns of NFV from its architectural perspective. To the best of our knowledge, no one investigated NFV security concerns in this way. We believe that architectural perspective is useful for better understanding and categorization of the security loop-holes. For instance, we have discussed several security threats with respect to hypervisor, shared memory, virtual switch etc. which are important architectural component of an NFV framework. In this context, our contribution is highlighting the security threats as a reference to their source.

We aim to provide an organized and methodical review for analyzing and tackling security and privacy concerns in NFV by recognizing and utilizing patterns, which may act as a basis for creating efficient solutions. This usage of patterns is a way to improves practitioners' ability to design safe and privacy-preserving NFV installations while also enhancing awareness of security and privacy challenges in NFV.

The rest of this paper is organized as follows: Section II gives a background on virtualization and NFV framework. In this section, we discuss the architecture of NFV frame work. In Section III, we discuss NFV security threats and categorize them from architectural perspective. In this regard, a taxonomy is presented. In Section IV, we analyze the general causes of NFV security threats. In Section V, we suggest several NFV design recommendations as a countermeasure to NFV security threats. Section VI finally concludes the paper with some future work directions.

II. Virtualization and NFV Framework Overview

Network Virtualization is commonly mistaken for NFV. We aim to clarify the difference first and then introduce the NFV framework. In this regard we briefly describe the evolution from classic virtualization solutions to the state-of-the-art NFV framework. Virtualization is very well principle since it began in the 1960s when the Institute of Business Machines (IBM) developed an operating system (OS) called CP-40.

ESTI (European Telecommunications Standards Institute) has established NFV standards and proposed a framework. This framework is used here as a reference to study the potential NFV security risks and threats. The framework is shown in Fig. 1. It consists of three major components which are given below.

1) Network Function Virtualization Infrastructure (NFVI)

2) Virtualized Network Function (VNF)

3) Network Function Virtualization Management and Orchestration (NFV-MANO)

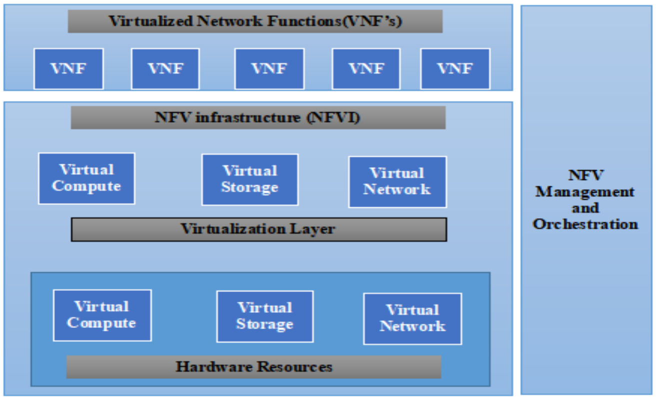

Fig. 1. NFV Frame.

A. Network Function Virtualization Infrastructure (NFVI)

NFVI is a form of a cloud data center that comprises both hardware and virtualization software, including servers, virtual machines and a network that creates the foundation for NFV framework. In this context, NFVI includes three key elements: virtualized services, the virtualization layer, and hardware resource.

B. Virtualized Network Function (VNF)

VNF is a network function (such as router, firewall, intrusion detection system etc.) which is completely implemented in software. VNFs may be joined-chained together in order to provide a network service; this is referred as service chaining.

C. NFV Management and Orchestration (NFV-MANO)

NFV-MANO consists of three key components; the first one is a virtualized infrastructure administrator that monitors and handles the VNF and NFVI interactions and computing and storing system resources; it is also capable of essential virtualization layer implementation monitoring.

D. Network Function Virtualization Security Threats

NFV is more prone to security threats as compared to traditional network systems. It is due to the fact that NFV supports a multi-tenancy environment and all physical resources are available for customers according to their requirements and service level agreements. It means that multiple VNFs which may belong to different customers are sharing the same physical infrastructure.

To better understating the security concerns of NFV architecture, we elaborate a scenario where a commodity computer system is virtualized to enable multiple parallel VNFs. The setup is shown in Fig. 2 with a hosting environment and a virtual environment. The hosting environment owns the physical resources (such as CPU, Memory, Network Interface Card) which are accessed by VNFs through the coordination of virtualization layer i.e., hypervisor. The ingress traffic stream towards the physical host may belong to different VNFs which is processed at virtual network switch to connect with appropriate VNF. Similarly, the egress traffic of VNFs access the physical NIC thorough virtual switch.

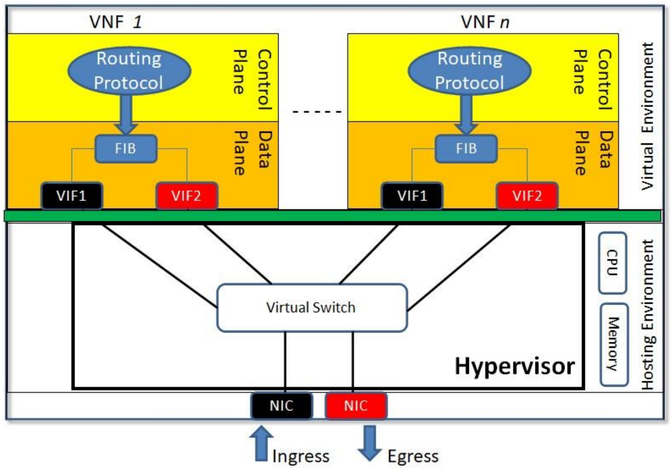

Fig. 2. A virtualized computer system with multiple VNFs.

In Fig. 2, it can be noticed there are several resources which are shared among VNFs.

Generally, these shared resources can be categorized into three types: Hypervisor, Compute and Network.

TABLE I. Various Challenges and their Solutions in Different Security Domains of NFV

Domain	Challenges	Solutions
Hypervisor	Data leakage and unauthorized access [9]	Virtual machine is authorized by SDN controller
Compute	Shared CPU and Memory [10]	VNFs should have protected data access
Network	Shared physical and logical networks [11]	SSH, TLS should be adopted

There is a vast literature with several network security threats which can target different components of NFV architecture. Therefore, first we categorize these threats in a systematic manner and then explain them one by one. In this regard, a taxonomy of NFV security threats is shown in Fig. 3 and Table I. There are different types of network threats (such as DoS attack, malware injection etc.) which are reported in NFV security related studies. In some cases, an attack is launched to target a specific component of NFV architecture which is shown at the second level of our taxonomy. The detailed description of these attacks is as follows:

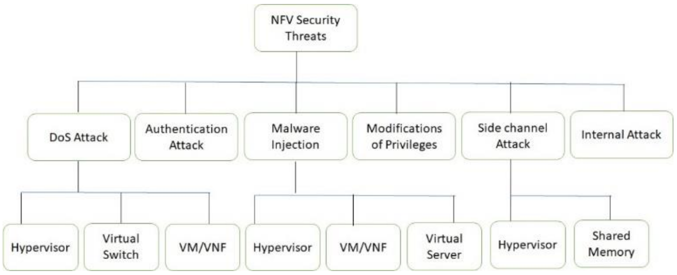

Fig. 3. Taxonomy of NFV security threats.

E. *Denial of Service Attack*

Denial of Service (DoS) or Distributed DoS (DDoS) attack overloads the network/system resources with meaningless traffic and causes service unavailability to legitimate customers. In 2013, 37% of the overall network attacks were DDoS attacks and grew to 65% in 2015, rendering them a major problem for network operators in the foreseeable future.

F. *Compromised Hypervisor*

In reality, the hypervisor takes good care of the interaction and separation of various entities that build the VNFs. However, we know from literature review that hypervisor security can be compromised due software bugs which are exploited by the intruders/hackers.

G. *Compromised Virtual Switch*

In NFV environment, a virtual switch (v Switch) is used to interconnect VNFs. It means that attacking the virtual switch may affect the numerous virtualized network functions that render them momentarily inaccessible to customers, impacting the whole device.

H. *Compromised VNF*

In this type of attack, a hacker gets control of a VNF/VM and use it to generate DDoS attack. The attacker VM generates heavy traffic to overload the system resources which results in resource scarcity for other VMs operating on the same physical host.

III. Authentication Attack

NFV allows the deployment, management, and delivery of virtualized network functions as a service. This process is known as NFV service computing process. When a hacker pretends to be a trustworthy service provider or other organization in order to obtain unauthorized access to the NFV service computing process, this is known as an authentication attack (see Table II).

A. *Malware Injection Attack*

In malware injection attack, a hacker modifies the original code of virtualized components by incorporating its own malicious code to harm the NFV setup. In literature, this attack is reported on different NFV components for which the details are given below:

B. *Compromised Hypervisor*

A hypervisor enables several virtual machines to interact and coordinate with one another, i.e., controlling the service virtualization layer of NFV framework [3]. Malware injection, which attempts to impact the virtualization layer of NFV's framework by modifying its internal code, is an instance of an assault that may change the GUI view of NFV, which means that updating the GUI depiction of the NFV infrastructure within the exploited hypervisor.

C. *Compromised Virtual Machines/VNFs*

Usually, getting VMs operating on a single server may also generate bugs which are exploited by an intruder to enforce malware injection attacks. Servers have many VMs; placing together all VMs in one location implies that if some are not adequately separated from the others, this can contribute to attacking and manipulating Virtual Memory System (VMS).

D. *Compromised Virtual Server*

Malware injection attacks that are carried out on virtual machines may also trigger virtual server access modifications. A related case reported in study [4] with the "Amazon EC Public IaaS cloud server" when a ransomware injection assault on it culminated in confidential customer details being accessible to other people using the same system, which is indeed the breach of customers privacy.

E. *Modification of Privileges Attack*

Another form of attack that could challenge NFV protection is known as a privilege modification attack. This threat involves the NFV infrastructure (NFVI) virtualization layer, specifically the hypervisor. In this attack the hypervisor is compromised in a such a that an intruder can modify the system access privileges for different users.

F. *Side Channel Attack*

A side channel attack is an attempt to take full advantage of unintentional information leakage or software bugs in NFV architecture to retrieve sensitive information or obtain unauthorized access. According to our literature study, side channel attacks are launched on two different components of NFV setup which are explained below.

G. *Compromised Shared Memory*

A side-channel is a method of attack that takes full advantage of shared infrastructure. Since multiple users share similar NFV platform, attackers may take full advantage of this reality and attempt to steal personal data of different customers by developing and executing such programs which run on this shared infrastructure. In a virtual system, memory area is shared among multiple VMs, the attacker get access to the illegal memory areas which results in data theft.

I. Compromised Hypervisor

An attacker targets the loophole (i.e., software bug) in the hypervisor scheduler, attacker snatches service time illegally and utilizes the joint virtualized services; this behavior is referred as a theft-of-service attack.

J. Malicious Internal Attacker

A malicious attacker is usually a trustworthy individual of the company, such as consultants, existing or even former staff who purposely try to hack on private information or even disrupt, motivated by economic or social reasons.

The summary of all discussed security threats is provided in Table II.

TABLE II. SUMMARY OF PREVIOUS RESEARCHES ON NFV SECURITY THREATS

S.NO	References	Security Threat	Compromised Device	Description
1	[1]	DoS Attack	Hypervisor	Resource release attack
2	[2]	DoS Attack	Virtual Switch	Bogus traffic generation
3	[3]	Authentication Attack	VNF	Attacker pretends as a network provider
4	[4]	Malware Injection	Hypervisor	Change GUI view of NFV
5	[5]	Malware Injection	VNF	Exploitation of shared memory system
6	[6]	Malware Injection	Cloud Server	Virtual server access modifications
7	[7]	Unauthorized Privileges	Hypervisor	Exploitation of hypervisor bugs
8	[8]	Side Channel Attack	Hypervisor	Exploitation of bugs in hypervisor scheduler
9	[9]	Side Channel Attack	Shared Memory	Illegal memory access
10	[10]	Internal Attacker	Any	Trustworthy staff exploits the system

K. Causes of NFV Security Threats

NFV breaks the network into modules (elements) that can operate on-the-shelf systems. Since these network elements are virtualized, there is a degree of abstractness in NFV networks that do not exist in conventional networks.

L. Hypervisor Dependencies

Currently, there are several hypervisor vendors aiming to become industry participants. However, this competition is being regulated by only a few hypervisor vendors. In this context, the security threats may occur due to the inefficiency of vendors.

M. Elastic Network Borders

An elastic network border means the possibility of altering and scaling the network's capacity dynamically in response to changing demands and workloads. Boundaries in classical network design are set and established by physical equipment such as routers, switches, and gateways [5].

N. Challenging Service Insertion

NFV's appeal is due to its versatility and adaptive strengths. However, as network topology evolves in reaction to demand, standard protection frameworks become stagnant and unable to adapt, making it challenging to respond to new security risks.

O. Firewall Selection Complications

The role of firewalls becomes more important in NFV setup since the infrastructure is open to attacks due to its shared nature. However, it is generally not obvious that which type of firewall is more suitable in some given network settings.

IV. NFV DESIGN CONSIDERATIONS FOR SECURITY

There are various requirements mentioned in literature for successful design and implementation of NFV frameworks for security purposes. We believe that if all these requirements are fulfilled, then security threats can be reduced. These design considerations are given below:

A. Standard Performance Consistency

A security-aware service architecture is required that takes performance, cost, and security concerns into account [6]. For reducing congestion spots in NFV-enabled networks, several strategies may be used at various phases of the process, including load balancing, placement of network functions, and resource allocation [7].

B. Enhancement of Network Security through Multi-Factor Authentication

Security is the fusion of policy and command that safeguard knowledge from danger. Therefore, it is mandatory to minimize the security threats and ensure the reliability of all NFV elements.

C. Policy Manager Contribution to NFV

A structure to extend security policy management to NFV was suggested by Basile et al. In the system, the NFV architecture is applied to a new program feature named Policy Manager. Users may describe protection policies by using high-level procedures (HLP) and the language of medium-level policies (MLP).

D. Security Lifecycle Management

The security lifecycle management of the Network Function Virtualization (NFV) architecture places a high priority on security planning, enforcement, and monitoring. These three components are integral part of security lifecycle as shown in Fig. 4 and details about each component are given below:

E. Security Planning

Organizations must identify and analyze possible security risks and vulnerabilities in the NFV architecture during the security planning process. To provide safe access to the virtualized network infrastructure, security planning also includes specifying access control methods, encryption criteria and protocols for identification [7].

F. Security Enforcement

Following the establishment of the security strategy, enforcement actions are put in place to apply the identified security controls and policies. To guarantee that only authorized individuals may access and administer the NFV environment, access restrictions and authentication measures are in place [7-12].

G. Security Monitoring

Continuous monitoring is required to guarantee that security protections in the NFV architecture remain effective. To detect suspicious behaviours, abnormalities, or possible incidents, security monitoring tools and procedures are used. To efficiently manage and minimize any security events that may arise, incident response protocols are essential to design [13-18].

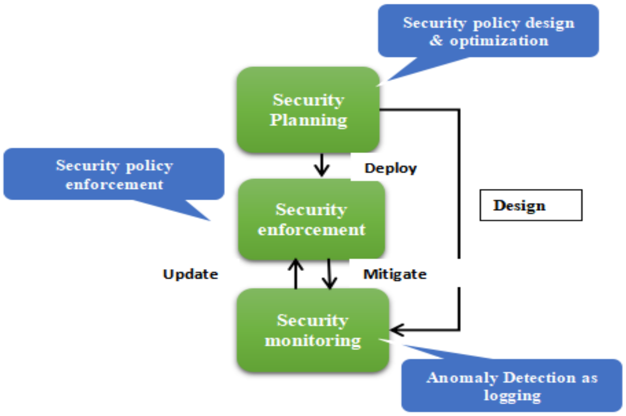
Security policy design & optimization
Security Planning
Deploy
Design
Security policy enforcement
Security enforcement
Update
Mitigate
Security monitoring
Anomaly Detection as logging

Fig. 4. Security planning, enforcement, and monitoring in security lifecycle management.

V. NFV Anomaly Detection Tools

NFV architecture is composed of many different components and it is not unlikely that an anomaly may occur at any place. It is however a challenging task to identify and fix such anomalies because of complicated NFV architecture and diverse range of anomalies. It is therefore important to have background knowledge of NFV anomalies along continuous monitoring of NFV set up. In this regard, there is a recent study that provides a categorization for various types of NFV anomalies [19]. Similarly, in another study [20], it is investigated how various machine-learning techniques can be used for NFV anomaly detection. In this context, it is indeed important to design anomaly detection tools and make them an integral part of our NFV monitoring system [21-25].

VI. Conclusion and Future Work

NFV is a revolutionary technology that has immense promise that can provide service providers with multiple advantages by lowering the expense of building up a network, enhancing it, and enabling consumers to implement such networks continuously. NFV's important features introduced a global shift in the deployment of network functions in the cloud via virtualization. By implementing software-based appliances and leveraging cloud storage, NFV offers several benefits but there are certainly some limitations and challenges. From security perspective, NFV still poses many major protection problems driven by virtualization and network infrastructure. This latest technology should be safeguarded from intruder and outsider assaults, taking into consideration that this network has its infrastructure of multiple organizations that need to be thoroughly examined to recognize future risks and weaknesses. We have provided an outline of numerous NFV security attacks in this article. Since there is a vast literature on NFV security threats, we have categorized different types of security threats in a taxonomy. We have also elaborated how these security threats can target different components of NFV architecture. Then we discussed potential causes which particularly makes an NFV architecture prone to various security threats. We have also presented design improvements which might be useful to countermeasure these attacks. Furthermore, the protection of NFV is still an area of active research, with several safety issues that need to be considered. In this context, the areas highlighted in the designed consideration section can certainly be further explored as future research directions. To illustrate our safety principles in NFV, as a future work, we are also planning to design and implement a secure NFV test bed to investigate various security solutions.

References

[1] He, Gang, Xingxing Liao, and Caixia Liu. "A Security Survey of NFV: From Causes to Practices." In 2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE), pp. 624-628. IEEE, 2023.

[2] Madi, Taous, Hyame Assem Alameddine, Makan Pourzandi, and Amine Boukhtouta. "NFV security survey in 5G networks: A three-dimensional threat taxonomy." Computer Networks 197 (2021): 108288.

[3] Thyagaturu, Akhilesh S., Prateek Shantharama, Ahmed Nasrallah, and Martin Reisslein. "Operating systems and hypervisors for network functions: A survey of enabling technologies and research studies." IEEE Access (2022).

[4] Mazher, Alaa Noori, Jumana Waleed, and Abeer Tariq MaoLood. "The Security Threats and Solutions of Network Functions Virtualization: A Review." Journal of Al-Qadisiyah for computer science and mathematics 12, no. 4 (2020): Page-38.

[5] Qu, Kaige, Weihua Zhuang, Qiang Ye, Xuemin Shen, Xu Li, and Jaya Rao. "Dynamic flow migration for embedded services in SDN/NFV-enabled 5G core networks." IEEE Transactions on Communications 68, no. 4 (2020): 2394-2408.

[6] Pattaranantakul, Montida, Chalee Vorakulpipat, and Takeshi Takahashi. "Service Function Chaining security survey: Addressing security challenges and threats." Computer Networks 221 (2023): 109484.

[7] Benzaïd, Chafika, Tarik Taleb, and JaeSeung Song. "AI-Based Autonomic and Scalable Security Management Architecture for Secure Network Slicing in B5G." IEEE Network 36, no. 6 (2022): 165-174.

[8] Bringhenti, Daniele, Guido Marchetto, Riccardo Sisto, Fulvio Valenza, and Jalolliddin Yusupov. "Introducing programmability and automation in the synthesis of virtual firewall rules." In 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 473-478. IEEE, 2020.

[9] Firoozjaei, Mahdi & Jeong, Jaehoon & Ko, Hoon & Kim, Hyoungshick. (2016). Security challenges with network functions virtualization:. Future Generation Computer Systems. 67. 10.1016/j.future.2016.07.002.

[10] J. Wu, Z. Zhang, Y. Hong, and Y. Wen, “Cloud radio access network (C-RAN): a primer,” Network, IEEE, vol. 29, no. 1, pp. 35–41, Jan 2015. [2] China Mobile Research Institute, “C-RAN: The Road Towards Green RAN. White Paper. Version 2.5.” October 2011.

[11] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, “Network function virtualization: Challenges and opportunities for innovations,” Communications Magazine, IEEE, vol. 53, no. 2, pp. 90–97, Feb 2015.

[12] R. Guerzoni, “Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges and Call for Action. Introductory white paper,” in SDN and OpenFlow World Congress, June 2012.

[13] ETSI Industry Specification Group (ISG) NFV, “ETSI GS NFV 002 V1.2.1: Network Functions Virtualisation (NFV); Architectural Framework,” http://www.etsi.org/deliver/etsi gs/NFV/001 099/002/01. 02.01 60/gs NFV002v010201p.pdf, December 2014.

[14] P. Veitch, M. J. McGrath, and V. Bayon, “An instrumentation and analytics framework for optimal and robust NFV deployment,” Communications Magazine, IEEE, vol. 53, no. 2, pp. 126–133, Feb 2015.

[15] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal, “NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC),” Network, IEEE, vol. 28, no. 6, pp. 18–26, Nov 2014.

[16] ETSI, “European Telecommunications Standards Institute, Industry Specification Groups (ISG) - NFV,” http://www.etsi. org/technologies-clusters/technologies/nfv, 2015, Accessed: June 03, 2015.

[17] ETSI Industry Specification Group (ISG) NFV, “ETSI Group Specifications on Network Function Virtualization. 1st Phase Documents,” http://docbox.etsi.org/ISG/NFV/Open/Published/, January 2015.

[18] ETSI Industry Specification Group (ISG) NFV, “ETSI GS NFV 001 V1.1.1: Network Function Virtualization. Use Cases,” www.etsi.org/deliver/etsi gs/NFV/001 099/001/01.01.01 60/gs NFV001v010101p.pdf, October 2013.

[19] Zoure, Moubarak, Toufik Ahmed, and Laurent Réveillère. "Network services anomalies in NFV: Survey, taxonomy, and verification methods." IEEE Transactions on Network and Service Management 19, no. 2 (2022): 1567-1584.

[20] Zehra, Sehar, Ummay Faseeha, Hassan Jamil Syed, Fahad Samad, Ashraf Osman Ibrahim, Anas W. Abulfaraj, and Wamda Nagmeldin. "Machine Learning-Based Anomaly Detection in NFV: A Comprehensive Survey." Sensors 23, no.11 (2023): 53

[21] S. Lal, T. Taleb and A. Dutta, "NFV: Security Threats and Best Practices", *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211-217, 2017.

[22] M. Pattaranantakul, R. He, Q. Song, Z. Zhang and A. Meddahi, "NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures", IEEE Commun. Surv. Tutor., vol. 20, no. 4, pp. 3330-3368, 2018.

[23] M. Daghmehchi Firoozjaei, J. (Paul) Jeong, H. Ko and H. Kim, "Security challenges with network functions virtualization", Future Gener. Comput. Syst., vol. 67, pp. 315-324, 2018.

[24] X. Gao, B. Steenkamer, Z. Gu, M. Kayaalp, D. Pendarakis and H. Wang, "A Study on the Security Implications of Information Leakages in Container Clouds", IEEE Trans. Dependable Secure Comput., vol. 18, no. 1, pp. 174-191, 2021.

[25] L. Catuogno, C. Galdi and N. Pasquino, "An Effective Methodology for Measuring Software Resource Usage", IEEE Trans. Instrum. Meas., vol. 67, no. 10, pp. 2487-2494, 2018.