IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 22, 2019, accepted April 10, 2019, date of publication May 7, 2019, date of current version May 21, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2915195

Network Functions Virtualization: The Long Road to Commercial Deployments

A. U. REHMAN, RUI L. AGUIAR, AND JOÃO PAULO BARRACA
[1]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal
[2]Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

Corresponding author: A. U. Rehman (asad.rehman@av.it.pt)

This work is funded by FCT/MEC through national funds and when applicable co-funded by FEDER - PT2020 partnership agreement under the project UID/EEA/50008/2019, and Fundação para a Ciencia e Tecnologia under Grant PD/BD/113822/2015.

ABSTRACT Network operators are under pressure to offer efficient network-based services while keeping service deployment costs to a minimum. Network functions virtualization (NFV) can potentially revolutionize network-based services bringing low-deployment costs for network operators. The NFV has been introduced to ultimately extend the non-proprietary and open-standard-based model to network and service deployments, significant improvements to today's proprietary locked implementations. Notwithstanding the continuous efforts of both academia and industry to support the NFV paradigm, the current NFV solutions offered are still in its infancy. In this survey, we provide a detailed background of NFV to establish a comprehensive understanding of the subject, ranging from the basics to more advanced topics. Moreover, we offer a comprehensive overview of the NFV main concepts, standardization efforts, the benefits of NFV, and discussions of the NFV architecture as defined by the European telecommunications standardization institute (ETSI). Furthermore, we discuss the NFV applicability and current open source projects. We then highlight NFV requirements, design considerations, and developmental architectural impairments and barriers to commercial NFV deployments. Finally, we conclude enumerating future directions for NFV development.

INDEX TERMS Network functions virtualization, virtual network functions, server virtualization, hypervisors, containers, Unikernels, network management and orchestration, network programmability, network softwarization.

I. INTRODUCTION

The requirements for supporting Information Communication Technologies (ICTs) have recently evolved as never before. Due to the continuous growth of network devices. Shortly more and more devices will be connected simultaneously to ICTs infrastructure. To accommodate these devices requires re-designing the network architecture to support these large future computing scenarios (managing big data environments). Next Generation Networks (NGNs) research is building its foundation based on multiple evolving technologies. These includes, Network Functions Virtualization (NFV) [1], Software-Defined Networking (SDN) [2], Cloud computing [3], Internet of Things (IoT) [4], Information-Centric Networking (ICN) [5] and the Fifth-Generation (5G) [6] of telecommunications networks, all reputed to transform ICTs infrastructure to fulfill the needs of future computing. It is important to note that all these technologies directed towards supporting a fast-growing trend of network programmability and network softwarization of telecommunications systems.

NFV is a joint initiative of Telecommunication Service Providers (TSPs) to push Information Technology (IT) and telecommunication industry, to a new network production environment, by leveraging modern virtualization technologies [7]. NFV offers several advantages over today's networks such as better network administration, programmability and cost reduction. These advantages lead to an increase in overall network efficiency and performance. Further, NFV has been introduced to fulfill telecommunications operators needs in two main aspects: 1) First, by extending virtualization concept towards networking [8] i.e. (virtualizing network functions). Traditionally networks followed proprietary-based network appliance approaches (also known as middle-boxes) [9]. Typical examples are

The associate editor coordinating the review of this manuscript and approving it for publication was Matti Hamalainen.

load balancers, firewalls, Network Address Translator (NAT) and Wide Area Network (WAN) accelerators. Designing of proprietary-based hardware protocol and instantiates new service deployments is time-consuming and hard because it is difficult to update a protocol running on proprietary-based network appliances [10]. NFV aims to change the way networks are designed, deployed and maintained by realizing virtualized network functions (virtual appliance, i.e., the software implementation of a physical appliance). This software implementation enables the transformation of Network Functions (NFs) running on proprietary hardware appliances to software-based NFs that can run on Commercial-Off-The-Shelf (COTS) systems. These NFs then can enhance application delivery software portfolio to accelerate the network resources for TSPs. 2) Second, it allows TSPs to create and offer new on-demand services without worrying about vendor-specific equipment. NFV eases the management of network services (service provisioning) through virtualization of network functions [11]. This concept offers TSPs more flexibility to deploy new network services.

ETSI, in collaboration with several prominent Telecommunications Network Operators (TNOs), formed the Industry Specification Group (ISG) for NFV on November 2012. NFV has been proposed to address the challenges faced by network operators such as dependence on proprietary-based hardware appliances, and reduced hardware/product life cycles. NFV will also reduce the efforts and expertise needed to design, deploy and integrate complex hardware-based appliances [12]. Other problems arise, though: the challenges of NFV Management and Orchestration (NFV-MANO) framework defined by ETSI must be addressed [13], [14] to accelerate NFV deployments. Currently, several NFV related projects such as OPNFV [15], HP OpenNFV [16], ZOOM [17], ClickOS [18], and 5GEx [19] (and several others) are expected to speed up NFV deployments, mainly focus on different aspects of NFV-MANO framework. Besides these ETSI efforts, the Internet Engineering Task Force (IETF), Internet Research Task Force (IRTF) and 3rd Generation Partnership Project (3GPP) also develop NFV research groups [20].

We believe that NFV is important and useful for future networks for two reasons; Firstly, it increases reliability and resilience without deploying a dedicated physical architecture. Secondly, it can potentially reduce Capital Expenditure (CAPEX) and Operational Expenses (OPEX) cost [1], [21], [22], [23]. In this survey paper, we overview the current state of the art of NFV and provide NFV comprehensive overview. We also examine recent NFV developments as per the NFV architecture framework defined by ETSI. Furthermore, we identified important design consideration necessary for the near future NFV deployments. Finally, we address and discuss essential areas for NFV future direction.

The rest of the paper is structured as follows. Section II discusses previous studies generic and specific to NFV. Section III provides detailed background on NFV and its related concepts. Section IV provides comprehensive NFV overview. Section V discusses main NFV requirements, design goals and key considerations. Section VI discusses realization of ETSI NFV architectural implementation challenges. Section VII discusses generic NFV security, privacy and trustworthiness. Section VIII illustrates impairments to commercial NFV deployment. Section IX discusses perspective NFV future research directions. Section X concludes the paper. The list of abbreviations/acronyms are provided after Section X.

II. RELATED WORK

There are several research studies related to NFV which have applied and explored NFV potential for future networking environments to achieve different sets of objectives. Furthermore, these research efforts related to NFV can be classified into three main categories according to their area of focus [10].

The first category covers the previous efforts and studies that have been focusing on integrating NFV with other technologies such as Optical networks [24], [25], IoT [26], 5G [27], [28], [29], SDN [30], [31], [32], and Cloud computing [33]. All of these studies adopted a generic NFV reference framework which is not designed for any specific scenario. Hence, the real integration of NFV with other technological paradigms is lightly touched and can cause compatibility issues. The compatibility issues are not usually addressed properly in these research studies.

The second category covers efforts that have been focusing on NFV resource allocation [34] and orchestration [35], and aspects which focuses on Virtual Network Functions (VNFs) placement [36]–[38] scheduling [39], [40], and migration algorithms [41], [42]. The center point of these studies is to develop heuristic algorithms that can offer near to optimal solution for scaling VNFs with faster execution time [43].

Finally, the third category includes efforts and studies that focus on tutorials, surveys, and reviews related to either specific NFV topics or a generic review on NFV. For instance, research studies that focuses on specific NFV topics example includes, NFV-MANO [13], [34], [44], NFV security [45], [46], [47], NFV for next-generation mobile networks [28], NFV in 5G [48] etc. Other research studies provide a more generic review on NFV. For instance, [1], [7], [8], [10], [49] have attempted to survey NFV and discusses state of the art, NFV relationship with Cloud computing and SDN, research challenges and opportunities for NFV innovations etc.

These previous studies have not laid down the foundation of the NFV basic topics, neither the road to the NFV journey. Furthermore, ETSI is still changing its architecture and reference framework (and other aspects of NFV). This survey addresses these points and presents an updated view of the status of the NFV-based ecosystem as it moves to commercial deployment. We have clearly distinguished our contribution in this paper in comparison to the other NFV related work as follows:

- We shed a different light on NFV by revealing its past, present, and future research directions.
- We identify barriers that restrict NFV commercial deployments, which was not addressed before.
- We have discussed in details requirements, design goals and critical considerations in the perspective of NFV.
- We provide, organize, comprehensive NFV overview including recent changes that have been made to ETSI NFV architectures and reference framework.
- We highlight the realization of ETSI NFV architectural implementation challenges and outline NFV future research direction from the perspective of softwarization of the telecommunications systems.

III. BACKGROUND AND RELATED CONCEPTS

In this section, we lay down the foundation for NFV and discussed the journey briefly to NFV, its advantages, and we offer a detailed background of NFV, ranging from the basics to more advanced topics, to establish a comprehensive understanding of the subject.

A. VIRTUALIZATION, NETWORK VIRTUALIZATION AND NETWORK FUNCTIONS VIRTUALIZATION

Virtualization is a well-known concept, as virtualization can be claimed to have started in the 1960s when Institute of Business Machines (IBM) introduced an Operating System (OS) named CP-40. The purpose of this was to implement time and memory sharing across users and applications in mainframe computers. This Mainframe virtualization concept laid down the foundation for virtualization that exists today [50]. Today, we define virtualization as a technology that provides an abstract view of underlying resources (hardware systems). This abstract view enables the creation of multiple simulated environments running multiple OS and applications on top of (potentially) different physical hardware systems. Virtualization can be applied in several ways to achieve different goals in computing, storage, and network. For instance, the concept of virtualization can be applied to achieve virtualization of data, desktop, server, the OS, and network functions [51].

Network Virtualization is the process of combining software, hardware resources, and network functionalities into a unified administrative domain known as a virtual network. One of the first initiatives of network virtualization was the Tempest project [52], which introduced the concept of switchlets in Asynchronous Transfer Mode Networks (ATM). This approach was quickly followed by a diversity of projects over the internet. examples are, MBone (for multicast) [53], the 6bone (for IPv6) [54], the X-Bone [55] and many others carried out by several projects including PlanetLab [56], Global Environment for Networking Innovations (GENI) [57] and Virtual Network Infrastructure (VINI) [58](these last examples developed for experimentation, testing and validation of the new concepts at scale). Furthermore, network virtualization plays a significant role throughout the evolution of the programmable network.

Network virtualization provides a logical abstracted view of the physical infrastructure. These logical networks run over shared infrastructures, leading to a reduction in CAPEX and OPEX. Overlay networks are one form of network virtualization. There are many forms of overlay networks [59]. For instance, a current example is a Virtual Private Networks (VPNs), created by the network administrator as a dedicated network to connect multiple sites through the secure tunnel over public networks. Another examples are Virtual Local Area Networks (VLANs), acting as a private Local Area Network (LAN). VLANs can run over the same infrastructure of the normal network (i.e., switches and routers). VLANs can provide efficient traffic isolation for up to 4096 logical networks as specified in Institute of Electrical and Electronics Engineering (IEEE) 802.1q VLANs tagging [60], [61]. Unfortunately, VLANs does not scale, as it is hard to configure and manage when it comes to dividing one physical resource into multiple isolated virtual environments increasingly. Due to this scalability issue with VLANs [62], Virtual eXtensible Local Area Network (VXLAN) have been developed to overcome practical network limitation of the VLANs using an overlay-based network virtualization approach [63]. Currently, IEEE 802.1aq allows to support more than 16 million possible virtual networks as compared to 4096 possible virtual networks available with IEEE 802.1q VLANs tagging.

The idea of an overlay network is quite old. Internet services started to run on top of the telephone network. Hence, an overlay acts as a computing paradigm of virtualization [64], [65]. Typically, in an Internet Service Provider (ISP) several overlay networks are running over the same network infrastructure to offer different services Voice Over Internet Protocol (VoIP), Video and broadband, for instance). These services can be logically separated within the same network infrastructure. Therefore, ISPs can save network infrastructure deployment, management, and maintenance cost by sharing some infrastructure to support multiple services. Network Virtualization usually confused with NFV. For clarity, the main difference is that Network Virtualization provides virtualized networking at layer 2 and on layer 3, while NFV aims to provide virtualized networking at layers (4-7). This approach enables the softwarization of protocol stacks beyond existing network virtualization solutions, thus allowing Communication Service Providers (CSPs) to operate, configure and deploy fully virtualized networking environments with flexibility and agility. NFV has been proposed to assist CSPs to get rid of proprietary-based networking appliances. Furthermore, NFV moves the cost of specialized hardware-based middle-boxes (Layers 4-7) network functions to more flexible and programmable customized pre-packaged software-based VNFs. The disruptiveness of NFV is illustrated in Fig.1, which shows a comparison of traditional hardware-based appliances approach versus the NFV approach [66].

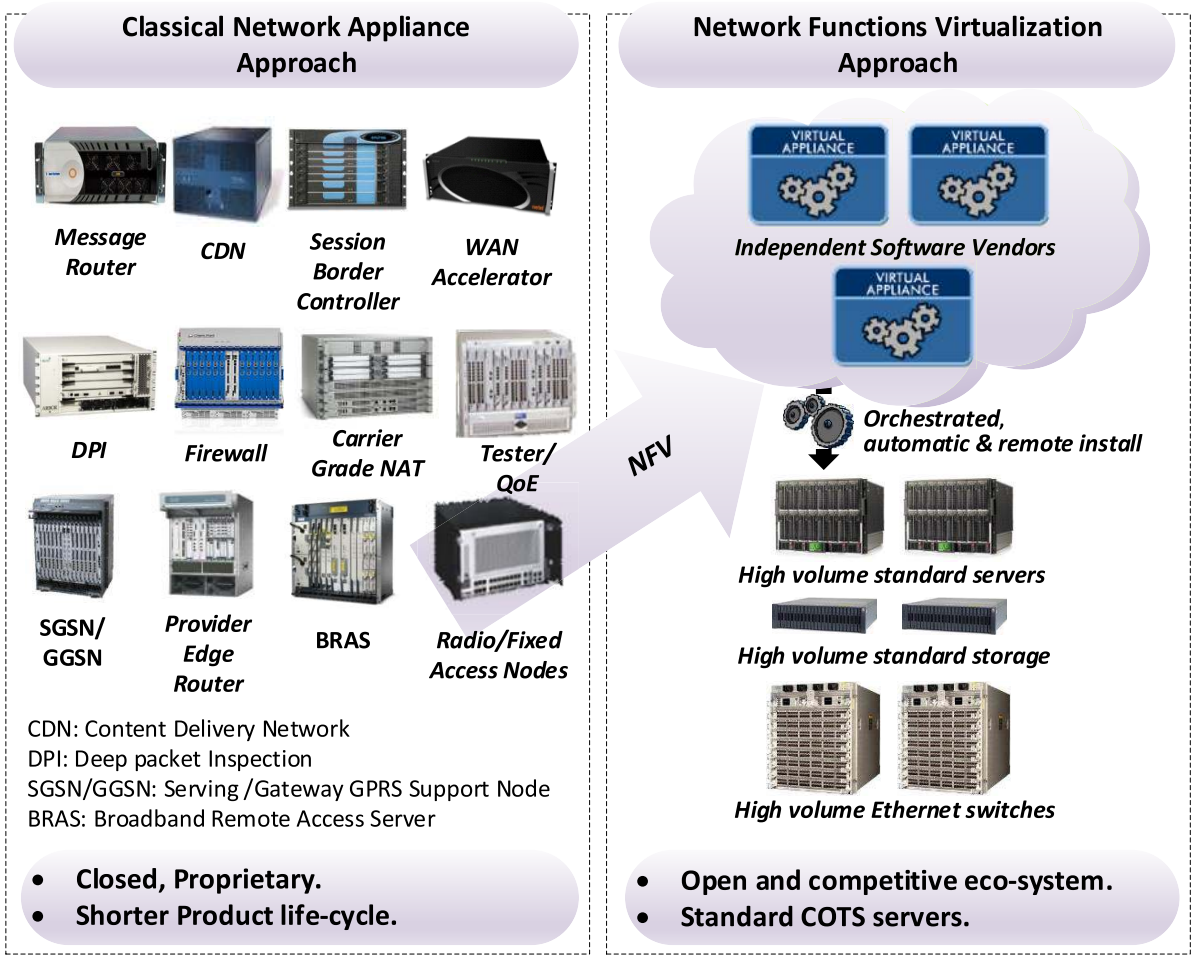

FIGURE 1. Traditional hardware-based network appliances approach versus NFV Approach.

ADVANTAGES OF NFV

NFV offer several advantages to CSPs as compared to the existing hardware-based network functions [66]. The four main advantages of NFV are as following:

- NFV enable the efficient use of ICTs infrastructure through softwarization of NFs. Hence, it brings more flexibility and agility and eases the management of the telecommunications systems.
- NFV offers freedom to (CSPs) to create, deploy and manage network services without worrying about vendor-specific networking devices configuration, since, VNFs are hosted on COTS.
- CSPs appreciate NFV because network functions are virtualized in a way that they can be chained together to create and deploy network services on the fly. Thus, it enables both dynamic scaling and service provisioning.
- NFV offer flexibility to adapt rapidly to technological innovation and provide a better return on investment for CSPs then the case of hardware-based appliances. As product life-cycles are becoming shorter, this can often become critical to support new network services.

B. SERVER VIRTUALIZATION AND HYPERVISORS

In this section, we present concepts and terminologies that are found recently in NFV literature. In this section, we discuss NFV in detail.

1) FROM SERVER PROLIFERATION TO VIRTUAL MACHINE DEVELOPMENT

Traditionally, each application required to run a single server and the server to run continuously, even when the server is not used to its fullest capacity (hardware resources) by the application. Therefore, this has led to the infrastructure challenge known as server proliferation. This problem was due to two reasons: First, the number of servers was growing and second, these servers were highly underutilized. Furthermore, operational challenges such as power and cooling systems for servers, as well as operational expenses to own or buy a place to support such infrastructure became increasingly costly. On top of that, additional servers for backup (probably

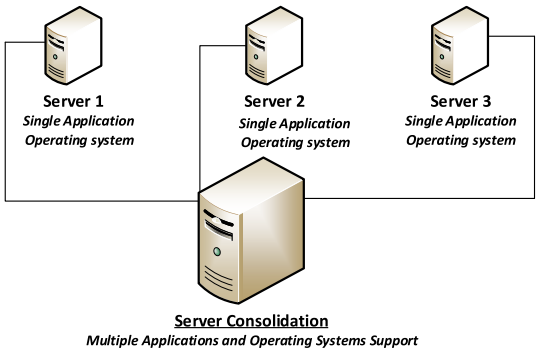

FIGURE 2. Server consolidation.

in different locations) increase even more infrastructure costs for infrastructure owners. The development of the Virtual Machine (VM) concept has fixed the server proliferation problem by consolidating servers through virtualization as shown in Fig. 2 [67]. Due to this, it was possible to use servers more efficiently, offering cost saving for infrastructures owners, service providers, and businesses. In short, the VM development has fixed the server proliferation challenge.

VMware defines VM as follows: "A VM is a tightly isolated software container that runs its own OS and applications as if it were a physical computer [68]." The three main components of a VM are: the host OS, the hypervisor or Virtual Machine Manager (VMM), and the guest OS [69].

A host OS is directly installed on the physical hardware.

The hypervisor is not a new concept; it was introduced in the 60s to run different OSs on a single mainframe computer. A Hypervisor is a software program that is capable of hosting different VMs with different OSs installed and running over the same single hardware resources. Hence, it has the flexibility to support several VMs with multiple OS and applications running on a single hardware resource. Moreover, a Hypervisor is responsible for resource allocation to the VM as well as responsible for monitoring and managing VMs through coordination with the underlying hardware primary OS.

Hypervisors are divided into two types: Type I and Type II, as shown in Fig. 3.

Type-I hypervisors, also known as bare metal or native or embedded hypervisors (hardware-based hypervisors), do not need any host OS because the communication to hardware resources is direct with full visibility of hardware resources [67]. Currently, there are several Type-I hypervisors in the market, with different flavors lead by different vendors (for instance, Microsoft Hyper-V, Open source Kernel Based Virtual Machine (KVM), Xen/Citrix Xen Server, Red Hat Enterprise Virtualization (RHEV) and VMware vsphere/ESXI).

The type II hypervisors, also known as hosted or embedded hypervisor (software-based hypervisor), requires a host OS because the type II hypervisors run on top of the supported OS (an additional layer that interacts with the underlying hardware resources in order to manage VM/Server). Currently, there are several Type-II hypervisors, such as (Oracle virtual box, VMware Workstation, and Microsoft Virtual PC) [71].

Type-I hypervisors are more secure than Type-II, are faster and more efficient. Type-I hypervisors sit on hardware and communicate directly without any additional virtualization layer. However, they are hard to set-up. The Type-II hypervisors are less secure as compared to Type-I. These types of hypervisors are slightly slower and less efficient because an additional layer is needed to manage VM indirect communication to hardware. However, they are easy to set-up. Indeed, the different types of hypervisor utilize different virtualization techniques and would be classified based on their virtualization techniques. Thus, Hypervisors are an integral part of any research on networks virtualization [72]. We summarize the features of Type I and Type II hypervisor in Table 1.

TABLE 1. Type I and Type II hypervisor comparison.

Type I Hypervisor	Type II Hypervisor
Directly runs on server hardware	Runs on top of the supported OS
Minimizing overhead due to direct hypervisor interaction with hardware resources.	Incur overhead as hypervisor runs on top of the supported OS.
Provide better hardware resource utilization	Provide less hardware resource utilization.
More secure due to hardware-based hypervisor	Less secure due to a software-based hypervisor.
Hard to Set-up	Easy to Set-up.
Examples:vSphere, XenServer, Hyper-V, KVM .	Examples: VMware Workstation, VMware Player, Microsoft Virtual PC, Oracle Virtual Box, and Free BSD, etc.

As explained above, VMs created on the top of a hypervisor layer acts as a virtual server running different OSs and application. Thus, it requires an operating system to boot up, manage device and application within the virtual server environment. This is known as a guest OS. Unlike the host OS, the guest OS does not need any modification to run on VMs, therefore, does not have accurate visibility of the underlying hardware. However, hypervisor manages application request from users that are supported by the guest OS through an additional layer and map these request to "physical" hardware or host OS, and allocates resources, in such a way that it seems that guest OS is directly interacting to physical hardware or host OS.

2) CONTAINERIZATION (LIGHTWEIGHT VIRTUALIZATION)

The VM concept and implementations discussed earlier fixed the problem of server proliferation. However, this method still imposes a performance and resource cost due to the overhead associated while imitating the hardware into a virtual environment with high-level isolation and non-shared host Kernel/OS to create a VM. To cope with this overhead and hypervisor performance degradation, a lighter packaged/Kernel-based virtualization with low-level isolation and shared Kernel OS can be used instead. This is called container-based virtualization or containerization [73]. Containers are sometimes

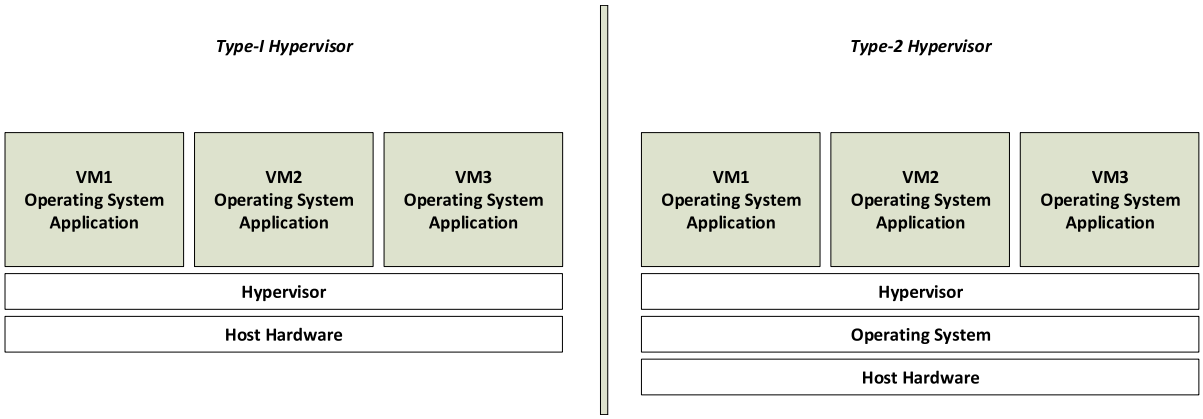

FIGURE 3. Comparison type-I Versus type-II hypervisors [70].

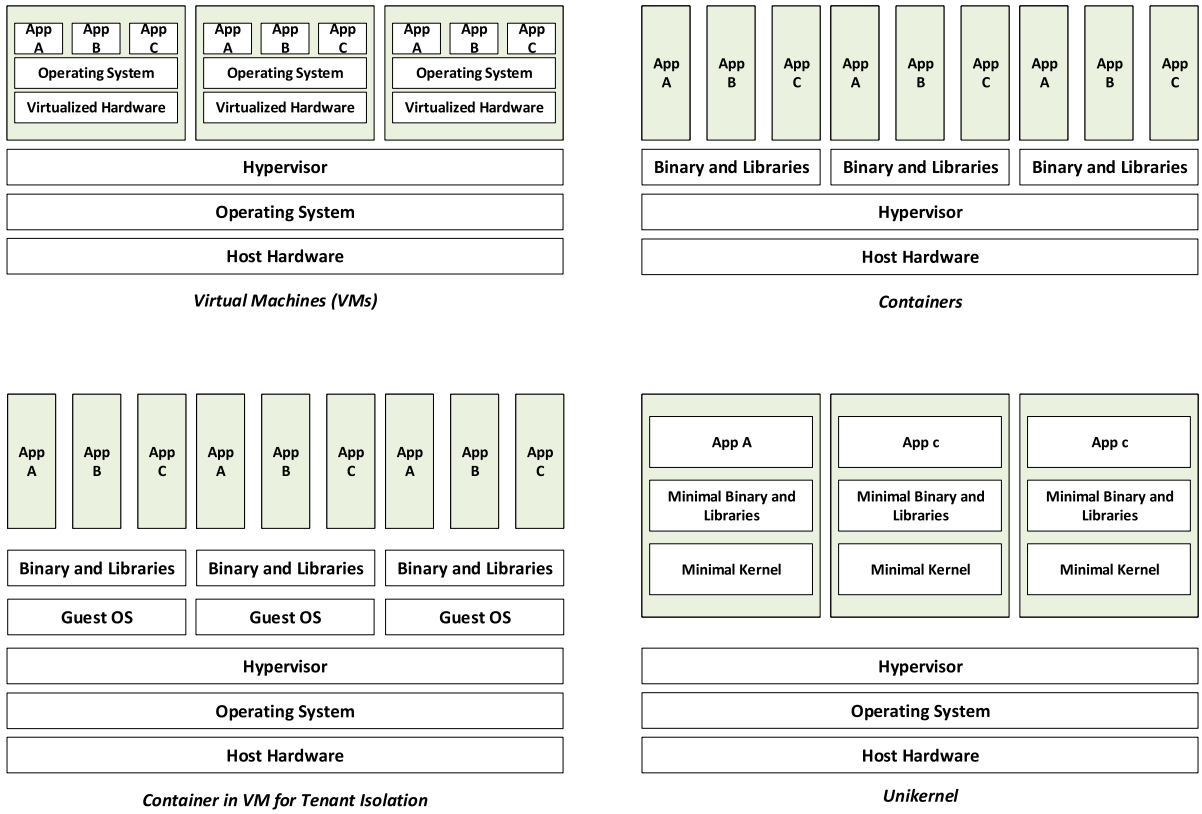

FIGURE 4. Virtualization technologies comparison.

referred to as Linux Containers (LXC) because of their origin on the Linux Kernel. Nevertheless, not all containers are Linux-based containers. Containerization differs from VMs because it provides a policy based segregation of system resources usage. Containers offer superior performance as compared to the VMs [73], [74] because hypervisors are not being used but instead lightweight Application Programmable Interfaces (APIs) within the Kernel. This bypasses the overhead created during hypervisors interaction in VMs environments on thus, offer enhanced performance. Due to the shared Kernel, container-based virtualization is much less secure than VM virtualization.

In addition to that, containers can also be deployed in VMs to provide multi-tenant isolation. The concept of 5G network slicing is an example of such isolation where multi-tenancy can be supported by slicing underlying physical infrastructure [75], [76].

3) UNIKERNELS

"Unikernels are specialized, single-address-space machine images constructed by using library OSs" [77], [78]. These specialized unikernels can then be run on standard hypervisors. The footprint of unikernel is considerably smaller then VM, and containers thus can provide better performance [79].

TABLE 2. Virtual machines versus containers versus Unikernels.

Virtual Machines	Containers	Unikernels
Heavyweight	Lightweight	Tiny
Useful when power and storage are not an issue	Useful when power and storage become critical	Useful when power and storage are in short supply
Run its own OS	Shared Kernel OS	Specialized, single addressed-space machine images using library OS
Limited performance	Superior performance	Superior performance
Fully isolated and hence more secure	Shared Kernel-based isolation hence less secure	Fully isolated and hence more secure
Booting time in minutes	Booting time in milliseconds	Booting time in milliseconds
High overhead due to hypervisor interaction	Low overhead due to lightweight APIs instead of using hypervisor	Minimal overhead due to specialized library OS
Supports multiple applications at a time	Supports multiple application at a time	Supports single application at a time

TABLE 3. ETSI NFV research areas and working groups.

Working Groups	Research Area
NFV-INF	Deals with architecture for the virtualization Infrastructure
NFV-MANO	Deals with the management and orchestration support.
NFV-SWA	Focuses on research purely on software architecture.
NFV-REL	This group focuses on the aspect of reliability, availability, resilience and fault tolerance.
NFV-TST	Focuses on pre-deployment testing and validation of open source NFV.
NFV-TSC	Technical steering committee group to keep an eye on NFV work and facilitate its acceleration.
NFV-IFA	Focuses on Interface and architectural aspect of NFV reference framework.
NFV-NOC	Focuses on network operators councils to develop NFV solution based on their feedback.
NFV-SEC	Focuses on security aspects of NFV.
NFV-EVE	Focuses on evolutionary aspects and ecosystem strategies for NFV.

Unikernels are designed to be able to run a single process. They are also not meant to be multi-user or multi-process. Thanks to this single-minded design, a unikernel is small, lightweight, and quick [80]. Open source work on unikernels includes projects to name a few such as ClickOS, IncludeOS, and MirageOS. [81]. As discussed above virtualization approaches (VM, container, and unikernel) are critical when it comes to applying it to NFV. To explain this, we illustrated the internal architectures of these virtualization technologies and their possible level of implementation in Fig.4. Also, In Table 2 we have provided a brief comparison.

In Table 2 we have provided a brief comparison of these virtualization technologies, which can be useful to determine (from the network designing perspective) which of the virtualization technology can be suitable (concerning performance and deployment cost) for different opted scenarios within virtual networking environments [82].

In the next section, we address the prominent NFV architecture defined by ETSI, its developments and efforts for standardization of NFV-based solutions.

IV. NFV COMPREHENSIVE OVERVIEW

The collaborative work on NFV started in October 2012 when leading TSPs produced a white paper [83] jointly, highlighting the NFV concept, benefits and call for industrial research actions. Moreover, in November 2012 AT&T, British Telecom, Verizon and other leading TNOs developed an Industry Specification Group (ISG) for NFV inside ETSI. Since then ETSI NFV-ISG became the home of the Industry Specification Group for NFV [84]. Further, ETSI is working and primarily has accomplished work of ''level-one'' with the publication of the first five ETSI Group Specifications documents in October 2013 [85]. The first four were focused on NFV across the industry and the fifth about promoting and coordinating public demonstrations, i.e., Proof of Concept (PoC). In 2014, eleven other documents were published, and the first phase was completed as pre-standardization work.

The First phase (''Release 1'') includes an overview of infrastructure update, architectural framework, hypervisor, and domain of network infrastructure. Furthermore, these specifications also covered aspects of NFV-MANO, security, reliability, resilience, and Quality of Service (QoS) metrics [86].

The follow-up ''Release 2'' was then focused on inter-networking of equipment and services, addressing functional blocks requirements, including ETSI NFV architecture framework interfacing and reference points. The ''Release 2'' documentation was completed in 2016.

ETSI NFV ''Release 3'' is underway, and all the evolutions show that NFV is evolving very rapidly. NFV already moved from the conceptual framework to a PoC stage.

NFV-based solutions and research activities span around two main areas: TSPs and Next-Generation Data Center Networking (NGDCN) [87]. NFV provides TNOs with the advantage to combine and expand their current networks with smooth evolution. However, the scope for NFV to transform operator network architecture include scalability, high-performance backbone, Overlay VPN and internet services, amongst others.

Currently, ten working groups are exploring different aspects of NFV architectural framework. We list the details of these working group in Table 3. ETSI has also formed NFV-ISG PoC forum. We list in Table 4. Selected PoC modules demonstrated by different TNOs in liaison with ETSI [88], the open demonstration of the PoC at ETSI is intended to show that NFV is an operable technology. The demos listed in Table 4 suggest different business motivations from operators and vendors in validating different PoCs. Most of these demonstrations used an implementation based on Cloud technologies, (e.g., OpenStack). Also, most of the

TABLE 4. NFV industry specification group PoC demonstrations.

Organization	PoC Demos
British Telecom	Virtual Broadband Remote Access Server (BRAS)
Deutsche Telekom	Virtual IP Multimedia Subsystem (IMS)
Orange Silicon Valley	Virtual Evolved Packet Core (vEPC)
Telefonica	Carrier-Grade Network Address Translator (CGNAT) and Deep Packet Inspection (DPI)

operators have not yet publicized their PoCs. Subsequently, ETSI-NFV-ISG works closely with TSPs and equipment vendors, to specify their requirements for NFV adaptation based on their working environment. This assessment is important to prevent interoperability problems in NFV standardization. Therefore, in reality, NFV is progressing rapidly to reshape the Carrier-Grade Network (CGN) services for ISPs shortly.

A. DESCRIPTION OF NFV ARCHITECTURE FRAMEWORK

Architectures based on the traditional network are tightly integrated because of vendors specialized hardware and customized software's based systems. Unlike the traditional network, the NFV-based architecture allows open source development of software's that can run on generic shared hardware [89]. In this section, we provide a detail description of NFV architecture.

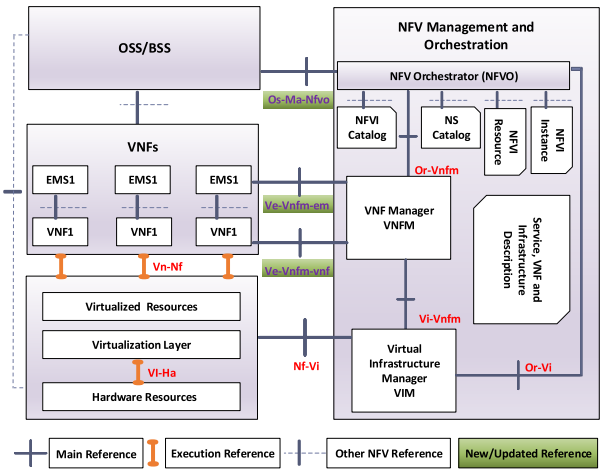

FIGURE 5. ETSI architecture and reference framework for NFV.

ETSI proposed the NFV architectural framework and identified functional blocks and the main reference points between the functional blocks as shown in Fig.5 [21]. ETSI describes the NFV architectural framework at the functional level and does not propose any specific implementation. However, NFV architectural framework is proposed considering the changes that possibly occur in an operator's network due to the network virtualization process (Transition) [21]. Due to these expected changes that can occur in an operator's network, ETSI also defines NFV reference points to ensure consistent information exchange between functional blocks is guaranteed across vendors implementations for functional blocks. The details of these functional blocks are as follows.

1) NFVI

The Network Functions Virtualization Infrastructure (NFVI) functional block is the combination of physical hardware (compute, storage, and network) and virtualized resources (abstracted view of computing, storage, and network). Generally, a hypervisor provides an abstraction to create a virtual environment over underlying infrastructure, in which VNFs can be deployed, managed and executed [90].

NFVIs can be geographically distributed and generally, VNFs deployment location may not be visible (i.e., it can be implemented using available physical resources across different geographical locations).

2) VNFs

The VNFs functional block is composed of multiple VNF and multiple Element Management System (EMS). VNF is the virtualization of legacy (hardware-based) NFs and EMS is responsible for the management aspects of these VNFs. A VNF can be deployed stand alone in a single VM, or it can be deployed across multiple VMs. However, when VNFs are deployed collectively in a group to implement a specific network service, then it must be processed in a certain order due to the possibility that some of the functions have dependencies on others.

3) NFV-MANO

The NFV-MANO functional block is the management and orchestration framework required for the provisioning of the VNFs. It steered the deployment and operation of VNFs on to the NFVI [91]. Moreover, it has a database that stores information which can be helpful in determining the life-cycle properties of services and resources.

4) OSS/BSS

This block is also responsible for coordinating with the traditional network system such as Operation Support System (OSS) and Business Support System (BSS) to ensure the NFV-MANO, NFVI and functions running on legacy equipment with pre-defined communications interfaces.

We have noticed some recent changes that have been made ETSI NFV architecture and reference framework. The changes that are being made to a revised ETSI architecture and reference framework include [92] the re-positioning of the "Service VNF and Infrastructure Description" which was moved inside the NFV-MANO. Previously this was outside the NFV-MANO block with reference point "se-Ma". Since "Service VNF and Infrastructure Description" is re-positioned the "se-Ma" reference point become obsolete. Also, new interfaces were defined for the MANO, including reference points explicitly re-positioned and renamed "Os-Ma" to "Os-Ma-Nfvo", "ve-vnfm" to "ve-vnfm-vnf" and new additional reference point "ve-vnfm-em" as

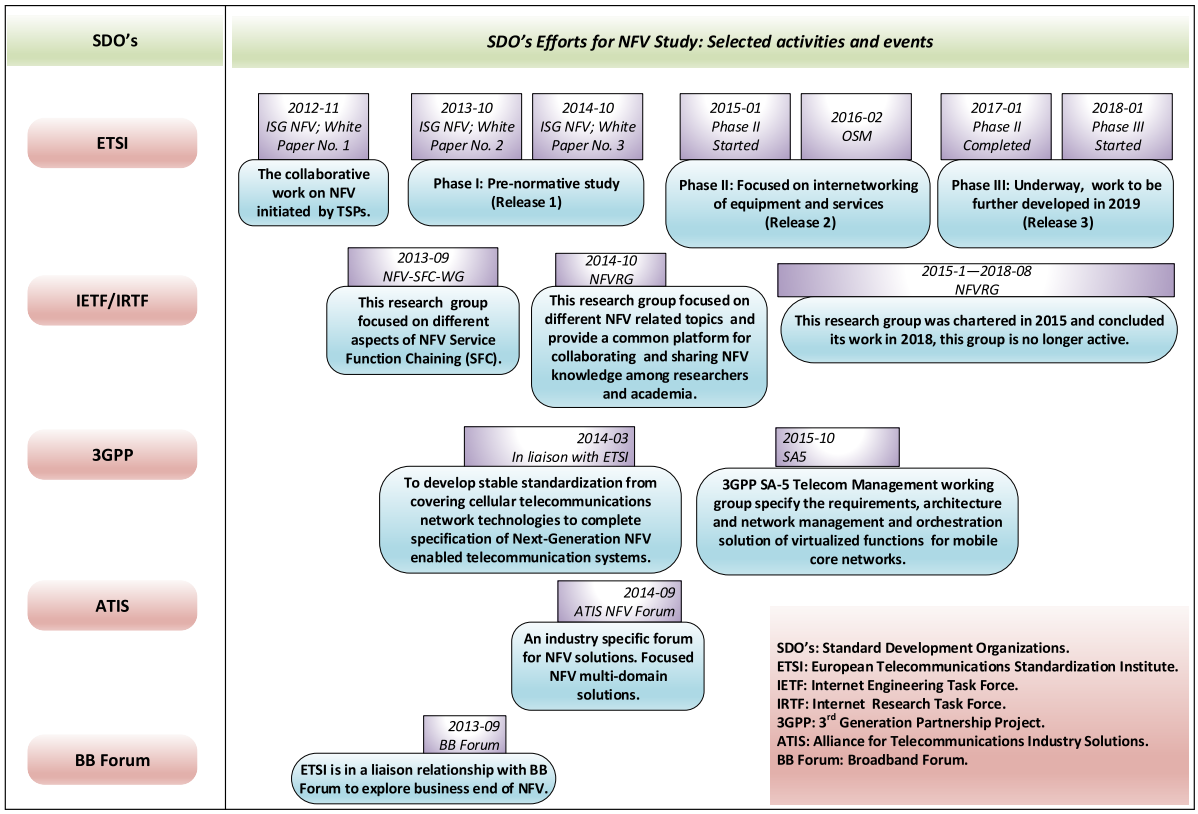

FIGURE 6. SDO's activities over the years for NFV standardization.

depicted in Fig.5. All these recent changes show that NFV is still undergoing major standardization developments.

B. EFFORTS FOR NFV STANDARDIZATION

There are several related standardization entities (Standard Organizations) such as IETF, IRTF, ETSI, Broadband Forum (BB-Forum), Alliance for Telecommunications Industry Solutions (ATIS) (which is also in collaboration with industry organizations such Global System for Mobile Communications (GSMA), Metro Ethernet Forum (MEF), Tele Management Forum (TM-Forum)) under which specific NFV research groups carry out different research activities to contribute to different areas of NFV for its continuous standardization development.

The IRTF mainly focus on long-term research issues related to the internet while the IETF works in parallel to IRTF but focus only on short-term issues related to internet and make efforts to support engineering and uniform standardization of the Internet [93]. NFV Research Group (NFVRG) is one of the research groups in IRTF to address NFV-related topics [94], [95] (this research group was chartered in 2015 and concluded its work in 2018 [96]). Another group is IETF Service Function Chaining Working Group (IETF-SFC-WG) which focuses on NFV Service Function Chaining (SFC) and perform standardization activities for new service delivery approaches, operation, and management [97].

ETSI NFV-ISG mainly focuses on the NFV architecture and reference framework, NFV-MANO [84]. Further, several subgroups are currently involved in exploring different areas of NFV details, listed in Table 3, to accelerate its deployment. IETF and IRTF work closely with these groups (and others) to regulate NFV standardization.

The ATIS NFV forum focuses on advancing industry solutions to define new business models and requirements for supporting the use of NFV technology [98]. The objective of the ATIS NFV forum is to provide interoperability and inter-networking between service providers. Moreover, the ATIS NFV forum has an emphasis on NFV services in the multi-administrative domain, unlike ETSI and other NFV standard activities which focuses on the single administrative domain. Although, security and service discovery in inter-domain is a challenge and ATIS NFV forum is exploring this challenge while collaborating with industry organizations to enable the commercial deployment of the ATIS NFV leading to inter-domain systematic framework.

The Broadband Forum (BB Forum) is an association of several TNOs, companies, vendor and businesses related to the broadband networks solutions. The BB Forum relies on these partners for the new technological developments and recognizes their contribution. Also, their partners rely on BB Forum to identify potential new market and implementation focus for their new technological developments in the broadband market. The BB Forum set the new vision ''Broadband

2020'' as a hyper-connected, agile and valuable broadband network. This evolution of broadband aims to enable seamless user connectivity everywhere, performance-assured services. Furthermore, the Broadband 2020 vision opens potential new market segments for NFV-based technology [99].

There are also seven Standard Development Organizations (SDO's) across the world that partner with 3GPP for working on wireless NFV, namely: The Association of Radio Industries and Businesses (ARIB), the Telecommunication Technology Committee (TTC) of Japan, the ATIS, the Telecommunications Industry Association (TIA) of the USA, the China Communications Standards Association (CCSA), ETSI and the Telecommunications Technology Association (TTA) of Korea. 3GPP collaborates with these partner organization to develop stable standardization from covering cellular telecommunications network technologies to complete specification of Next-Generation NFV enabled telecommunications systems. 3GPP produces technical specification and exchange information with the standard partner organizations and eventually become an appropriate global standard. Moreover, 3GPPs define Technical Specification Group Service System Aspects (TSG-SA) in which working group SA5-Telecom Management specifies the requirements, architecture and network management and orchestration solution of virtualized functions for mobile core networks. 3GPP SA-5 Telecom Management ''Release 13'' focuses on NFV-MANO as defined by ETSI and ''Release 14'' focuses on E2E management solution (management concept, architecture and requirements for mobile networks that include VNFs, life-cycle management, configuration management, fault management, and performance management). These are normative specification work towards NFV-MANO in liaison with the ETSI [100].

C. NFV APPLICABILITY

ETSI has proposed several use cases for NFV [101], [102]. We discuss here three prominent use cases, where the NFV concept is applied to Customer Premises Equipment (CPE), Evolved Packet Core (EPC) and Network slicing. These use cases highlight the benefit of isolation, CAPEX and OPEX as well as facilitating the deployment of new services with existing infrastructure in faster time as compared to traditional use cases of such implementation [103]. Moreover, NFV is a promising technology with more flexibility that brings forward the possibility of several new services to users and better service agility.

1) NFV FOR CPE

In Fig.7, we illustrated a traditional way of implementing a CPE. It is made up of several functions including firewalls, Dynamic Host Control Protocol (DHCP), NAT, Switching and routing. Currently, these functionalities are operational only through physical devices located at each customer site. It is hard to make changes to these network functions in order to add, remove or update functionality. Making changes to network functions sometimes requires replacement of the hardware at the customer site. This process is costly for the ISP as well as (in some cases) for the customer. As illustrated in Fig.7 the possible cost-effective and efficient solution uses NFV by transferring some of the functionalities of CPE to the shared infrastructure in the vicinity of the service provider [104], [105]. This sharing of resources enables adding and removing network functions within CPEs more efficiently and reliably without any additional cost of changing hardware. Hence, a considerable cost saving of CPE at a large scale.

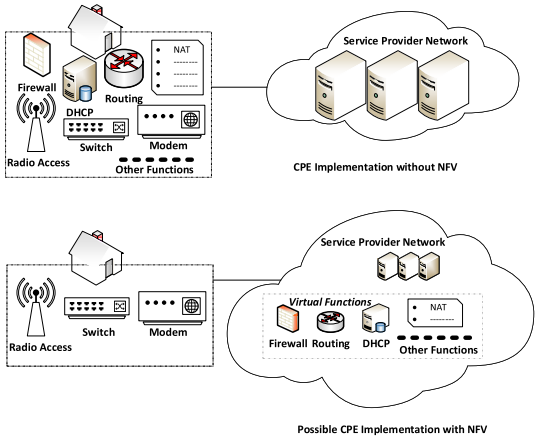

FIGURE 7. CPE with NFV and without NFV.

2) NFV FOR EPC

Virtualization of EPC is another use case of NFV that recently attracted significant interest from industry. 3GPP specifies the EPC as a core network for Long-term Evolution (LTE) [106].

EPC is composed of several elements based on hardware: Serving Gateway (S-GW), Mobility Management Entity (MME), Policy and Charging Rules Function (PCRF), Packet

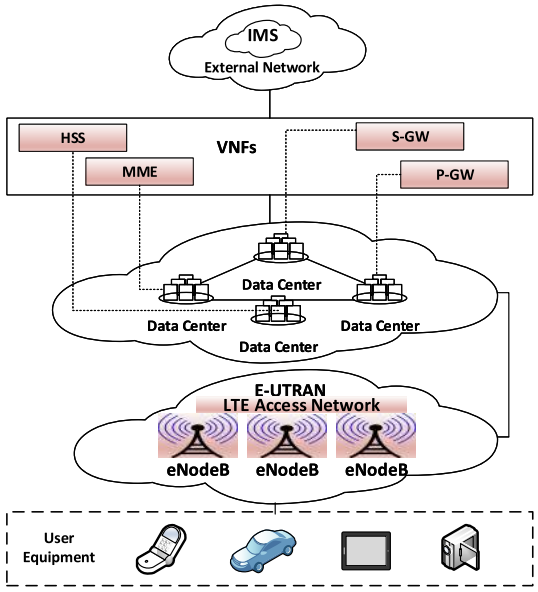

FIGURE 8. Virtualization of EPC.

TABLE 5. Current selected active NFV open source projects and their characteristics.

Projects Names	Leaders, Company or Organizations	Focus Area in NFV Framework	Main Purpose
OPNFV	Linux Foundation [107]	VIM, NFVI	Support NFV testing, and integration; to build an open-source platform to accelerate NFV deployment for future networks.
OpenNFV	Hewlett-Packard [16]	VNFM/EMS, VIM, NFVO, OSS/BSS, NFVI	Open, flexible NFV ecosystem to speed-up NFV deployment for communications service providers
ZOOM	TM Forum [108]	VNFM/EMS, VIM NFVO, OSS/BSS	Enable service automation and control for NFV dynamic environment with agility.
ClickOS	European Union [109]	VNFs, VNFM/EMS.	High performance virtualized software middle-box platform to enable fast and lightweight NFV solutions.
Blue Planet	Nuage and Ciena [110]	VIM, NFO, OSS/BSS	Enable Multi-domain and Multi-tenant end-to-end services and use orchestration as a tool to create and deliver services intelligently.
5GEx	European Union [111]	VIM, NFVO, OSS/BSS, NFVI	Focus 5G infrastructure and direct towards unified multi-domain orchestration to support heterogeneity
Aria	GigaSpaces [112]	VNF, MANO, NFVO	Open source orchestration engine for implementing TOSCA specification (Topology and Orchestration Specification for Cloud Applications) with focus on developing an embeddable lightweight library of orchestration tools for NFV and hybrid Cloud orchestration solution based on TOSCA.
Cloudify	GigaSpaces [113]	VNFM, MANO, NFVO	Cloud orchestration platform based on TOSCA designed to provide automation of network services and simplify orchestration of various stacks and hybrid Cloud environments.
Gohan	NTT Data [114]	VNFM, MANO, NFVO	Unified and simple Cloud service architecture that enable micro-services in a minute and as a single unified process for developers for creating and managing Representational State Transfer (REST) style API's.
Kubernetes	Google [115]	VIM, MANO, NFVO	A system for automating containerized applications its deployment, scaling, and management. It enables advance scheduling and orchestration for intensive business and enterprise computing environments.
OpenSource MANO (OSM)	ETSI [116]	VNFM, VIM, MANO, NFVO	Management, and Orchestration (MANO) software stack aligned with ETSI information models to meet commercial deployment of NFV networks.
OPEN BATON	Fraunhofer Berlin [117]	VNFM, VIM, MANO, NFVO	Design extensible and customized orchestration of network services across heterogeneous networks. Moreover, to support features such as openness, interoperability, and extensibility in an NFV environment.
Sonata NFV	European Union Horizon 2020 [118]	VNFM, VIM, MANO, NFVO	Design NFV architecture for the operators and service developers. Moreover, enable flexible programmability of software networks, development of tools for virtualized services and integrated solution for Development and Operation (DevOps) service platform and orchestration system.
Tacker	OpenStack [119]	VNF,VNFM, MANO, NFVO	Enable NFV orchestration for OpenStack platform based on ETSI MANO architectural framework.

Data Network Gateway (P-GW) and Home Subscriber Server (HSS) [106]. It is important to note that the compatibility issues with current EPC still exist because the equipment that supports various network functions are still proprietary [28]. Due to this, it is difficult to manage this situation as minor changes to a given network function can cause compatibility problems and thus, requires replacement of the equipment. In order to solve this problem, EPC can be virtualized using NFV. Depending on the level of implementation of some cases, full or partial functions of EPC can be transferred to shared infrastructure as illustrated in Fig. 8. Therefore, virtualization of the EPC could lead to dynamic scaling and better flexibility regarding adding new services and improving existing ones in a faster and efficient way.

3) NFV FOR 5G NETWORK SLICING

The 5G technology is forming a basis for NGNs development. 5G network slicing concept is introduced to support multi-tenancy, multi-vendor, and multi-domain in virtualized networking environments [75], [76]. In Fig. 9, the concept of 5G network slicing is illustrated, in which a common underlying physical infrastructure that is sliced to enable multi-vendor and multi-domain networking in 5G.

A network slice is independently managed and isolated environment of NFs and infrastructure resources [48]. Therefore, NFV is considered as a key enabler to achieve the realization of network slicing concept in 5G and beyond 5G [75]. Moreover, multi-domain orchestration is also a key concern for NFV [120]. Therefore, the multi-domain orchestration is a must offer to support multi-domain-multi-vendor and

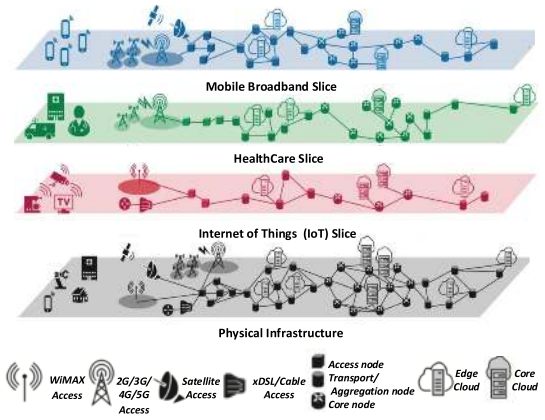

FIGURE 9. Multi-tenancy, multi-vendor and multi-domain networking scenarios (network slicing) [75].

multi-tenant communication in 5G and beyond 5G networking environments.

D. NFV RELATED ACTIVE PROJECTS

Currently, several active projects focusing on NFV, such as OpenNFV, Opensource MANO (OSM), OPEN BATON, Kubernetes, and others [121]. The detailed description of some relevant projects are listed in Table 5. All the projects mentioned in the table focus on different blocks of the NFV reference architecture framework (as defined by ETSI) to accelerate NFV deployment and automate the provisioning of dynamic services through intelligent management and orchestration. Generally, these Open-source projects contribute to the development of the future standardization [122].

V. NFV: REQUIREMENTS, DESIGN GOALS AND KEY CONSIDERATIONS

The technical requirements for implementing VNFs (including network performance, and manageability, reliability, and security) are discussed in [49]. We also identified several design considerations essential to build TNOs confidence in NFV as a viable technology. We argue that for any solution of NFV or related concept the following technical aspects in NFV design must be considered. In the next subsections, we discuss these aspects in detail.

A. INTEROPERABILITY

The initial expectation to deploy NFV in a virtualized networking environment is that it must offer to decouple from proprietary-based hardware appliances. This decoupling is necessary to avoid any compatibility (interoperability) issues between different manufacturer's that develop hardware equipment. When interoperability testing is successful, service providers then have the freedom to implement a dynamic range of network topology, customized routing policies, and forwarding, regardless of the complexity of the underlying systems. VNFs are hosted by COTS equipment, therefore, NFV infrastructure should be able to instantiate VNFs dynamically at the right time in the right locations to compose service chaining and scale hardware resources. This means that the TNOs can achieve greater flexibility by defining specific service to a particular service chain [123]. Hence, this simplifies the service provision as well as allows network operators to initiate quickly, move and alter network services with ease. Therefore, it enables flexibility to re-program network elements rather than replace them in a costly procurement process.

B. RESILIENCY

Traditionally, resiliency refers to the design feature where network failures are to be made small with rapid convergence time. Moreover, resilience procedures are considered essential to overcome network issues such as failure, attacks and traffic congestion. These issues can cause an interruption in network services and directly degrade the performance of a network [124]. Further to that, in an NFV environment, most of the networking components and functions are software-based. Therefore, to ensure service continuity and availability, the reliability issues during NFV software upgrades must be addressed. Mechanisms must be developed that supports reliable software update and added functions without affecting service continuity of the users.

C. PERFORMANCE CONSISTENCY

Due to different vendor hardware, provider hardware performance varies depending on parameters such as the Central Processing Unit (CPU), memory and type of storage [125]. These parameters are critical to performance. Therefore, all potential bottlenecks that can affect performance must be mitigated so that functions running over dedicated infrastructure and network function created after virtualization can maintain performance consistency. However, this needs a lot of effort and research to identify all the possible bottlenecks at a different layer of networking as well as different approaches to identify and mitigate performance bottlenecks in a shared infrastructure.

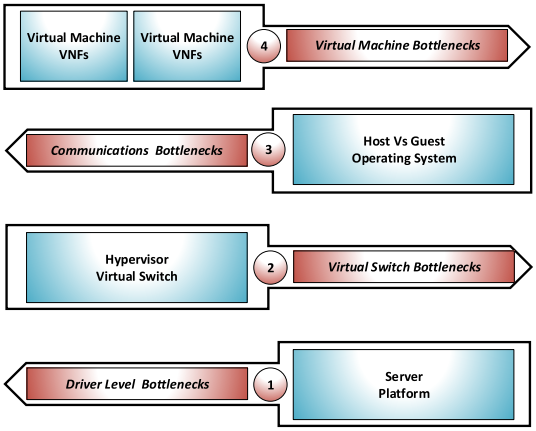

FIGURE 10. Virtualization bottlenecks [125].

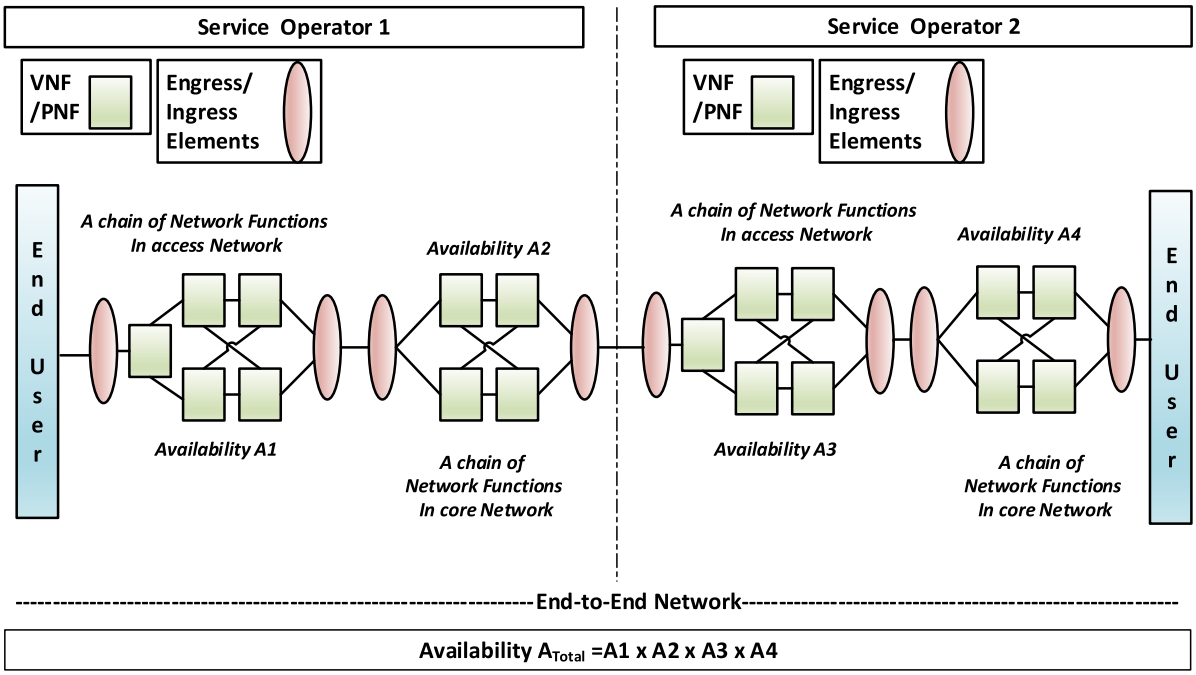

FIGURE 11. E2E Availability of network service incorporated of four separate service chains, provided by two different service operators [129].

In NFV, two main areas where performance challenges have not been alleviated yet are 1) Virtual Switch (vSwitch): The vSwitch seems to have become a performance bottleneck in bidirectional traffic (voice, video, and date) scenarios. 2) Hardware Acceleration: Typically, Field-Programmable Gate Arrays (FPGAs) are used to accelerate the performance. However, hardware level acceleration must be fine-tuned in NFV-based deployment to maximize the performance and VNFs elasticity across the networks [126].

Fig. 10 shows possible bottlenecks by utilizing the common infrastructure. A recent research study carried in [127] described enhanced VNFs performance by utilizing Data Plane Development Kits (DPDKs), and shows achieved performance for small and large packet processing, like what can be performed using dedicated hardware?. In addition to that important study in [126], [128] also identifies that FPGAs can also enhance the performance of VNFs. However, these offered solutions are still far from optimal.

D. RELIABILITY AND AVAILABILITY OF END-TO-END SERVICES

Reliability of networks relates to the traditional low probability of failure in networks and availability of networks relates to the traditional low probability of networks system to run without failure. These two concepts are vital for network operators when deploying E2E services. Historically, the Public Switched Telephone Network (PSTN) architecture built on "Five 9s" that ensure 99.999% End-to-End (E2E) reliability and availability. However, most of today's virtualized network does not provide availability and reliability equivalent to PSTN levels.

Generally, a E2E network service could be, for instance, mobile voice/data, Internet access, VPN and can be defined by one, or several NFs forwarding graph linked to the endpoints through interconnected NFs [129]. Moreover, the network service behavior is the reflection of the combination of its essential functional block (which can include NFs and virtual links). Thus, the reliability and availability of a network service or services must be estimated (realized) based on the reliability and availability of these essential functional blocks.

E2E reliability and availability are the key considerations for network operators when deploying services, which is typically done by composing service chain of NFs that can drive different policies in dynamic environments [130]. ETSI also addressed modeling of an E2E service to estimate reliability and availability in an NFV environment. Although, the reliability, availability and other aspects usually are observed after deployment, using a set of tools to monitor the performance level of these services in a dynamic networking environment.

Conventionally, operators evaluate reliability and availability of E2E services by evaluating each of service chain separately and calculate them (as a function of availability) according to the connected patterns of the chains [129]. Furthermore, NFs can be implemented in a single domain (single operator network) or E2E service can be partitioned in multi-domain (different operators) in multiple service chains, for instance, access and core networks as shown in Fig. 11. This concept applies to both traditional and virtual

environments, for instance, as shown in Fig. 11, the availability of E2E service can be calculated as the product of the different service chains consisting the E2E network (1).

$$A_{Total} = A1 \times A2 \times A3 \times A4. \quad (1)$$

Network operator's use this concept from Open System Interconnection (OSI) layer 4-7 to virtualize connected network services to offer a variety of services and different characteristic of services under a single network connection. Moreover, this enables the network provider to automate network services as well as ease the management of traffic flow between connected services.

In NFV settings, VNFs, and virtual links are positioned over an NFV Infrastructure with defined interfaces. This NFV-based infrastructure is composed of a hypervisor and hardware resources (elements) in some physical locations. However, we argue that it is quite challenging to find the relationship between these elements and NFV-MANO functions to estimate the reliability and availability of a virtualized service chain. Furthermore, this includes life-cycle operations, fault management cycle, and a set of mechanisms to implement them which can affect reliability and service downtime [131]

NFV must evolve to enhanced E2E reliability. Currently, NFV approaches new reliability and availability models that can be used to estimate E2E services in NFV-based dynamic networking environments [132]. Furthermore, the design goals details for E2E reliability defined by OPNFV forum are given in Table 6 which defines different reliability testing criteria for NFV environments (based on service downtime for specific products).

TABLE 6. The design goals for reliability testing in NFV [133].

Availability	Down Time in a year (In minutes)	Product applied to
99.9%	500	Computer/Server
99.99%	50	Enterprise Class Device
99.999%	5	Common Carrier-Class Device
99.9999%	0.5	High Carrier-Class Device

E. CONTROLLING DYNAMICITY IN MULTI-TENANT ENVIRONMENTS

Generally, there are two types of customer deployment architecture: single tenant and multi-tenant.

In single tenant architecture, resources are isolated and secure. Thus, they offer more flexibility and manageability to implement customized changes without superior handling because of single ownership. However, single tenant ownership is costly.

In Multi-tenant architectures, resources are utilized more efficiently but provide limited isolation and reduced level of security. Moreover, in multi-tenancy, changes are not easy but only possible with the consent of other tenants, because of such multi-tenant ownership. Therefore, high availability, manageability, and data plane performance aspects in multi-tenant architectures are still not yet achieved. These aspects must be fulfilled before NFV wide-scale deployment.

From the infrastructure owner point of view, multi-tenancy provides market agility (i.e., shorter time to market) and less deployment risk. From the Operators point of view, they have the benefit of multi-tenancy because it saves CAPEX investment and commitments. However, in future multi-tenant based infrastructure, changes will occur more often, and within a wider range of possibilities, links can appear and disappear; capacity can fluctuate (e.g., through link conditions), either. Therefore, future NFV environments must be able to control high dynamicity as well as guarantee Service Level Agreements (SLAs) in a multi-tenant environment.

F. HETEROGENEITY

NFV should be able to provide openness to support the heterogeneous use of NFVI platform for TSPs to be able to run the various application over shared infrastructure without any compatibility issue from multi-vendor NFV deployment. Thus, it is essential for the success of NFV to support heterogeneity. Otherwise, more resource consumption will appear in NFV deployment. Transiting to NFV may not be justified without supporting heterogeneity.

G. SECURITY, PRIVACY AND TRUSTWORTHINESS

Network security refers to the combination of policies and control that protects data and network. Moreover, several trustworthiness mechanisms are defined to block the threats entering into the network [134]. In an NFV environment, several potential security risks must be considered [46]. Network virtualization must guarantee isolation to minimize security risks, as well as safeguard stability and convergence time. The advantages of NFV (such as cost and performance) also introduce new security challenges that are essential to consider for developing and ensuring accountability at each layer of security; domain isolation (improved confidentiality) and remote attestation (verification) [135]. Isolation can enhance Fault-tolerance, security, and privacy while attestation is necessary for verifying trust status of NFV platform [136], [137].

H. ELASTICITY, AUTOMATION AND SCALABILITY

Network capacity planning is essential for the successful deployment of NFV. Unlike the capacity planning of traditional networks based on hardware-centric approaches. NFV requires new capacity planning measures with software/information-centric approaches to address dynamicity in an NFV environment. Elasticity refers to scaling up and scaling down network services to meet service demand or improve network performance in an NFV environment [138]. Therefore, consumption-based modeling can improve elasticity in NFV. Next, automation refers to the ability of the system to recover the error with minimum or no human intervention. The prerequisite for network automation is to simplify the configuration so that reduced troubleshooting

time can be guaranteed. At last, the NFV design must scale on commodity hardware with ultra-low latency and optimal performance [139].

I. ENERGY-AWARE INFRASTRUCTURE

The fast-paced technological developments over the past few years have enabled a deep digital transformation undercurrent in society. This means that shortly there will be a significant increase in the usage of ICTs infrastructure which has an associated growing impact on energy consumption [140]. Nowadays, societies are globally facing energy efficiency challenges (coupled with ICTs carbon footprint reduction pressure) [141], [142], [143]. Recently, significant research efforts are being focused on the development of energy-aware ICTs infrastructure (supporting green networking environment) [144]. According to ETSI, studies have indicated that NFV can provide up to 50% reduction of inefficient energy consumption [145]. However, this claim has not been yet demonstrated comprehensively. There are some studies that addressed different aspects of NFV energy efficiency [146], [147], [148]. Energy efficiency in NFV is still a key issue, and there is still a need to develop an energy-efficient NFV-based ecosystem for ICTs.

VI. REALIZATION OF NFV ARCHITECTURAL IMPLEMENTATION CHALLENGES

In this section, we discuss ETSI NFV architectural implementation challenges. Providing a solution to these challenges can significantly improve demand for NFV. The ETSI NFV-ISG group architectural framework has to define NFV architecture building blocks and reference points but has not yet indicated specified NFV implementation and PoCs. We discuss challenges of NFV architectural framework briefly as defined by ETSI.

A. NFVI:NETWORK FUNCTION VIRTUALIZATION INFRASTRUCTURE

Earlier we discussed the NFVI block, of the NFV architectural and reference framework. NFVI covers three-layer: Hardware resources, Hypervisor domain, and Virtualized resources. Moreover, this block supports a virtual environment where VNFs are executed and deployed over the underlying hardware resources. The virtualized environment is composed of servers, virtual machines switches, and virtual switches, etc.

We consider several main challenges for functional block of NFVI as follows [34]:

- How hardware resources can be designed and utilized to translate the virtual environment efficiently?
- How to maintain and update a software-based environment (virtualized environment)?
- How to keep track of continuous development and integration of software that is interacting with underlying hardware resources?
- How can NFVI maintains connectivity between locations such as data center and private/public Cloud or hybrid Cloud environment?

The questions as above-mentioned arise because the standard procedure and implementation of NFVI are not yet fully regularized. The NFVI functional block is critical to NFV-based VNFs implementation such as, vEPC, Content Delivery Network (vCDN) and Virtual Customer Premises Equipment (vCPE) etc. [45]. Therefore, establishing Key Performance Indicators (KPIs) to ensure VNFs consistency and performance becomes challenging.

Hypervisor, hardware resources (compute, storage and network) are going to be provided by different vendors. Therefore, integrating and incorporating trust and security in a multi-vendor virtual environment is also challenging.

Managing virtualized resources is critical for NFVI, as NFV mostly depends on the software and developing a practice to maintain the continuous quality of software in NFVI is also challenging. However, it is well-known that VNFs are independently deployed through a cross-layer platform such as OpenStack, but additional tools for monitoring and managing such VNFs are deployed over the COTS hardware need to be developed to implement VNFs functionality across the network [28] successfully. The Above mentioned challenges for ETSI NFVI blocks must be addressed before NFV pre-deployment testing and validation phases.

B. VNF'S:VIRTUAL NETWORK FUNCTIONS

The VNFs block consists of multiple VNFs and multiple EMS. Each VNF is assigned to specific EMS to implement services in a virtualized environment. EMS system keeps track of associated VNFs configuration, and its monitoring while VNFs are running on single or multiple VMs. VNFs are created uniquely and in isolated virtual environments to meet the scalability, security and performance requirements. However, guaranteeing these aspects is challenging [34]. Since VNFs deployment utilized NFVI, three main challenges arise as follows: Portability, Resource allocation, and Performance.

First of all, the performance of VNFs depends on both the hardware and the software that builds together a virtual environment, where the concept of the NFV is practically realized [149], [150]. The VNFs must provide performance values on commodity servers similar to NFs running on hardware equipment. VNF software must be of high quality and must avoid performance bottlenecks, and maintain accountability at each layer of the virtual environment. Indeed, network service functions such as firewall, Intrusion Detection System (IDS), Intrusion Prevention Systems (IPS) are now virtualized to support multi-user multi-service environment (multi-tenancy). Thus, a physical switch can connect the service node to the network, but users are logically separated through virtual switching inside the multi-tenant environment.

This virtual switching is implemented in software to mirror the functionality of the physical switch and require sev-

eral operations such as encapsulation, de-encapsulation, NAT and policy that are implemented to shape traffic inside a multitenancy environment. This consumes significant computing resources that lead to performance degradation of the virtualized system (especially in high data rates environment) to avoid such consumption of resources there is a need to and increase the efficiency of virtual switching by developing high performance virtualized systems and environments [151].

Another challenge is portability. The VNFs must be portable between servers and across the network. The live migration of VNFs must be possible without any performance degradation. Several cross-platforms such as OpenStack, Eucalyptus, oVirt, OpenNebula, and Nimbula are also working towards supporting the portability of VNFs in an NFV environment [28].

C. OSS/BSS: OPERATIONAL AND BUSINESS SUPPORT SYSTEM

NFV is transforming the way the telecommunications infrastructure is deployed. Therefore, the way service is delivered by CSPs is going to change significantly. Thus, NFV is imposing new demands for OSS.

Traditionally, the OSS/BSS system is oriented to a reasonably static networking environment. However, in today's highly dynamic networking environment, The OSS/BSS system already needs some re-designing to adapt it to the dynamic nature of businesses. This is compounded by the need to provide the operational and business support of deploying services using software-defined infrastructure [152]. CSPs need to advance their OSS system to simplify and align with evolving software-defined infrastructure. Moreover, to control the dynamicity of NFV, new mechanisms to keep track of performance need an enhanced service assurance system to handle the dynamic nature of the NFV.

This service assurance system must be integrated with an OSS for two main reasons. First, to meet the service level agreements and second, to act as a tool to identify and manage network failure. In today's changing networking environments service assurance must be adaptive to fit well in order to meet the requirements of future heterogeneous networks. At present, there is a need to modernized legacy OSS/BSS system according to the NFV, and new evolving technologies introduce to achieve enhanced automation, scalability, capacity optimization and service elasticity in Software-defined infrstructure [153].

D. NFV MANAGEMENT AND ORCHESTRATION

Resource allocation in NFV is also a challenging problem. When talking about resource allocation concerning the NFV architectural framework, NFVI and NFV-MANO blocks are mainly responsible for provisioning resource allocation for VNFs, because VNFs are deployed on the NFVI and resources are allocated through orchestration. According to [34] resource allocation in NFV is accomplish in three stages as follows:

1) VNFs Chain Composition or SFC: SFC is the mechanisms to connect VNFs in such that they form a chain of service functions [130]. This enables flexibility for CSPs to make the best use of virtualized software to define infrastructure [123]. Moreover, it enables to compose a chain of VFNs dynamically.

TSPs can get the benefit from the composed dynamic chain of VNFs and develop elastic network services according to their business needs [36]. However, the main challenge arising while composing such chain is that how efficiently NFVI can be utilized to concatenate VNFs and control dynamicity.

2) VNFs Forwarding Graph Embedding: VNFs Forwarding Graph Embedding in NFV is a concept closely related to the Virtual Network Embedding (VNE) [44] and Virtual Data Center Embedding (VDCE) as described above [154].

A chain composed of VNFs is a connection of graphs to form end-to-end service. This end-to-end service is known as VNFs forwarding graph embedding.

3) VNFs Scheduling: VNFs are deployed using NFVI that comprised of several high volume servers. VNFs scheduling is the process of embedding VNFs in such a way to compose a chain of VNFs that minimize the total run time service execution. VNFs scheduling is carried out carefully without performance degradation and effecting high volume server in operating NFVI.

It is important to note that VNFs deployment architectures vary based on the implementation of NFVI functional block. Examples include VM, container-based and unikernels based deployments [155], [156]. A study carried out in [157] showed how NFV deployment practices could be optimized to achieve higher performance. Moreover, it also discusses how a carrier can fine-tune NFV deployment on standard high volume servers by applying embedded instrumentation techniques.

All the above stages of acquiring resource allocation in NFV requires efficient algorithms to determine the locations of required VNFs in high volume servers located in the data center. This then enables migration of servers from one location to another for efficient utilization of the NFVI. Further, this flexible placement of VNFs can offer load balancing, optimization of traffic flow, recovery from failures and possible reduction in CAPEX and OPEX [105]. Placement of VNFs is naturally challenging and particularly the different problem of how to optimized VNFs placement arises?

In order to improve the aspects of VNFs scalability dynamically for initial VNFs placement three mechanisms are discussed as follows: i) horizontal scaling: Virtualized resources are either added or removed, ii) vertical scaling: Virtualized resources capacity or size is reconfigured, and iii) Migration: Virtualized resources are migrated to appropriate location [37], [158].

Several studies have been carried out for the optimization of VNFs function placement [159], [160], [161], [162], [163]. These studies carried out multiple approaches as

the optimization problem is a Non-deterministic Polynomial Time (NP), NP-Hard problem. Work-done towards solving this NP-Hard problem followed heuristic and meta-heuristic algorithms to minimize the complexity in solving mixed integer linear programming models [164], [165], [166]. To improve the computation efficiency close to the optimal is challenging. There is a need to enhance the computation efficiency of resources in NFV so that better resource allocation can be achieved in NFV environment. The management and orchestration challenge is really a big concern for NFV success [13], [14], [120]. In an NFV environment, new management aspects of virtual VNFs have been introduced for creating and maintaining lifecycle management of the virtualized resources for the VNFs. This includes instantiation, scaling, updating and terminating VNFs [14]. Furthermore, function placement and dynamic resources allocation must be automated and self-configurable in NFV. Currently, this is an area of intense investigation and development for NFV.

From the NFVI management and orchestration aspect, the Network Point of Presence (N-PoP)(a location where network function is implemented as Virtual Network Function (VNF) or Physical Network Function (PNF)) and NFVI Point of Presence (NFVI-PoP) (N-PoP where network function can be deployed as VNF) [167] is essential, resources such as memory and storage are accessed from N-PoP and must be handled in NFVI-PoP. This helps to chain VNFs with other VNFs or Physical Network Functions (PNFs)(physical appliance) to realize a network service [13].

Currently, several active research projects are focusing on different aspects and challenges of management and orchestration; details are listed in Table 6. However, there are still open issues related to NFV management and orchestration.

VII. NFV SECURITY, PRIVACY AND TRUSTWORTHINESS

Virtualization, in general, brings forward many benefits and aspects of innovation. However, it imposes critical security, privacy, and trust issues. As compared to hardware-based solutions, security, privacy, and trust in software-based virtual environments can be compromised easier than in hardware. The abstracted view of the network due to virtualization means hard to keep track of information logs in the infrastructure owner domain. Virtual networks environments are also lacking clear control visibility and are hard to monitor properly. Due to this, sometimes internal traffic is not monitored properly by external security mechanisms [168]. Therefore, it is very challenging to devise strategies that guarantee security, privacy, and trust in a virtualized environment. The authors in [86] emphasized on the importance of security in a virtual environment and discussed how the virtual environment could not be shaped to meet security, privacy and trust requirements in an NFV environment while at the same time offering scalability and flexibility (as compared to typically offered in a telco environment).

To explain security, privacy and trust in NFV, we relate to Cloud computing with NFV for the sake of explaining and broaden the vision about these aspects in NFV. In [1] part of the NFV reference architecture is mapped to the Cloud service model. Moreover, the authors also argue that most of the implementation and testing for NFV PoC are based on the Cloud model, because Cloud computing platforms offer greater flexibility and cost benefits for NFV pre-deployment testing and implementation.

However, mapping NFV architectures to a Cloud-based model require carrier-class performance considerations for developing and delivering services over the Cloud. Indeed, security, privacy, and trust definitions differ depending on the Cloud deployment model (such as private, public, community, hybrid) and partners [169]. According to [170] there is no standard definition of privacy, trust, and security. Also, defining a relationship among them is hard. In [171], ETSI security specific group identified potential security vulnerabilities of NFV. It also discussed different deployment scenarios where these vulnerabilities can be defined. At last, they concluded that NFV creates new security concerns depending on the deployment scenarios.

To attain security accreditation of the systems and avoid several vulnerabilities in NFV deployments, ETSI proposed security and trust guidelines specific to NFV deployments scenarios [172], [173], authored by network operators, on NFV industry progress highlighted multi-administrator isolation as a key area of research in the security domain. The reason for this is that once administrator access to computing platform (NFVI) is given to someone, the internal of the virtualized system on the computing platform (NFVI) is exposed to errors and network security attacks. The Segregation of Duties (SoD) becomes difficult, especially when lawful interception (the content of the communications) is virtualized [47], [174].

Another issue is incorporating trust in each layer of NFV [175]. ETSI NFV-ISG security group also provides a guideline for third parties to verify the trust of the computing platform. This is known as external trust, and in a telecommunication Cloud environment, service providers need to verify the trustworthiness of a computing platform before launching VNFs [176].

VIII. IMPAIRMENTS TO COMMERCIAL NFV DEPLOYMENT

This section addresses some aspects that are obstructing the swift deployment of NFV in commercial environments.

A. LACK OF NFV EQUIPMENT'S/PRODUCTS TO MEET CARRIER-GRADE REQUIREMENTS

The major problem faced today's in NFV commercial deployment is the strict carrier-grade requirements [177]. The main reason for this for CSPs is to ensure a higher level of trustworthiness and service protection. Moreover, this enables CSPs to meet customer expectations for specific services and develop new business models for revenue generation. Indeed, the CGN services are incredibly reliable, tested, and

compatible. This is not only concerning meeting ''Five 9s'' of reliability and availability but also with other requirements for CGN such as equipment management, security, billing, product development, and continuous operational support [178].

The basic research challenge is moving to all IP-based technology, how can future NGNs fulfill the reliability, resilience and security requirements offered by traditional telecommunications networks (i.e., ''Five 9s'' reliability)?

The OPNFV project proposed reliability design goals for NFV, as listed in Table 5. Meeting the CGN criteria of ''Five 9s'' reliability is essential for NFV, but it is challenging considering a virtual environment (Software-based). NFV offers benefits of agility and automation of network services, but CSPs have not yet assured that NFV appliances/products are matured for CGN services. Therefore, NFV-based products/ equipment's must satisfy the ''Five 9s'' reliability criteria for CGN. The CSPs are concerned about it because the testing and validation of NFV products/ equipment's are still in their early stages.

B. INCOMPLETE STANDARDIZATION AND OPENNESS APPROACHES

In this paper, we have discussed in detail efforts for standardization and prominent NFV projects initiatives efforts to develop NFV for standardization. However, despite these efforts of academia and industry which showed continuous improvement of NFV development over the years, the NFV standardization is still underway. Indeed, a unified fabric for NFV and IT is not yet developed.

Although several examples of commercial NFV deployment exist, there is still a need to extend NFV deployments specifically to implement VNFs in multi-vendor virtual environments. The technological innovation of NFV continues to grow but standardization is considered a key factor for rolling out NFV in a large scale production environment, and at the moment there is a need to standardize all aspects of NFV to accelerate its deployment. Another barrier to NFV deployment is openness. Openness is one of the benefits that NFV aims to offer. However, openness promoted by several vendors or industry-specific solutions or open-source NFV projects does not necessarily follow approaches to offer openness that attracts uniform acceptance from CSPs and NFV promoted community. This issue of openness has also affected the financial picture of NFV.

C. INTEROPERABILITY AND PORTABILITY ISSUES

Interoperability and portability are also crucial issues holding back commercial NFV deployment. Portability refers to the support that an NFV framework aims to provide to move VNFs across a different server in multi-vendor, multi-service and multi-network virtual environment [179]. Interoperability in virtual environment refers to the software exchange of information among different NFV vendor appliances in a multi-vendor, multi-service, and multi-network virtual environment.

To scale product and services software portability is essential for porting VNFs and VMs with ease and without vendor lock-in. Also, portability enables integration in a multi-domain networking environment. However, designing a standard interface for portability is a challenge. Once the standard for portability is designed a standard unified approach for integration must be enabled to offer inter-operable orchestration in multi-vendor and multi-domain virtual environment [180].

D. LIMITED BUSINESS CASES FOR SERVICE PROVIDERS

There has been an ongoing discussion on the business end of NFV because there is a lack of killer applications for NFV and business cases are challenging to define [181]. Moreover, most of the service providers have not yet transformed their operational support systems to support NFV [182].

The virtualization benefits of NFV was not the only benefit that CSP's are interested. There are other benefits such as how NFV can optimized networks, offer value-added service and market agility. ETSI is in a liaison relationship with BB Forum to explore the business end of NFV. BB Forum is optimistic about NFV application for broadband users and believes that NFV can create new revenue streams to sustain business growth in the broadband market [183].

E. LACK OF CERTIFIED ECOSYSTEM FOR NFV

There is a need to develop NFV ecosystems and offer full solutions to CSP's to adapt NFV with confidence. However, building an ecosystem is hard. Currently, ETSI NFV PoC testing and validation is lacking behind [88]. CSP's need assurance from NFV ecosystems to offer simple installation and development of customer service and also automated network management built-in capabilities with seamless integration with other legacy system and multi-domain networking with SLA guaranteed.

IX. NFV FUTURE RESEARCH DIRECTIONS

Indeed, NFV has potential to grow significantly and eventually transform traditional proprietary-based network appliances to non-proprietary and open-standard based network and service deployments. This is going to shift the trend towards softwarization of telecommunications systems [184]. The purpose is to move network management functionalities closer to the software development; this brings three main advantages 1) Eases the network management for administrators. 2) Enables administrators to run automatic automation in the fail-over scenario. 3) Facilitates service providers to add new services on the fly without worrying about hardware compatibility issues. However, to obtain these benefits, NFV must support intelligent and programmability and network automation.

In this section, we outline the future directions for NFV development from the perspective of NFV role in intelligent programmable networks, including network programmability

and automation, the softwarization of telecommunications systems and finally integration of NFV with other technologies.

A. NETWORK SOFTWARIZATION: NETWORK PROGRAMMABILITY AND AUTOMATION

Traditionally, proprietary-based implementations can offer limited programmability support, which means that launching new network services for customers (i.e., service provisioning) is not only difficult but also time-consuming and requires specialized knowledge.

Network administrators manually configure network appliance interfaces, and it varies not only across different vendors but even with the same vendor for different products and services. The network administration process remained stable in the last decade because to deploy a network; the administrator would ultimately resort to the traditional per box configuration through Command Line Interface (CLI). This involved specialized manual human intervention to perform network management operations and slowed down development in network automation [185]. Network automation is a practice in which software automatically configure and test network devices to reduce human error, network operation cost and save time for troubleshooting a network.

Recently, SDN, NFV, and Cloud computing based technologies have evolved leading to the rise of software-driven networks. These software-driven networks are designed to innovate self-management mechanisms that lead towards the autonomic management of communications networks [186], [187].

Undoubtedly, the trend of programmability is changing the traditional way of customizing and managing the network to be more efficient with standardized APIs; development can support customized scripting through which configuration of various vendor equipment will become easier. This value addition through programmability offers a simpler environment for network administrators to automate network efficiency with minimum human intervention. This practice is known as network programmability [188]. The near future networks will be programmable, more organized and more controllable [189] and NFV is considered a key enabler to support such scenarios in the future paradigm.

Network softwarization (Netsoft) is a paradigm to enhanced the network programmability which leads to enhanced automation. The term Netsoft refers to the networking industry transformation for designing, deploying, implementing and maintaining network devices/ network elements through software programming. This enables flexibility to re-design network services to optimize cost and enable self-management capabilities to manage network infrastructure. Furthermore, this term ''Netsoft'' was first introduced at the academic conference Network softwarization in 2015, to include broader interests regarding NFV, SDN, network virtualization, Multi-access Edge Computing (MEC) formerly known as mobile edge computing, Cloud computing, and IoT technologies [190].

To sum up, NFV architecture must be designed to support the softwarization of telecommunications systems, and we believe that this is an important area for future NFV-related research.

B. INTEGRATION OF NFV WITH OTHER TECHNOLOGIES

Another important research direction for NFV is the integration of NFV with other technologies. Over the past years, integration of NFV with other technologies, such as SDN, Cloud computing, and 5G has attracted significant attention from both the academic research community and industry. These technologies have been proposed to fulfill different demands of future networks. Similarly, some of the studies also identified IoT, ICN [1], [10], MEC [191], [192], [193] fog computing [192], [194] and Cloud Radio Access Network (C-RAN) [195], [196] as a use case for NFV and discussed it in the perspective of future NFV research direction.

However, several challenges arise when integrating these technologies with NFV. Firstly, the standardization of these emerging technologies is underway, and therefore, at this stage, a time-resilient integration is quite challenging. Secondly, NFV commercial deployment is still at its early stages (as identified and discussed in section VIII), hence integrating NFV with other new technologies is naturally difficult. Finally, the dynamic and multi-domain nature of future networks imposes new security risks and threats. Addressing the security aspect while integrating NFV with other technologies is very challenging, specifically to ensure data privacy and trustworthiness between different network domains. In order to get the full benefit of NFV, the main integration challenges must be addressed appropriately before deployment.

NFV integration with SDN and Cloud computing is reasonably accepted due to the complementary features and distinctive approaches followed by each technology toward providing solutions to today's and future networks [197], [198]. For instance, NFV provides functions/service abstractions (i.e., virtualization of network functions) supported by ETSI [92], SDN provides network abstractions supported by Open Networking Foundation (ONF) [199] and Cloud computing provides computing abstraction (i.e., a shared pool of configurable storage resources) supported by the Distributed Management Task Force (DMTF) [200].

These technologies have distinct features and when combined can provide a technological platform which integrates and combine technological concepts to fulfill the needs of new business verticals (as handled in 5G networks). These three main technologies provide a complete abstraction solution for networking (network, computing, and storage). Therefore, the industry is looking forward to this integration and believes that the integration of these technologies will result in the creation of fully programmable networks [10].

SDN, NFV, and Cloud computing technologies complementary to each other but are independent and can be deployed alone or together. A combination of these

technologies together in a network architecture is more desirable [8]. Moreover, integrating NFV with these technologies adds value (flexibility and agility) to telecommunications systems. Furthermore, it will offer freedom to CSPs to create and manage network services without worrying about vendor-specific networking devices configuration. Thus, this integration of NFV with other technologies offers enhanced privileges to CSPs to set up network services almost effortlessly.

X. CONCLUSION

NFV has attracted significant interest from academia and the telecommunications industry as a technology that will potentially revolutionize network-based services with low deployment costs for network operators.

Virtualization approaches are paving the way for NFV from VMs, containers to more advanced techniques such as unikernels. We discussed Type I and Type II hypervisors: the selection of correct hypervisor is essential for the efficient utilization of underlying hardware as well as virtual environments.

NFV standardization efforts have evolved in the last few years, but the standardization is still underway. NFV applicability and PoCs are progressed and NFV becoming a key enabler of the 5G network slicing concept.

We discussed NFV requirements, design goals and key consideration that are essential to accelerate the deployment of NFV. We provide a detailed comparison of currently selected NFV projects to lead by industry and CSPs to explore the different aspects of the ETSI NFV framework. We also discussed the NFV architectural challenges and discussed ongoing research efforts to overcome those challenges, and identified the impairments that cause a delay in NFV commercial deployment.

NFV offers several potential significant advantages over present solutions available for CSPs, but at the same time several challenges need to be overcome soon through collaborative work on NFV to gain industry and CSPs confidence. This will play a pivotal role in propelling NFV deployments.

The NFV-based solution aims to offer service reliability comparable to the ''Five 9s'' reliability of PSTN. However, validation and testing to achieve Quality of Service (QoS) equivalent to PSTN is still an intense area of investigation.

NFV usage is overgrowing, and innovative ideas and practices are in progress although, its deployment is still at an early stage. The most important aspect to consider in NFV is testing and validation of hypothetical models [201]. There are also unexplored research areas in the NFV-based proposed solution. For instance, fault management, interoperability, E2E reliability, security performance which must be addressed in-depth. Furthermore, network automation is essential for improving NFV resilience.

NFV is a still evolving paradigm for programmable networks [202]. Softwarization of the telecommunications systems can provide a long-term solution to the gradual network ossification problem faced by the existing internet and NFV is an essential element directed towards a solution to this problem.

LIST OF ABBREVIATIONS/ACRONYMS

3GPP	3rd Generation Partnership Project
5G	Fifth-Generation
APIs	Application Programmable Interfaces
ARIB	Association of Radio Industries and Businesses
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BB-Forum	Broadband Forum
BRAS	Broadband Remote Access Server
BSS	Business Support System
CAPEX	Capital Expenditure
CCSA	China Communications Standards Association
CGN	Carrier-Grade Network
CLI	Command Line Interface
COTS	Commercial-Off-The-Shelf
CPE	Customer Premises Equipment
C-RAN	Cloud Radio Access Network
CSPs	Communication Service Providers
DevOps	Development and Operation
DPDKs	Data Plane Development Kits
E2E	End-to-End
EMS	Element Management System
EPC	Evolved Packet Core
ETSI	European Telecommunications Standardization Institute
FPGAs	Field-Programmable Gate Arrays
GSMA	Global System for Mobile Communications
HSS	Home Subscriber Server
ICN	Information-Centric Networking
ICTs	Information Communication Technologies
IEEE	Institute of Electrical and Electronics Engineering
IETF	Internet Engineering Task Force
IETF-SFC-WG	IETF Service Function Chaining Working Group
IMS	IP Multimedia Subsystem
IoT	Internet of Things
IRTF	Internet Research Task Force
ISG	Industry Specification Group
ISP	Internet Service Provider
ISPs	Internet Service providers
KPIs	Key Performance Indicators
KVM	Kernel Based Virtual Machine
LAN	Local Area Network
LTE	Long-term Evolution
LXC	Linux Containers
MAC	Medium Access Control
MAC	Medium Access Control

MEC	Multi-access Edge Computing
MEF	Metro Ethernet Forum
MME	Mobility Management Entity
NFs	Network Functions
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVI-PoP	NFVI Point of Presence
NFV-ISG	NFV Industry Specification Group
NFV-MANO	NFV Management and Orchestration
NFVO	NFV Orchestrator
NFVRG	NFV Research Group
NGDCN	Next-Generation Data Center Networking
NGNs	Next Generation Networks
NP	Non-deterministic Polynomial Time
N-PoP	Network Point of Presence
NS	Network Service
NV	Network Virtualization
NVE	Network Virtualization Edge
OCI	Open Container Initiative
OPENSIG	Open Signaling
OPEX	Operational Expenses
OS	Operating System
OSI	Open System Interconnection
OSS	Operation Support System
PCRF	Policy and Charging Rules Function
P-GW	Packet Data Network Gateway
PNFs	Physical Network Functions
PoC	Proof of Concept
PSTN	Public Switched Telephone Network
REST	Representational State Transfer
RHEV	Red Hat Enterprise Virtualization
SDN	Software-Defined Networking
SDO	Standard Development Organization
SFC	Service Function Chaining
S-GW	Serving Gateway
SLAs	Service Level Agreements
TIA	Telecommunications Industry Association
TM-Forum	Tele Management Forum
TSG-SA	Technical Specification Group Service System Aspects
TSPs	Telecommunication Service Providers
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
vCDN	Content Delivery Network
vCPE	Virtual Customer Premises Equipment
vEPC	Virtual Evolved Packet Core
VLANs	Virtual Local Area Networks
VM	Virtual Machine
VMM	Virtual Machine Manager
VN	Virtual Network
VNFs	Virtual Network Functions
VPNs	Virtual Private Networks
VXLAN	Virtual eXtensible Local Area Network

REFERENCES

[1] R. Mijumbi *et al.*, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.

[2] D. Kreutz, F. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[3] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: A survey," *IEEE Commun. Mag.*, vol. 51, no. 11, pp. 24–31, Nov. 2013.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[5] G. Xylomenos *et al.*, "A survey of information-centric networking research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, 2nd Quart., 2014.

[6] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, Mar. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874490715000531

[7] C. Marcondes and C. E. Rothenberg. (May 2015). *Tutorial 2: Network functions virtualization NFV—Perspectives, Reality and Challenges*. [Online]. Available: http://www.dca.fee.unicamp.br/~chesteve/ppt/NFV-Full-IM15-Final-Screen-v150412.pdf

[8] Y. Li and M. Chen, "Software-defined network function virtualization: A survey," *IEEE Access*, vol. 3, pp. 2542–2553, 2015.

[9] Z. A. Qazi, C.-C. Tu, L. Chiang, R. Miao, V. Sekar, and M. Yu, "SIMPLE-fying middlebox policy enforcement using SDN," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 27–38, 2013. doi: 10.1145/2534169.2486022.

[10] B. Yi, X. Wang, S. K. Das, K. Li, and M. Huang, "A comprehensive survey of network function virtualization," *Comput. Netw.*, vol. 133, pp. 212–262, Mar. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618300306

[11] P. Wang, J. Lan, X. Zhang, Y. Hu, and S. Chen, "Dynamic function composition for network service chain," *Comput. Netw.*, vol. 92, no. P2, pp. 408–418, Dec. 2015. doi: 10.1016/j.comnet.2015.07.020.

[12] *What is ETSI ISG NFV? SDX Central*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.sdxcentral.com/nfv/definitions/etsi-isg-nfv/

[13] R. Mijumbi, J. Serrat, J.-L. Gorricho, S. Latré, M. Charalambides, and D. Lopez, "Management and orchestration challenges in network functions virtualization," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 98–105, Jan. 2016.

[14] *Network Functions Virtualisation (NFV); Management Orchestration*, document DGS/NFV-MAN001, ETSI GS NFV 001 V1.1.1, ETSI (ISG), Sophia-Antipolis, France, Dec. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf

[15] Technical Overview. *Open Platform for NFV (OPNFV)*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.opnfv.org/software/technical-overview

[16] P. Calif. (Dec. 2015). *Hewlett Packard Enterprise OpenNFV Solution Portal Brings Telcos Closer to Realizing NFV Benefits*. Accessed: Mar. 21, 2019. [Online]. Available: https://www8.hp.com/us/en/hp-news/press-release.html?id=2136079#.Wh3lxdJl82w

[17] Y. Demchenko *et al.*, "Enabling automated network services provisioning for cloud based applications using zero touch provisioning," in *Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Comput. (UCC)*, Dec. 2015, pp. 458–464.

[18] J. Martins *et al.*, "Clickos and the art of network function virtualization," in *Proc. 11th USENIX Conf. Netw. Syst. Design Implement.*, 2014, pp. 459–473.

[19] C. J. Bernardos, B. P. Gerö, M. Di Girolamo, A. Kern, B. Martini, and I. Vaishnavi, "5GEx: Realising a Europe-wide multi-domain framework for software-defined infrastructures," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 9, pp. 1271–1280, 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3085

[20] 3rd Generation Partnership Project (3GPP). *About 3GPP Home*. Accessed: Mar. 21, 2019. [Online]. Available: http://www.3gpp.org/about-3gpp/about-3gpp

[21] *Network Functions Virtualisation (NFV); Architectural Framework*, document RGS/NFV-002, ETSI GS NFV 002 V1.2.1, ETSI (ISG), Sophia-Antipolis, France, Dec. 2014. [Online]. Available: https://docbox.etsi.org/ISG/NFV/open/Publications_pdf/Specs-Reports/NFV%20002v1.2.1%20-%20GS%20-%20NFV%20Architectural%20Framework.pdf

[22] *Network Functions Virtualisation (NFV); Architectural Framework*, document DGS/NFV-0010, ETSI GS NFV 002 V1.1.1, ETSI (ISG), Sophia-Antipolis, France, Oct. 2013. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf

[23] M. Veeraraghavan, T. Sato, M. Buchanan, R. Rahimi, S. Okamoto, and N. Yamanaka, "Network function virtualization: A survey," *IEICE Trans. Commun.*, vol. E100.B, no. 11, pp. 1978–1991, 2017.

[24] R. Muñoz *et al.*, "SDN/NFV orchestration for dynamic deployment of virtual SDN controllers as VNF for multi-tenant optical networks," in *Proc. Opt. Fiber Commun. Conf.*, 2015, pp. 1–3, Paper W4J.5. [Online]. Available: http://www.osapublishing.org/abstract.cfm?URI=OFC-2015-W4J.5

[25] R. Nejabati, S. Peng, M. Channegowda, B. Guo, and D. Simeonidou, "SDN and NFV convergence a technology enabler for abstracting and virtualising hardware and control of optical networks (invited)," in *Proc. Opt. Fiber Commun. Conf.*, 2015, pp. 1–3, Paper W4J.6. [Online]. Available: http://www.osapublishing.org/abstract.cfm?URI=OFC-2015-W4J.6

[26] N. Omnes, M. Bouillon, G. Fromentoux, and O. L. Grand, "A programmable and virtualized network and it infrastructure for the Internet of Things: How can NFV and SDN help for facing the upcoming challenges," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw.*, Feb. 2015, pp. 64–69.

[27] F. Yang, H. Wang, C. Mei, J. Zhang, and M. Wang, "A flexible three clouds 5G mobile network architecture based on NFV and SDN," *China Commun.*, vol. 12, pp. 121–131, Dec. 2015.

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

[29] I. F. Akyildiz, S.-C. Lin, and P. Wang, "Wireless software-defined networks (W-SDNs) and network function virtualization (NFV) for 5G cellular systems: An overview and qualitative evaluation," *Comput. Netw.*, vol. 93, pp. 66–79, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128615003862

[30] E. Haleplidis *et al.*, "Forces applicability to SDN-enhanced NFV," in *Proc. 3rd Eur. Workshop Softw. Defined Netw.*, Sep. 2014, pp. 43–48.

[31] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, "Toward an SDN-enabled NFV architecture," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 187–193, Apr. 2015.

[32] W. Ding, W. Qi, J. Wang, and B. Chen, "OpenSCaaS: An open service chain as a service platform toward the integration of SDN and NFV," *IEEE Netw.*, vol. 29, no. 3, pp. 30–35, May 2015.

[33] B. Wang, Z. Qi, R. Ma, H. Guan, and A. V. Vasilakos, "A survey on data center networking for cloud computing," *Comput. Netw.*, vol. 91, pp. 528–547, Nov. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861500300

[34] J. G. Herrera and J. F. Botero, "Resource allocation in NFV: A comprehensive survey," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 3, pp. 518–532, Sep. 2016.

[35] M. F. Bari, S. R. Chowdhury, R. Ahmed, and R. Boutaba, "On orchestrating virtual network functions," in *Proc. 11th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2015, pp. 50–56.

[36] R. Szabo, M. Kind, F. J. Westphal, H. Woesner, D. Jocha, and A. Csaszar, "Elastic network functions: Opportunities and challenges," *IEEE Netw.*, vol. 29, no. 3, pp. 15–21, May 2015.

[37] M. Ghaznavi *et al.*, "Elastic virtual network function placement," in *Proc. IEEE CloudNet*, Oct. 2015, pp. 255–260.

[38] A. Laghrissi and T. Taleb, "A survey on the placement of virtual resources and virtual network functions," *IEEE Commun. Surveys Tuts.*, to be published.

[39] J. F. Riera, E. Escalona, J. Batallé, E. Grasa, and J. A. García-Espín, "Virtual network function scheduling: Concept and challenges," in *Proc. Int. Conf. Smart Commun. Netw. Technol. (SaCoNeT)*, Jun. 2014, pp. 1–5.

[40] M. Shifrin, E. Biton, and O. Gurewitz, "Optimal control of VNF deployment and scheduling," in *Proc. IEEE Int. Conf. Sci. Elect. Eng. (ICSEE)*, Nov. 2016, pp. 1–5.

[41] V. Eramo, E. Miucci, M. Ammar, and F. G. Lavacca, "An approach for service function chain routing and virtual function network instance migration in network function virtualization architectures," *IEEE/ACM Trans. Netw.*, vol. 25, no. 4, pp. 2008–2025, Aug. 2017.

[42] J. Xia, Z. Cai, and M. Xu, "Optimized virtual network functions migration for NFV," in *Proc. IEEE 22nd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2016, pp. 340–346.

[43] S. Clayman, E. Maini, A. Galis, A. Manzalini, and N. Mazzocca, "The dynamic placement of virtual network functions," in *Proc. IEEE Netw. Oper. Manage. Symp. (NOMS)*, May 2014, pp. 1–9.

[44] A. Fischer, J. F. Botero, M. T. Beck, H. de Meer, and X. Hesselbach, "Virtual network embedding: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1888–1906, 4th Quart., 2013.

[45] W. Yang and C. Fung, "A survey on security in network functions virtualization," in *Proc. IEEE NetSoft Conf. Workshops (NetSoft)*, Jun. 2016, pp. 15–19.

[46] M. D. Firoozjaei, J. P. Jeong, H. Ko, and H. Kim, "Security challenges with network functions virtualization," *Future Gener. Comput. Syst.*, vol. 67, pp. 315–324, Feb. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16302321

[47] 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. Surveys Tuts.*, vol. 20, no. 4, pp. 3330–3368, 4th Quart., 2018.

[48] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, "Network function virtualization in 5G," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 84–91, Apr. 2016.

[49] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

[50] IBM Corporation. (2012). *z/VM—A Brief Review of Its 40 Year History*. [Online]. Available: http://www.vm.ibm.com/vm40hist.pdf

[51] RedHat Corporation. *Understanding Virtualization*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.redhat.com/en/topics/virtualization

[52] J. E. van der Merwe, S. Rooney, L. Leslie, and S. Crosby, "The tempest—A practical framework for network programmability," *IEEE Netw.*, vol. 12, no. 3, pp. 20–28, May 1998.

[53] M. R. Macedonia and D. P. Brutzman, "MBone provides audio and video across the Internet," *Computer*, vol. 27, no. 4, pp. 30–36, Apr. 1994.

[54] R. Hinden and J. Postel, *IPV6 Testing Address Allocation. Internet Engineering Task Force*, document RFC 1897 and RFC 2471, Jan. 1996.

[55] J. Touch, "Dynamic Internet overlay deployment and management using the X-bone," *Comput. Netw.*, vol. 36, no. 2, pp. 117–135, 2001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128601001724

[56] B. Chun *et al.*, "PlanetLab: An overlay testbed for broad-coverage services," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 3, pp. 3–12, Jul. 2003.

[57] L. Peterson *et al.*, "Geni design principles," *Computer*, vol. 39, no. 9, pp. 102–105, Sep. 2006.

[58] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: Realistic and controlled network experimentation," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 4, pp. 3–14, 2006.

[59] Y. Zhang, *Network Function Virtualization*, 1st ed. Hoboken, NJ, USA: Wiley, 2018, pp. 22–36.

[60] *IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks*, IEEE Standard 802.1Q-2014 (Revision IEEE Standard 802.1Q-2011), Dec. 2014, pp. 1–1832.

[61] D. McPherson and B. Dykes, *VLAN Aggregation for Efficient IP Address Allocation*, document RFC 3069, Internet Requests for Comments, RFC Editor, Feb. 2001. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc3069.txt.pdf

[62] V. Moreno and K. Reddy, *Network Virtualization*, 1st ed. Indianapolis, IN, USA: Cisco Press, 2006, pp. 35–53.

[63] M. Mahalingam *et al.*, *Virtual Extensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks Over Layer 3 Networks*, document RFC 7348, Internet Requests for Comments, RFC Editor, Aug. 2014. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc7348.txt.pdf

[64] R. K. Sitaraman, M. Kasbekar, W. Lichtenstein, and M. Jain, *Overlay Networks: An Akamai Perspective*. Hoboken, NJ, USA: Wiley, 2014, ch. 16, pp. 305–328. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118909690.ch16

[65] M. Napierala, L. Kreeger, T. Narten, D. Black, L. Fang, and E. Gray, *Problem Statement: Overlays for Network Virtualization*, document RFC 7364, Internet Requests for Comments, RFC Editor, Oct. 2014. [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc7364.txt.pdf

[66] M. Chiosi *et al.*, "Network functions virtualisation: An introduction, benefits, enablers, challenges and call for action," in *Proc. SDN OpenFlow World Congr.*, vol. 48, 2012, p. 2224.

[67] J. Doherty, *SDN and NFV Simplified: A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization*, 1st ed. USA, Reading, MA, USA: Addison-Wesley, 2016, pp. 3–34.

[68] VMware. *What is Virtual Machine*. Accessed: Mar. 21, 2019. [Online]. Available: https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-CEFF6D89-8C19-4143-8C26-4B6D6734D2CB.html

[69] R. Chayapathi, S. F. Hassan, and P. Shah, *Network Functions Virtualization (NFV) with a Touch of SDN: Netw Fun Vir*, 1st ed. Reading, MA, USA: Addison-Wesley, 2016, pp. 37–62.

[70] IBM. *Learn About Hypervisors, System Virtualization, and How it Works in a Cloud Environment*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.ibm.com/developerworks/cloud/library/cl-hypervisorcompare/

[71] H. Lee, "Virtualization basics: Understanding techniques and fundamentals," School Inform. Comput., Indiana Univ., Bloomington, IN, USA, 2014, vol. 815. Accessed: Mar. 21, 2019. [Online]. Available: http://dsc.soic.indiana.edu/publications/virtualization.pdf

[72] P. Matthew, *Virtualization Essentials*, 2nd ed. Hoboken, NJ, USA: Sybex, 2016, pp. 21–36.

[73] W. Felter, A. Ferreira, R. Rajamony, and J. Rubio, "An updated performance comparison of virtual machines and Linux containers," in *Proc. IEEE Int. Symp. Perform. Anal. Syst. Softw.*, Philadelphia, PA, USA, Mar. 2015, pp. 171–172.

[74] P. S. V. Indukuri, "Performance comparison of linux containers (LXC) and OpenVZ during live migration an experiment," master's dissertation, Blekinge Inst. Technol., Karlskrona, Sweden, 2016.

[75] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017.

[76] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.

[77] *Unikernels*. Accessed: Mar. 21, 2019. [Online]. Available: https://wiki.xenproject.org/wiki/Unikernels

[78] A. Madhavapeddy *et al.*, "Unikernels: Library operating systems for the cloud," *SIGPLAN Notes*, vol. 48, no. 4, pp. 461–472, Mar. 2013. doi: 10.1145/2499368.2451167.

[79] M. J. De Lucia, "A survey on security isolation of virtualization, containers, and unikernels," U.S. Army Res. Laboratory, Aberdeen Proving Ground, MD, USA, USA, Tech. Rep., 2017.

[80] *What is a container*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.docker.com/resources/what-container

[81] *Projects Open Source Work on Unikernels*. Accessed: Mar. 21, 2019. [Online]. Available: http://unikernel.org/projects/

[82] P. Enberg, "A performance evaluation of hypervisor, unikernel, and container network i/o virtualization," master's dissertation, Dept. Comput. Sci., Univ. Helsinki, Helsinki, Finland, 2016.

[83] N. Operators, "Network functions virtualization, an introduction, benefits, enablers, challenges and call for action," in *Proc. SDN OpenFlow SDN OpenFlow World Congr.*, 2012.

[84] ETSI. *Network Functions Virtualisation*. Accessed: Mar. 21, 2019. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/nfv

[85] ETSI. *Network Functions Virtualisation Completes First Phase of Work*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.etsi.org/news-events/news/864-2015-01-press-etsi-network-functions-virtualisation

[86] K. Gray and T. D. Nadeau, *Network Function Virtualization*, 1st ed. San Mateo, CA, USA: Morgan Kaufmann, 2016, pp. 49–76.

[87] SDx Central. *2018 NFV Report Series Part 2: MANO, LSO & Assurance: State VNF Ecosystem*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.sdxcentral.com/reports/next-gen-data-center-networking-download-2018/

[88] ETSI. *NFV Proofs Concept*. Accessed: Mar. 21, 2019. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/nfv/nfv-poc

[89] W. Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*, 1st ed. Reading, MA, USA: Addison-Wesley, 2015, pp. 175–220.

[90] *Network Functions Virtualisation (NFV); Architectural Framework*, document DGS/NFV-0010, ETSI GS NFV 003 V1.3.1, ETSI (ISG), Sophia-Antipolis, France, Jan. 2018. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/003/01.03.01_60/gs_nfv003v010301p.pdf

[91] P. Krish and D. John, *Building the Network of the Future*, 1st ed. Boca Raton, FL, USA: CRC Press, 2017, pp. 49–66.

[92] ETSI. *Network Functions Virtualisation (NFV)*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.etsi.org/technologies-clusters/technologies/nfv

[93] IRTF. *Internet Research Task Force*. Accessed: Mar. 21, 2019. [Online]. Available: https://irtf.org/

[94] D. Lopez and R. Krishnan, "The NFVRG network function virtualization research at the IRTF," *J. ICT Standardization*, vol. 3, no. 1, pp. 57–66, 2015.

[95] IETF. *Network Function Virtualization Resesarch Group (NFVRG)*. Accessed: Mar. 21, 2019. [Online]. Available: https://datatracker.ietf.org/rg/nfvrg/about/

[96] IETF. *Network Function Virtualization Research Group (NFVRG)*. Accessed: Mar. 21, 2019. [Online]. Available: https://irtf.org/concluded/nfvrg

[97] IETF. *Service Function Chaining (SFC)*. Accessed: Mar. 21, 2019. [Online]. Available: https://datatracker.ietf.org/wg/sfc/about/

[98] ATIS Overview. ATIS, Washington, DC, USA, 2019. [Online]. Available: https://sites.atis.org/wp-content/uploads/2019/02/ATIS-Overview-2019.pdf

[99] *About BBF*, Fremont, CA, USA, Accessed: Mar. 21, 2019. [Online]. Available: https://www.broadband-forum.org/about-bbf

[100] 3rd Generation Partnership Project (3GPP). *Management of Mobile Networks that Include Virtualized Network Functions (MANO)*. Accessed: Mar. 21, 2019. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1738-sa5_nfv_study

[101] *Network Functions Virtualisation (NFV); Use Cases*, document DGS/NFV-009, ETSI GS NFV 001 V1.1.1, ETSI (ISG), Sophia-Antipolis, France, Oct. 2013. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

[102] *Network Functions Virtualisation (NFV); Use Cases*, ETSI (ISG), document RGR/NFV-001ed121, ETSI GR NFV 001 V1.2.1, Sophia-Antipolis, France, May 2017. [Online]. Available: https://docbox.etsi.org/ISG/NFV/open/Publications_pdf/Specs-Reports/NFV%20001%20v1.2.1%20-%20GR%20-%20NFV%20Use%20Cases%20revision.pdf

[103] S. K. N. Rao, "SDN and its use-cases-NV and NFV a state-of-the-art survey," Semantic Scholar, NEC Technol., Chennai, India, White Paper, 2014. Accessed: Mar. 21, 2019. [Online]. Available: https://in.nec.com/en_IN/pdf/NTI_whitepaper_SDN_NFV.pdf

[104] Z. Bronstein and E. Shraga, "NFV virtualisation of the home environment," in *Proc. IEEE 11th Consumer Commun. Netw. Conf. (CCNC)*, Jan. 2014, pp. 899–904.

[105] E. Hernandez-Valencia, S. Izzo, and B. Polonsky, "How will NFV/SDN transform service provider Opex?" *IEEE Netw.*, vol. 29, no. 3, pp. 60–67, May 2015.

[106] F. Firmin. *The Evolved Packet Core*. Accessed: Mar. 21, 2019. [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

[107] *Open Platform For NFV (OPNFV)*. Accessed: Mar. 21, 2019. [Online]. Available: https://wiki.opnfv.org/

[108] *Zoom Project*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.tmforum.org/collaboration/zoom-project/

[109] *Clickos Fast and Lightweight Network Functions Virtualization*. Accessed: Mar. 21, 2019. [Online]. Available: http://cnp.neclab.eu/projects/clickos/

[110] *NFV Orchestration*. Accessed: Mar. 21, 2019. [Online]. Available: http://www.blueplanet.com/products/nfv-orchestration.html

[111] A. Sgambelluri *et al.*, "Orchestration of network services across multiple operators: The 5G exchange prototype," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2017, pp. 1–5.
[112] *Apache ARIA TOSCA Orchestration Engine*. Accessed: Mar. 21, 2019. [Online]. Available: http://ariatosca.incubator.apache.org/
[113] *Telco Self Service—Accelerated With Orchestration*. Accessed: Mar. 21, 2019. [Online]. Available: https://cloudify.co/nfv/
[114] *Micro Services in a Minute Simple and Unified Cloud Service Architecture*. Accessed: Mar. 21, 2019. [Online]. Available: http://gohan.cloudwan.io/
[115] *Production-Grade Container Orchestration*. Accessed: Mar. 21, 2019. [Online]. Available: https://kubernetes.io/
[116] *What is OSM*. Accessed: Mar. 21, 2019. [Online]. Available: https://osm.etsi.org/
[117] *Open Baton An Extensible And Customizable NFV Mano-Compliant Framework*. Accessed: Mar. 21, 2019. [Online]. Available: http://openbaton.github.io/
[118] *About Sonata*. Accessed: Mar. 21, 2019. [Online]. Available: http://sonata-nfv.eu/content/about-sonata
[119] *Tacker Openstack NFV Orchestration*. Accessed: Mar. 21, 2019. [Online]. Available: https://wiki.openstack.org/wiki/Tacker
[120] K. Katsalis, N. Nikaein, and A. Edmonds, "Multi-domain orchestration for NFV: Challenges and research directions," in *Proc. 15th Int. Conf. Ubiquitous Comput. Commun. Int. Symp. Cyberspace Secur. (IUCC-CSS)*, Dec. 2016, pp. 189–195.
[121] C. Tipantuña and P. Yanchapaxi, "Network functions virtualization: An overview and open-source projects," in *Proc. IEEE 2nd Ecuador Tech. Chapters Meeting (ETCM)*, Oct. 2017, pp. 1–6.
[122] B. Naudts, W. Tavernier, S. Verbrugge, D. Colle, and M. Pickavet, "Deploying SDN and NFV at the speed of innovation: toward a new bond between standards development organizations, industry fora, and open-source software projects," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 46–53, Mar. 2016.
[123] D. Bhamare, R. Jain, M. Samaka, and A. Erbad, "A survey on service function chaining," *J. Netw. Comput. Appl.*, vol. 75, pp. 138–155, Nov. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S108480451630198
[124] G. Arfaoui, J. M. S. Vilchez, and J. P. Wary, "Security and resilience in 5G: Current challenges and future directions," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 1010–1015.
[125] P. Lynch, M. Haugh, L. Kurtz, and J. Zeto, *Demystifying NFV in Carrier Networks*, 1st ed. Calabasas, CA, USA: Ixia, 2014, pp. 53–58.
[126] L. Nobach and D. Hausheer, "Open, elastic provisioning of hardware acceleration in NFV environments," in *Proc. Int. Conf. Workshops Netw. Syst. (NetSys)*, Mar. 2015, pp. 1–5.
[127] J. DiGiglio and D. Ricci, "High performance, open standard virtualization with NFV and SDN," Intel Corporation Wind River, White Paper, 2013.
[128] X. Ge *et al.*, "OpenANFV: Accelerating network function virtualization with a consolidated framework in openstack," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 353–354, 2014.
[129] *Network Functions Virtualisation (NFV);Reliability; Report on Models and Features for End-to-End Reliability*, document DGS/NFV-REL003, ETSI GS NFV-REL 003 V1.1.1, ETSI (ISG), Sophia-Antipolis, France, Apr. 2016. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/003/01.01.01_60/gs_nfv-rel003v010101p.pdf
[130] V. A. Cunha, I. D. Cardoso, J. P. Barraca, and R. L. Aguiar, "Policy-driven vCPE through dynamic network service function chaining," in *Proc. IEEE NetSoft Conf. Workshops (NetSoft)*, Jun. 2016, pp. 156–160.
[131] A. M. Medhat, T. Taleb, A. Elmangoush, G. A. Carella, S. Covaci, and T. Magedanz, "Service function chaining in next generation networks: State of the art and research challenges," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 216–223, Feb. 2017.
[132] *Network Functions Virtualisation (NFV);Reliability; Report on Models and Features for End-to-End Reliability*, document RGS/NFV-REL003ed112, ETSI GS NFV-REL 003 V1.1.2, ETSI (ISG), Sophia-Antipolis, France, Jul. 2016. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/003/01.01.02_60/gs_nfv-rel003v010102p.pdf
[133] H. Pang. *Reliability Testing in OPNFV*, Huawei, San Fransico, CA, USA. Accessed: Mar. 21, 2019. [Online]. Available: https://www.slideshare.net/OPNFV/reliability-testing-in-opnfv
[134] S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211–217, Aug. 2017.
[135] L. Jacquin, A. Lioy, D. R. Lopez, A. L. Shaw, and T. Su, "The trust problem in modern network infrastructures," in *Cyber Security and Privacy*, F. Cleary and M. Felici, Eds. Cham, Switzerland: Springer, 2015, pp. 116–127.
[136] *Security Considerations for Network Functions Virtualization for Communications Service Providers*, Intel Corp., Santa Clara, CA, USA, Oct. 2016. [Online]. Available: https://builders.intel.com/docs/networkbuilders/security_considerations_for_network_functions_virtualization_for_communications_service_providers.pdf
[137] M. Pearce, S. Zeadally, and R. Hunt, "Virtualization: Issues, security threats, and solutions," *ACM Comput. Surv.*, vol. 45, no. 2, pp. 17:1–17:39, Mar. 2013. doi: 10.1145/2431211.2431216.
[138] T. Taleb *et al.*, "EASE: EPC as a service to ease mobile core network deployment over cloud," *IEEE Netw. Mag.*, vol. 29, no. 2, pp. 78–88, Mar. 2015.
[139] C. Wang, O. Spatscheck, V. Gopalakrishnan, Y. Xu, and D. Applegate, "Toward high-performance and scalable network functions virtualization," *IEEE Internet Comput.*, vol. 20, no. 6, pp. 10–20, Nov. 2016.
[140] W. Van Heddeghem, S. Lambert, B. Lannoo, D. Colle, M. Pickavet, and P. Demeester, "Trends in worldwide ICT electricity consumption from 2007 to 2012," *Comput. Commun.*, vol. 50, pp. 64–76, Sep. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366414000619
[141] A. Fehske, G. Fettweis, J. Malmodin, and G. Biczok, "The global footprint of mobile communications: The ecological and economic perspective," *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 55–62, Aug. 2011.
[142] W. Vereecken, W. V. Heddeghem, D. Colle, M. Pickavet, and P. Demeester, "Overall ICT footprint and green communication technologies," in *Proc. 4th Int. Symp. Commun., Control Signal Process. (ISCCSP)*, Mar. 2010, pp. 1–6.
[143] W. V. Heddeghem, W. Vereecken, D. Colle, M. Pickavet, and P. Demeester, "Distributed computing for carbon footprint reduction by exploiting low-footprint energy availability," *Future Gener. Comput. Syst.*, vol. 28, no. 2, pp. 405–414, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X11000859
[144] A. P. Bianzino, C. Chaudet, D. Rossi, and J.-L. Rougier, "A survey of green networking research," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 1, pp. 3–20, 1st Quart., 2012.
[145] *Network Functions Virtualisation (NFV);Infrastructure; Hypervisor Domain*, document ETSI GS NFV-INF 004 V1.1.1, DGS/NFV-INF004, ETSI (ISG), Sophia-Antipolis, France, Jan. 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/004/01.01.01_60/gs_nfv-inf004v010101p.pdf
[146] Z. Xu, F. Liu, T. Wang, and H. Xu, "Demystifying the energy efficiency of network function virtualization," in *Proc. IEEE/ACM 24th Int. Symp. Qual. Service (IWQoS)*, Jun. 2016, pp. 1–10.
[147] R. Krishnan, T. Hinrichs, D. Krishnawamy, and R. Krishnaswamy, "Policy-based monitoring and energy management for NFV data centers," in *Proc. Int. Conf. Comput. Netw. Commun. (CoCoNet)*, Dec. 2015, pp. 10–17.
[148] R. Bolla, C. Lombardo, R. Bruschi, and S. Mangialardi, "DROPv2: Energy efficiency through network function virtualization," *IEEE Netw.*, vol. 28, no. 2, pp. 26–32, Mar. 2014.
[149] *Network Functions Virtualisation (NFVs); NFV Performance & Portability Best Practises*, ETSI (ISG), ETSI GS NFV-PER 001 V1.1.1, DGS/NFV-PER001, Sophia-Antipolis, France, Jun. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-PER/001_099/001/01.01.01_60/gs_nfv-per001v010101p.pdf
[150] *Network Functions Virtualisation (NFV); NFV Performance & Portability Best Practises*, document RGS/NFV-PER001ed112, ETSI GS NFV-PER 001 V1.1.2, ETSI (ISG), Sophia-Antipolis, France, Dec. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-PER/001_099/001/01.01.02_60/gs_nfv-per001v010102p.pdf
[151] *Hardware Acceleration for Network Services*, Netronome Syst., Inc., WP-HW-ACCERELATION-NS-1/2017, Santa Clara, CA, USA, 2017. [Online]. Available: https://www.netronome.com/media/documents/WP_Hardware_Acceleration.pdf
[152] Manage the Future Now. Hewlett-Packard Development Company, Jan. 2015. [Online]. Available: http://www.5gamericas.org/files/6414/3274/6235/White-Paper-Transforming-OSS-for-NFV.pdf

[153] *Operational Opportunities and Challenges of SDN/NFV Programmable Infrastructure*, ATIS, Washington, DC, USA, Oct. 2013. [Online]. Available: https://access.atis.org/apps/group_public/download.php/20398/Operational%20Opportunities.pdf

[154] M. G. Rabbani, R. P. Esteves, M. Podlesny, G. Simon, L. Z. Granville, and R. Boutaba, "On tackling virtual data center embedding problem," in *Proc. Integr. Netw. Manage. (IM)*, May 2013, pp. 177–184.

[155] M. Falkner, A. Leivadeas, I. Lambadaris, and G. Kesidis, "Performance analysis of virtualized network functions on virtualized systems architectures," in *Proc. IEEE 21st Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Oct. 2016, pp. 71–76.

[156] J. Anderson, H. Hu, U. Agarwal, C. Lowery, H. Li, and A. Apon, "Performance considerations of network functions virtualization using containers," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2016, pp. 1–7.

[157] P. Veitch, M. J. McGrath, and V. Bayon, "An instrumentation and analytics framework for optimal and robust NFV deployment," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 126–133, Feb. 2015.

[158] G. Galante and L. C. E. D. Bona, "A survey on cloud computing elasticity," in *Proc. IEEE 5th Int. Conf. Utility Cloud Comput. (UCC)*, Nov. 2012, pp. 263–270.

[159] H. Moens and F. De Turck, "VNF-P: A model for efficient placement of virtualized network functions," in *Proc. 10th Int. Conf. Netw. Service Manage. (CNSM)*, 2014, pp. 418–423.

[160] M. Bagaa, T. Taleb, and A. Ksentini, "Service-aware network function placement for efficient traffic handling in carrier cloud," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Istanbul, Turkey, Apr. 2014, pp. 2402–2407.

[161] S. Mehraghdam, M. Keller, and H. Karl, "Specifying and placing chains of virtual network functions," in *Proc. IEEE 3rd Int. Conf. Cloud Netw. (CloudNet)*, Oct. 2014, pp. 7–13.

[162] M. Bouet, J. Leguay, and V. Conan, "Cost-based placement of vDPI functions in NFV infrastructures," in *Proc. Netw. Softw.*, Apr. 2015, pp. 1–9.

[163] O. Houidi, O. Soualah, W. Louati, M. Mechtri, D. Zeghlache, and F. Kamoun, "An efficient algorithm for virtual network function scaling," in *Proc. IEEE Global Commun. Conf. GLOBECOM*, Dec. 2017, pp. 1–7.

[164] M. Yoshida, W. Shen, T. Kawabata, K. Minato, and W. Imajuku, "MORSA: A multi-objective resource scheduling algorithm for NFV infrastructure," in *Proc. 16th APNOMS*, Sep. 2014, pp. 1–6.

[165] M. C. Luizelli, L. R. Bays, L. S. Buriol, M. P. Barcellos, and L. P. Gaspary, "Piecing together the NFV provisioning puzzle: Efficient placement and chaining of virtual network functions," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 98–106.

[166] B. Addis, D. Belabed, M. Bouet, and S. Secci, "Virtual network functions placement and routing optimization," in *Proc. IEEE 4th Int. Conf. Cloud Netw. (CloudNet)*, Oct. 2015, pp. 171–177.

[167] *Network Functions Virtualisation (NFV); Terminology for Main Concepts NFV*, document RGS/NFV-003ed141, ETSI GS NFV 003 V1.4.1, ETSI (ISG), Sophia-Antipolis, France, Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV/001_099/003/01.04.01_60/gs_nfv003v010401p.pdf

[168] D. Shackleford, *Virtualization Security: Protecting Virtualized Environments*, 1st ed. Hoboken, NJ, USA: Sybex, 2012, pp. 1–20.

[169] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804510001281

[170] S. Pearson, *Privacy, Security and Trust in Cloud Computing*. London, U.K.: Springer, 2013, pp. 3–42. doi: 10.1007/978-1-4471-4189-1_1.

[171] *Network Functions Virtualisation (NFV); NFV Security; Problem Statement*, document DGS/NFV-SEC001, ETSI GS NFV-SEC 001 V1.1.1, ETSI (ISG), Sophia-Antipolis, France, Oct. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_nfv-sec001v010101p.pdf

[172] *Network Functions Virtualisation (NFV); NFV Security; Security Trust Guid.*, document DGS/NFV-SEC003, ETSI GS NFV-SEC 003 V1.1.1, ETSI (ISG), Sophia-Antipolis, France, Dec. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/003/01.01.01_60/gs_nfv-sec003v010101p.pdf

[173] M. Chiosi *et al.*, "Network functions virtualisation," ETSI, Dusseldorf, Germany, White Paper 3, 2014. [Online]. Available: https://portal.etsi.org/Portals/0/TBpages/NFV/Docs/NFV_White_Paper3.pdf

[174] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in *Advances in Digital Forensics VII*, G. Peterson and S. Shenoi, Eds. Berlin, Germany: Springer, 2011, pp. 35–46.

[175] S. Ravidas, S. Lal, I. Oliver, and L. Hippelainen, "Incorporating trust in NFV: Addressing the challenges," in *Proc. 20th Conf. Innov. Clouds, Internet Netw. (ICIN)*, Mar. 2017, pp. 87–91.

[176] *Network Functions Virtualisation (NFV);Security; Report on NFV LI Architecture*, document DGR/NFV-SEC007, ETSI GR NFV-SEC 007 V1.1.1, ETSI (ISG), Sophia-Antipolis, France, Oct. 2017. [Online]. Available: http://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/007/01.01.01_60/gr_nfv-sec007v010101p.pdf

[177] W. River. Carrier-grade checklist for network functions virtualization. Wind River Systems. Accessed: Mar. 11, 2019. [Online]. Available: https://www.windriver.com/products/product-overviews/Carrier-Grade-NFV_Checklist.pdf

[178] VMWare. *Delivering High Availability in Carrier-Grade NFV Infrastructures*. Accessed: Mar. 11, 2019. [Online]. Available: https://www.vmware.com/files/pdf/techpaper/vmware-vcloud-nfv-high-availability.pdf

[179] B. Chatras and F. F. Ozog, "Network functions virtualization: The portability challenge," *IEEE Netw.*, vol. 30, no. 4, pp. 4–8, Jul. 2016.

[180] T. R. Halfhill, "Beyond the data center: How network-function virtualization enables new customer-premise services," The Linley Group, Mountain View, CA, USA, Feb. 2016. [Online]. Available: https://www.nxp.com/docs/en/white-paper/NXP-NFV-WHITEPAPER.pdf

[181] L. M. Contreras, P. Doolan, H. Lønsethagen, and D. R. López, "Operational, organizational and business challenges for network operators in the context of SDN and NFV," *Comput. Netw.*, vol. 92, pp. 211–217, Dec. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128615002492

[182] Netcracker. *Survey: The Top 5 Challenges Preventing SDN/NFV Deployment*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.netcracker.com/insights/general/survey-top-5-challenges-preventing-sdn-nfv-deployment.html

[183] *The Business End of NFV*, Broadband Forum Fremont, CA, USA. Accessed: Mar. 21, 2019. [Online]. Available: http://www.intercomms.net/issue-29/pdfs/articles/broadband-forum.pdf

[184] A. Manzalini, "Softwarization of telecommunications," *IT-Inf. Technol.*, vol. 57, no. 5, pp. 321–329, 2015.

[185] E. Jason, L. Scott, and O. Matt, *Network Programmability and Automation*, 1st ed. Newton, MA, USA: O'Reilly Media, 2017, pp. 1–35.

[186] B. Jennings *et al.*, "Towards autonomic management of communications networks," *IEEE Commun. Mag.*, vol. 45, no. 10, pp. 112–121, Oct. 2007.

[187] S. Dobson *et al.*, "A survey of autonomic communications," *ACM Trans. Auto. Adapt. Syst.*, vol. 1, no. 2, pp. 223–259, Dec. 2006.

[188] G. Ryan, *Programming and Automating Cisco Networks: A Guide to Network Programmability and Automation in the Data Center, Campus, and WAN (Networking Technology)*, 1st ed. Indianapolis, IN, USA: Cisco Press, 2016, pp. 1–64.

[189] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN: An intellectual history of programmable networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 2, pp. 87–98, Apr. 2014. doi: 10.1145/2602204.2602219.

[190] B. Blanco *et al.*, "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," *Comput. Standards Interfaces*, vol. 54, pp. 216–228, Nov. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548916302446

[191] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[192] R. Roman *et al.*, "Mobile edge computing, fog: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16305635

[193] E. Ahmed and M. H. Rehmani, "Mobile edge computing: Opportunities, solutions, and challenges," *Future Gener. Comput. Syst.*, vol. 70, pp. 59–63, May 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16303260

[194] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 416–464, 1st Quart., 2018.
[195] G. C. Valastro, D. Panno, and S. Riolo, "A SDN/NFV based C-RAN architecture for 5G mobile networks," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Jun. 2018, pp. 1–8.
[196] J. Costa-Requena *et al.*, "SDN and NFV integration in generalized mobile network architecture," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2015, pp. 154–158.
[197] M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, "Integrated NFV/SDN architectures: A systematic literature review," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 114:1–114:39, Feb. 2019. doi: 10.1145/3172866.
[198] V. Nguyen, A. Brunstrom, K. Grinnemo, and J. Taheri, "SDN/NFV-based mobile packet core network architectures: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1567–1602, 3rd Quart., 2017.
[199] *Standards and Technology*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.opennetworking.org/software-defined-standards/overview/
[200] *An Innovative Combination of Standards and Open Source Software*. Accessed: Mar. 21, 2019. [Online]. Available: https://www.dmtf.org/standards
[201] P. Veitch, M. J. McGrath, and V. Bayon, "An instrumentation and analytics framework for optimal and robust NFV deployment," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 126–133, Feb. 2015.
[202] H. Packard, "Network functions virtualization," Hewlett Packard, Hewlett Packard Enterprise Develop. LP, Palo Alto, CA, YSA, Tech. Rep. 4AA5-1114ENW, Jun. 2017. [Online]. Available: https://h20195.www2.hpe.com/V2/getpdf.aspx/4AA5-1114ENW

A. U. REHMAN received the bachelor's degree (Hons.) in telecommunications engineering from Mohammad Ali Jinnah University, Pakistan, in 2009, and the master's degree (Hons.) in telecommunications engineering from The University of Sunderland, U.K., in 2011. He is currently pursuing the Ph.D. degree in telecommunications with MAP-tele (a joint Doctoral Program of the Universidade do Porto, the Universidade de Aveiro, and the Universidade do Minho, Portugal, three universities with a strong tradition in the area of telecommunications engineering). He was a Visiting Instructor with Telecom Foundation, Pakistan. He was a Teaching Assistant with Mohammad Ali Jinnah University, for several years. He is currently involved in the research areas of telecommunications and Internet with the Instituto de Telecomunicações, Portugal, where he is an Active Member of the Network Application and Services Group. His research interests include software-defined networking (SDN), network functions virtualization (NFV), and the reliability and resilience of future networks. He is also a member of the Communication Society (ComSoc) and the Software Defined Networks Community, IEEE.

RUI L. AGUIAR received the degree in telecommunication engineering and the Ph.D. degree in electrical engineering from the Universidade de Aveiro, in 1990 and 2001, respectively, where he is currently a Full Professor and responsible for networking area. He has been an Adjunct Professor with INI, Carnegie Mellon University, and a Visiting Research Scholar with the Universidade Federal de Uberlândia, Brazil. He is coordinating a research line in the area of networks and multimedia nationwide with the Instituto de Telecomunicações. His current research interests include the implementation of 5G networks and the future Internet. He has over 450 published papers in his research areas, including standardization contributions to the IEEE and the IETF. He has served as the Technical and General Chair of several IEEE, ACM, and IFIP conferences, and as an IEEE ComSoc Distinguished Lecturer. He is regularly invited for keynotes on 5G and the future Internet subjects. He sits on the TPC of most major IEEE ComSoc conferences. He is the current Chair of the steering board of the Networld 2020 ETP. He is Senior Member of the Portugal ComSoc Chapter Chair and a member of the ACM. He is Associate Editor of ETT (Wiley) and *Wireless Networks* (Springer). He has helped on the launch of *ICT Express* (Elsevier).

JOÃO PAULO BARRACA received the Ph.D. degree in informatics engineering from the Universidade de Aveiro, in 2012, where he is an acting Assistant Professor. He conducts research with the Instituto de Telecomunicações, having led the TN-AV Group, from 2015 to 2016, for two years. He has close to 100 peer-reviewed publications and reports related to solutions for the Internet of Things and software for cloud environments, with a focus on software-defined networking and 5G Networks. Having participated in many review panels, he has also organized workshops and conferences. He has participated in more than 20 projects, either developing novel concepts or applying these concepts in innovative products and solutions. He leads the FCT/CAPES DEVNF Project in Portugal devoted to NFV orchestration, the local teams of EU LIFE-PAYT, participates in European Science Cloud for Astronomy (EU AENEAS), the local team in the P2020 (CRUISE Project), the security team at P2020-Social, participates in the EU Interreg CISMOB smart cities pilot, the Engage SKA research infrastructure, and the Square Kilometer Array System (SKA) Team, having lead activities for TM-LINFRA, among a dozen other innovation projects. Recently, he has received the third place from the INCM Innovation Challenge, for the development of a project targeting smarter environments for public transports in smart cities, using Block-chain technologies.