RESEARCH ARTICLE

Enhancing Network Slicing Architectures With Machine Learning, Security, Sustainability and Experimental Networks Integration

JOBERTO S. B. MARTINS[1], (Life Senior Member, IEEE), TEREZA C. CARVALHO[2],
RODRIGO MOREIRA[3], CRISTIANO BONATO BOTH[4], ADNEI DONATTI[2],
JOÃO H. CORRÊA[5], JOSÉ A. SURUAGY[6], (Member, IEEE), SAND L. CORRÊA[7],
ANTONIO J. G. ABELEM[8], (Member, IEEE), MOISÉS R. N. RIBEIRO[9],
JOSÉ-MARCOS S. NOGUEIRA[10], (Member, IEEE), LUIZ C. S. MAGALHÃES[11],
JULIANO WICKBOLDT[12], TIAGO C. FERRETO[13], (Member, IEEE), RICARDO MELLO[9],
RAFAEL PASQUINI[14], (Senior Member, IEEE), MARCOS SCHWARZ[15],
LEOBINO N. SAMPAIO[16], (Member, IEEE), DANIEL F. MACEDO[10],
JOSÉ F. DE REZENDE[17], (Member, IEEE), KLEBER V. CARDOSO[7],
AND FLÁVIO DE OLIVEIRA SILVA[14], (Member, IEEE)

[1]Computer Science Department, Universidade Salvador (UNIFACS), Salvador 41770-235, Brazil
[2]Computer Engineering and Digital Systems Department, Universidade de São Paulo (USP), São Paulo 05508-020, Brazil
[3]Institute of Exact and Technological Sciences, Universidade Federal de Viçosa (UFV), Viçosa 36570-000, Brazil
[4]Universidade Federal do Vale dos Sinos (UNISINOS), PPGCA, Porto Alegre 90470-280, Brazil
[5]Universidade Federal do Ceará (UFC), Fortaleza 62600-00, Brazil
[6]Informatics Center, Universidade Federal de Pernambuco (UFPE), Recife 50740-560, Brazil
[7]Institute of Informatics, Universidade Federal de Goiás (UFG), Goiania 74690-900, Brazil
[8]Computer Science Department, Universidade Federal do Pará (UFPA), Belém 66075-110, Brazil
[9]Electrical Engineering Department, Universidade Federal do Espírito Santos (UFES), Vitória 29075-910, Brazil
[10]Computer Science Department, Universidade Federal de Minas Gerais (UFMG), Belo Horizonte 31270-010, Brazil
[11]Telecommunications Engineering Department, Universidade Federal Fluminense (UFF), Niteroi 24210-240, Brazil
[12]Institute of Informatics, Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre 90040-060, Brazil
[13]School of Technology, Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Porto Alegre 90619-900, Brazil
[14]Faculty of Computing, Universidade Federal de Uberlândia (UFU), Uberlândia 38408-100, Brazil
[15]Research, Development and Innovation Directory, Rede Nacional de Pesquisa (RNP), Rio de Janeiro 22290-906, Brazil
[16]Computer Science Department, Universidade Federal da Bahia (UFBA), Salvador 40110-909, Brazil
[17]Systems and Computer Engineering Program, Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro 21941-901, Brazil

Corresponding author: Joberto S. B. Martins (joberto@ieee.org)

ABSTRACT Network Slicing (NS) is an essential technique extensively used in 5G networks computing strategies, mobile edge computing, mobile cloud computing, and verticals like the Internet of Vehicles and industrial IoT, among others. NS is foreseen as one of the leading enablers for 6G futuristic and highly demanding applications since it allows the optimization and customization of scarce and disputed resources among dynamic, demanding clients with highly distinct application requirements. Various standardization organizations, like 3GPP's proposal for new generation networks and state-of-the-art 5G/6G research projects, are proposing new NS architectures. However, new NS architectures have to deal with an extensive range of requirements that inherently result in having NS architecture proposals typically fulfilling the needs of specific sets of domains with commonalities. The Slicing Future Internet Infrastructures (SFI2) architecture proposal explores the gap resulting from the diversity of NS architectures target domains by proposing a new NS reference architecture with a defined focus on integrating experimental networks and

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

enhancing the NS architecture with Machine Learning (ML) native optimizations, energy-efficient slicing, and slicing-tailored security functionalities. The SFI2 architectural main contribution includes the utilization of the slice-as-a-service paradigm for end-to-end orchestration of resources across multi-domains and multi-technology experimental networks. In addition, the SFI2 reference architecture instantiations will enhance the multi-domain and multi-technology integrated experimental network deployment with native ML optimization, energy-efficient aware slicing, and slicing-tailored security functionalities for the practical domain.

INDEX TERMS Network slicing, network slicing architecture, experimental networks integration, architectural slicing enhancements, ML-native optimization, energy-efficient slicing, slicing-tailored security.

I. INTRODUCTION

Network slicing (NS) is being extensively used in domains such as 5G, the Internet of Things (IoT), the Internet of Vehicles (IoV), Industry 4.0, drone networks, smart transportation systems, smart health care, and smart grids, among others [1], [2], [3], [4], [5]. However, given its large domain of application and inherent requirements, network slicing architectures and deployment aspects like multi-domain coverage, technology-specific proposals, end-to-end effectiveness, lightweight deployments, and network segment integration are still open research issues.

The Slicing Future Internet Infrastructures (SFI2)[1] research project [6] leading technical and innovative emphasis is to develop a network slicing solution that provides orchestration and allocation of resources for multi-domain experimentation network infrastructures. The experimentation testbeds FIBRE-NG [7], FUTEBOL [8], Cloud-NEXT [9], FIWARE [10], 5GINFIRE [11], and NECOS [12], are the main targets of the SFI2 project. In this context, the SFI2 project aims to integrate resources and services from the legacy experimental infrastructures mentioned above by defining a reference architecture and functionalities, allowing its instantiation and deployment on distinct domains.

The SFI2 reference architecture proposed in this article is a new enhanced architecture for network slicing and a practical realization of the Slice-as-a-Service (SlaaS) paradigm, with intelligent end-to-end slice orchestration, considering security requirements and sustainability aspects at different stages of the slice life cycle. In the context of integrated, multi-domain, and multi-technology experimental networks, the focus of the SFI2 reference architecture, autonomy, and efficiency are critical requirements to orchestrate a complex and dynamic multi-domain virtual network composed of slices. The SFI2 reference architecture uses an ML-native approach to improve performance on complex decision-making problems throughout the slicing life cycle.

A network slicing system provides services with multiple security requirements. Providing various services in a multi-domain infrastructure for multiple customers makes security services crucial and complex. SFI2 leverages recent discussions, such as [13], [14], and [15], to comprehensively address security issues for the slicing life cycle, i.e., preparation, commissioning, operation, and decommissioning, as well as for intra-slice and inter-slice communication.

So, the main contributions of the architecture proposed involve the enhancement of the following aspects:

- **Artificial Intelligence and Machine Learning**. The proposed architecture uses machine learning techniques natively to improve network slicing in its phases, supporting the orchestration of network slices and prediction of resources and quality of service.
- **Energy Efficiency and Sustainability**. By focusing on strategies for resource allocation, SFI2 targets sustainability and energy efficiency at different stages of the slice life cycle (i.e., preparation, commissioning, and operation) according to their demands.
- **Security**. We clearly define security in the context and scope of slicing architectures since current frameworks can operate over complex domains involving diverse computing resources over a shared infrastructure. In this sense, SFI aims to assure isolation and integrity.

This article is structured as follows. Section II presents network slicing architecture and project approaches. Section III details the SFI2 architecture functionality and building blocks. Section IV presents the SFI2 architectural enhancements regarding machine learning support, sustainability, and security. Section V focuses on instantiating the SFI2 architecture on the FIBRE experimental network, and Section VI presents an experimental scenario demonstrating the sustainability architectural enhancement. Finally, Section VII concludes with an overview of SFI2 main highlights, contributions, and future work.

II. CURRENT NETWORK SLICING APPROACHES

Network slicing is an essential technological enabler for 5G & Beyond (5G&B), vehicle and drone communications, IoT deployments, Telco clouds, Industry 4.0, Augmented Reality/Virtual Reality (AR/VR) technologies, and Multi-Access Edge Computing (MEC), among others. Some commonplace service characteristics in these areas include dealing with diversified and stringent user requirements, supporting dynamic and on-demand resource allocation, and the need for efficient resource orchestration and allocation [4].

In this sense, network slicing provides a new virtualization approach for the components of wired and wireless networks, such as communication resources, Radio Access Network (RAN) connection, switching equipment, cloud infrastructures, and computation and storage resources. Network slicing allows the partitioning of physical and virtual

---

[1]Available at https://sites.google.com/view/sfi2/home

resources with the capability to create, orchestrate, configure, and redefine the slice partitions as needed. Network slicing adds value to the networking perspective by allowing abstraction, isolation, orchestration, and softwarization of service deployments on network architectures [16].

Network slicing is gaining a substantial research track with the proposals of network slicing-oriented architectures, standardization efforts, network slicing frameworks, and efficient network slicing solutions, typically based on machine learning techniques [17], [18]. Standardization institutions like the Third Generation Partnership Project (3GPP), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), International Telecommunication Union — Telecommunication Standardization Sector (ITU-T), Open Network Forum (ONF), and Next Generation Mobile Network (NGMN) alliance are developing NS-oriented architectures. The network slicing architectures and standards proposed by these organizations are, to some extent, focused on or siloed in their actuation domains (telecommunications, 5G&B, industry, Internet, others) and tend to anchor the service aspects prevalent in these domains, presenting divergences on their approaches [19]. In the following subsection, we describe the main initiatives of standardization institutions for network slicing.

A. NETWORK SLICING STANDARDIZATION INITIATIVES

The 3GPP network slicing architecture mainly addresses the 5G/6G wireless domain [15]. The architecture reflects that 3GPP is the main standard body for mobile communication networks, focusing on the next generation of mobile networks. The 3GPP architecture includes the slice concept and definition in terms of services chains with virtualized or physical resources, network components like access network, transport, and core, the end-to-end concept, and the life cycle of a network slice with four main phases: Preparation, Commissioning, Operation, and Decommissioning [20].

The ETSI network slicing effort focuses on a general end-to-end next-generation network slicing (NGNS) framework and architecture for service providers. The intent is to coordinate and operate services as active network slices. The ETSI slice design includes a service-oriented approach, defining a slice abstraction, its reusability, and autonomy [21]. Significant results from ETSI efforts are Zero-Touch network and service management for management automation [22].

The IETF NS architecture proposal accommodates network slicing definitions, services, components, and features in the IETF networking set of protocol, nomenclature, and recommendations ecosystem. In summary, the IETF NS architectural proposal defines the functionalities of deploying services by slicing physical and virtual resources and maps them to the overall and general IETF concept of management, control, and data planes. The NS IETF architectural focus is on the transport network part of the end-to-end network slices that involves, in addition, the edge (RAN) and core slices [23].

The Open Networking Foundation (ONF) network slicing architecture is based on the Software-Defined Networking (SDN) paradigm. In the ONF NS architecture proposal, the SDN controller and SDN clients are the key components. A slice is comparable to an SDN client isolated by the controller's virtualization and client policy functions. The orchestration and the defined global policy functions control and optimize the slice. The overall slice controller is an SDN controller application [24].

The ITU-T NS conceptual architecture consists of Logically Isolated Network Partitions (LINPs) over physical resources supporting network virtualization. LINP is an essential conceptual ITU-T architectural component. According to ITU-T Y.3011 [25], slicing allows logically isolated network partitions with a slice considered a unit of programmable resources such as network, computation, and storage. A LINP is an isolated and programmable entity that provides users and service providers capabilities similar to traditional networks without network slicing.

The NGMN network alliance provides a network slicing conceptual architecture outline with three layers. It defines an end-user service or a business Service Instance Layer (SIL), a Network Slice Instance (NSI) providing a set of network functions required by a service instance, and a resource layer [26].

5G enhanced wireless mobile capabilities with massive Machine-Type Communication (mMTC), enhanced Mobile Broadband (eMBB), and Ultra-Reliable and Low-Latency Communication (URLLC) services are concentrating the research and development efforts around the world. Slicing is a fundamental tool for 5G&B; consequently, the most relevant projects concerning network slicing address the 5G scenario. Relevant research projects proposing NS approaches for 5G include the projects 5GEx, 5G-SONATA, 5G-PAGODA, 5G-SLICENET, NECOS (Novel Enablers in Cloud Slicing), and 5Growth [12]. The following subsection describes the main research projects for network slicing.

In order to highlight our contributions, we summarize the related works in Table 1, where we represent relevant characteristics for the realization of network slices for standardization initiatives and slicing projects [19]. For standardization bodies, it is indicated only the explicit network slicing characteristic support. For this, we use the marker (●) to represent the achievement of the characteristic by the network slicing approach and the marker (○) to represent the non-compliance of the characteristic.

B. NETWORK SLICING PROJECTS

The 5GEx project mainly aims to enable cross-domain orchestration of services over multiple or multi-domain single administrations [27]. The project focuses on designing a networking factory where a new network infrastructure and associated services are instantiated and deployed by software. In 5GEx, a slice manager supports the resource orchestrator functionality with multi-tenancy resources and multi-vendor

TABLE 1. Network Slicing Characteristics for Standardization Initiatives and Network Slicing Projects.

Characteristics / Initiative	3GPP	ITU-T	NGMN	IETF	ETSI	ONF	5G-SONATA	5G-PAGODA	5GEx	NECOS	SFI2
Multi-domain Slicing	O	O	O	●	O	O	O	O	●	●	●
Slicing across Experimental Networks	O	O	O	O	O	O	O	O	O	O	●
AI-Native Architecture	O	O	O	O	O	O	O	O	O	O	●
Security with Slicing-aware Capabilities	O	O	O	O	O	O	O	O	O	O	●
Sustainability-aware Slice Building Capability	O	O	O	O	O	O	O	O	O	O	●
Marketplace for Slices	O	O	O	O	O	O	O	O	O	●	●
Domain Customized Infrastructure Interfaces	O	O	O	O	O	O	O	O	O	●	●
Domain Customized Monitoring Interfaces	O	O	O	O	O	O	O	O	O	●	●
End-to-End Slicing	●	O	O	O	●	O	O	O	O	●	●
Slice-as-a-Service	●	O	O	O	O	O	O	O	●	●	●
Infrastructure Monitoring	O	●	O	O	●	O	●	O	●	●	●

Virtualized Network Function (VNF) management. 5GEx allows end-to-end network and service elements to mix in multi-vendor, heterogeneous technology, and resource environments.

The 5G SONATA project focuses on the flexible programmability of networks and the optimization of their deployments. A SONATA slice is a basic unit of programmability with a set of resources used in an end-to-end network service comprised of VNFs. The SONATA framework leverages the virtualization offered by cloud infrastructures and network programmability to develop and deploy network services and VNFs [28].

The 5G-PAGODA project aims to create a scalable 5G slicing architecture by extending the current Network Virtualization Function (NFV) architecture to support network slices composed of multi-vendor VNFs. PAGODA architecture approach enables network flexibility and programmability to create and manage virtual network slices tailored to the needs of 5G verticals for Mobile Virtual Network Operators (MVNOs) [29]. As a complementary objective, the 5G-SLICENET project proposes an end-to-end intelligent network slicing approach with a slice management framework supporting virtualized multi-domain and multi-tenant in SDN/NFV-enabled 5G networks [30].

The NECOS project creates a reference architecture for cloud-networking slicing enforcing the realization of the Slice-as-a-Service (SlaaS) paradigm [12]. The NECOS project addresses cloud and network slicing and considers the end-to-end and multi-administrative domain scenarios while embracing the SlaaS paradigm. Beyond those essential characteristics, NECOS has unique features such as a new Virtual Infrastructure Manager (VIM) on-demand, a new Wide-area Infrastructure Manager (WIM) on-demand slicing models, and a marketplace approach, which other current approaches to slicing architectures have not considered.

Lately, projects such as 5G-Solutions [31], 5G-Tours [32], 5G-Victori [33], and 5Growth [34] have been proposed to validate the network slicing concept across multiple vertical industries, including transportation, energy, media, entertainment, and factories of the future. Among such projects, 5Growth has used artificial intelligence and machine learning solutions to enhance service automation in network slices.

Also, Moreira et al. [35] designed and evaluated the NASOR, an orchestration concept towards multi-domain network slicing on top of Internet routers.

Current network slicing solutions envision highly relevant aspects: optimized resource allocation and orchestration, end-to-end network slicing, multi-technology, multi-tenant slicing support, automated slicing management, and elastic and dynamic resource allocation [36]. An open research issue currently addressed by network slicing architectures and projects such as 5Growth is an intelligent end-to-end slice orchestration and management solution that could fulfill diverse service requirements while ensuring efficient resource utilization and appropriate slice isolation.

The architectural enhancements proposed by the SFI2 architecture discussed in the following sections aim to add machine learning and security new capabilities to current network slicing architectures preserving a sustainable solution concomitantly.

III. THE SFI2 NETWORK SLICING ARCHITECTURE

The SFI2 network slicing architecture proposal is fundamentally a reference architecture that allows slicing functionalities for instantiation and deployment in distinct experimental network domains. The SFI2 architecture advances state-of-the-art by offering slice-as-a-service instantiation and deployment capabilities for multi-domain experimental networks. In this context, the SFI2 architecture aims to fulfill an existing gap in providing a virtual experimental network using the network slicing paradigm across multiple experimental network domains. This integration aims, from the user's point of view, to support multi-technology experimental networks by integrating existing experimental networks that focus, in most cases, on specific technologies.

The SFI2 architecture offers dynamic slice building, instantiation, and supervision with machine learning-based embedded optimization. The SFI2 slicing capabilities have intradomain, interdomain, intraslice, interslice, and life cycle slicing security and an entirely new sustainable-aware approach for slice resource selection, orchestration, and deployment. SFI2 architecture's basic functionalities and modules are illustrated in Fig. 1. The architecture comprises a set of functional module components interrelated according
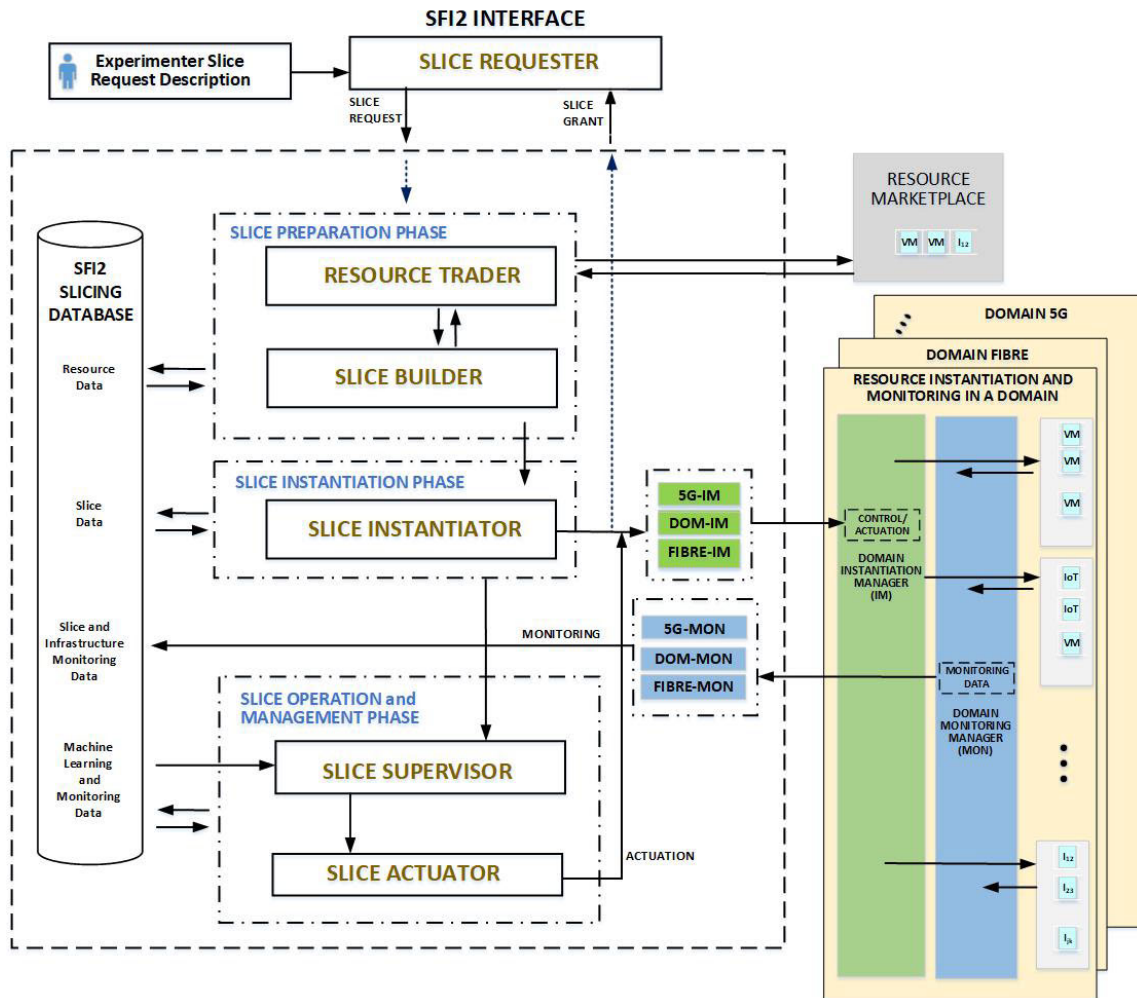
FIGURE 1. SFI2 Network Slicing Architecture and Functional Blocks.

to the slicing life cycle phases of preparation, commissioning, operation, and decommissioning [15].

SFI2 has an external interface that allows experimenters and tenants to request the creation of sliced virtual networks. To make the facility's utilization easier, SFI2 adopts intent-based and script descriptions for network setup across single and multiple domains. The resource marketplace plays an essential role in the network slicing process by, firstly, collecting resources from different providers in eventually different network domains and, subsequently, displaying and trading these resources to compose a sliced virtual network.

The SFI2 resource marketplace innovates compared to other existing resource marketplaces by aggregating and trading multi-technology resources like virtual machines, SDN-capable switches, IoT resources, and 5G setups, among others, to compose a single virtual network. These resources are currently available on specialized and independent experimental networks, and SFI2 groups them in a structured way. At this point, it is important to remark that the SFI2 deployment focus is the set of experimental networks currently

available in Brazil: FIBRE-NG [7], CloudNEXT [9], FUTEBOL [8], FIWARE [10], 5GINFIRE [11], and NECOS [12].

The preparation of the sliced virtual network, composed of multi-technology resources belonging to eventually distinct domains, is the task of the resource trader and slice builder. The resource trader and slice builder modules cooperate to orchestrate the slice preparation by finding resources and allocating them to a specific sliced network. In the SFI2 architecture, the building process, composed of slice resource trading and slice orchestration modules, considers user-defined sustainability and energy-efficiency parameters and constraints. On top of that, resource orchestration is optimized by using machine learning algorithms.

The slice instantiation module carries out the instantiation phase. It effectively deploys the assigned resources of a virtual network on their respective domains. The instantiation involves all domain-related aspects and specificities and includes all network slices and communication facilities required to allow slice operation. The per-domain instantiation uses specific domain interface managers (DOM-IM)

customized for each domain involved in the slicing process. From an architectural point-of-view, the SFI2 use of the DOM-IM modules approach allows an agnostic resource deployment in different domains.

The slice operation and management phase of the network slicing process is executed by the slice supervision, slice actuator, and monitoring interface managers (DOM-MON). Slice supervision in the SFI2 architecture consists of dynamically verifying per-slice conformance of actual slice key performance indicators (KPI) concerning the user-defined slice key performance parameter (KPP) and management requirements like high-level SLA, QoE, or QoS specifications [37], [38].

An innovative supervision capability of the SFI2 architecture is its ability to monitor application-specific performance parameters. As illustrated in Fig. 1, the architecture allows monitoring application-specific characteristics at the slice level. The application level monitoring facility (APP-MON) notifies the slice supervision module of alerts to allow on-the-fly slice reconfiguration.

Slice supervision in the SFI2 architecture uses machine learning techniques to support on-the-fly slice reconfiguration and slice elasticity. The slice actuator module executes the reconfiguration and elasticity required deployments at the request of the slice supervision module.

Monitoring is an essential part of any shared dynamic environment such as SFI2 in which several simultaneous users and tenants request network, processing, and memory resources and expect that specific quality, performance, security, and energy efficiency levels be met during the lifetime of their experiments and service deployments. Monitoring in SFI2 architecture attempts to be agnostic. The performance parameters monitoring data can be generated and collected by several tools, such as Prometheus, Casandra, and others, at each infrastructure and resource provider domain. The monitoring interface managers (DOM-MON) collect the required monitoring data at the domain and transfer them to SFI2 modules processing providing the required customization of the acquired data.

The SFI2 slice database supports the entire slicing process in the preparation, instantiation, slice operation, and management phases. The SFI2 slicing database stores and shares monitoring data, slicing resources and slicing deployment information among the SFI2 modules. The SFI2 database also supports the security functionalities that encompass the set of activities concerning user access and the SFI2 module's operation.

The main contribution of the SFI2 network slicing architecture is to enhance current slicing architectures with new fundamental capabilities. The new capabilities enhancements are threefold:

- Slice creation and operation with sustainable resource allocation;
- Resource trading, slice building, and slice operation elasticity with machine learning and optimization techniques support (AI-native architecture); and

- Security features and functionalities embedded within slice operation and experimental network domain deployment.

In summary, the SFI2 architecture aims to create slices for experimental networks, including operation and management optimization, while considering the utilization of sustainable resources in a secure environment, as discussed in the following sections.

IV. SFI2 FUNCTIONAL ENHANCEMENTS
This section gives details of the architectural enhancements of the SFI2 architecture.

A. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ENHANCEMENTS
The SFI2 architectural machine learning enhancements are illustrated in Fig. 2. In the life cycle of network slices, some phases are foreseen, such as preparation, commissioning, operation, and decommissioning. The SFI2 proposal is to use machine learning techniques natively in the architecture to improve network slicing in some of these phases [39].

Among the enhancements supported by machine learning techniques in the orchestration of network slices, resource prediction and quality of service prediction stand out. Different techniques ranged from combinatorial optimization to machine learning, such as reinforcement learning and supervised and unsupervised learning. Notably, their applications predominantly focused on commissioning, instantiation and monitoring, and control for all the techniques considered. However, intelligent and autonomous actions based on planning on already deployed network slices lack innovation, leading SFI2 to propose an intelligently-native orchestrator for the entire network slicing life cycle.

Furthermore, the SFI2 orchestrator aims to operate over heterogeneous infrastructures to support native distributed machine learning on its building blocks [40], [41]. SFI2 will follow the concept of Machine Learning as a Service (MLaaS) using distributed agents. To do so, SFI2 builds ML-based management that interacts with the monitoring system and with other blocks of the network slicing management. The ML management module maintains already-trained machine learning models and carries out distributed training between target domains for building specific models and up-to-date ones.

The SFI2 ML manages learning agents throughout all infrastructure components to support distributed machine learning. Those agents can perform training or prediction tasks coordinated by the principal ML agent. In our orchestration framework, we are pursuing a mechanism capable of enclosing numerous machine-learning paradigms and using them depending on the network slicing life cycle phase.

B. ENERGY EFFICIENCY AND SUSTAINABILITY ENHANCEMENTS
Adopting energy-efficient and renewable-energy-aware practices is a prime goal for any organization in the Information and Communications Technology (ICT) industry concerned
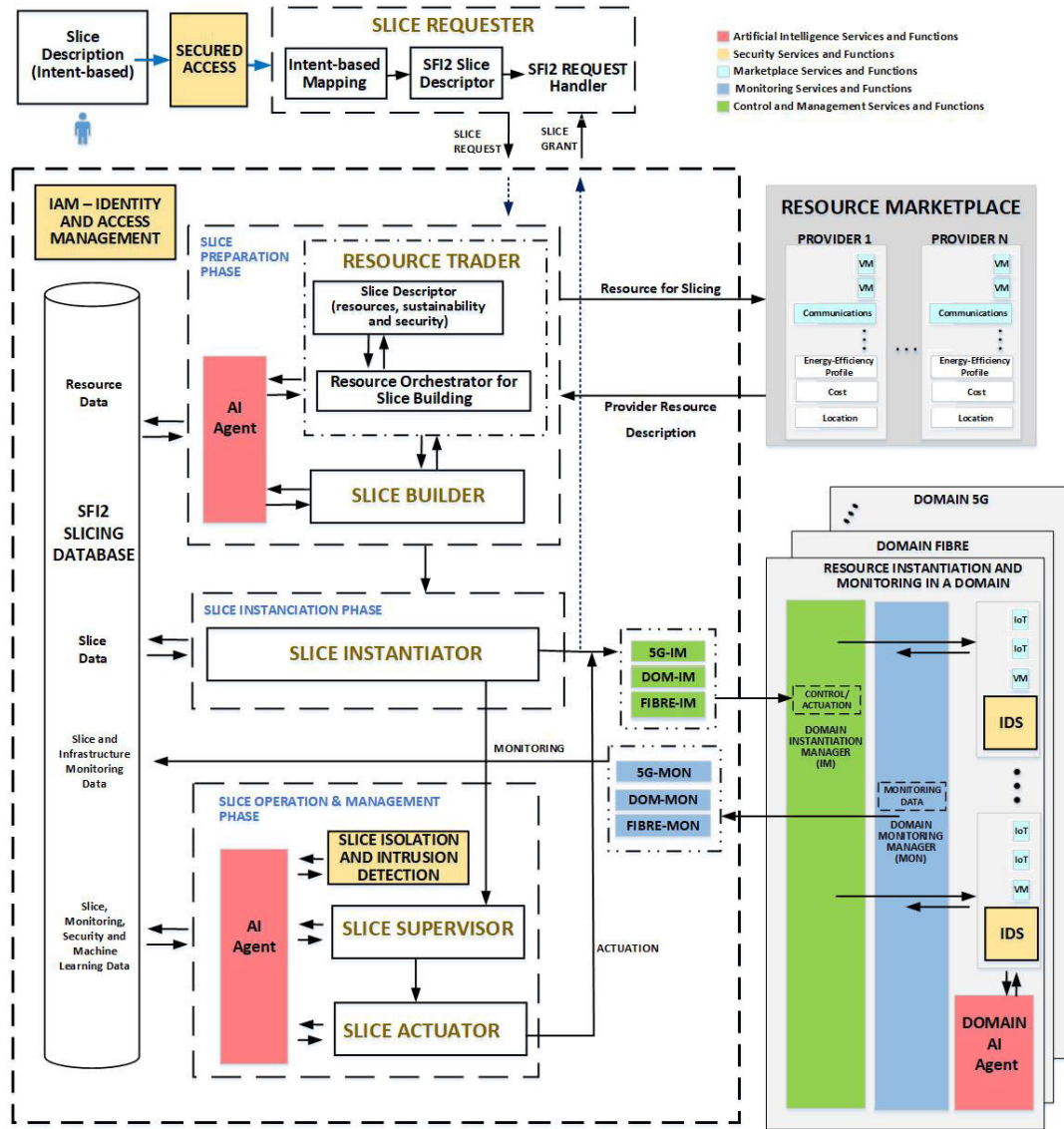
FIGURE 2. SFI2 Machine Learning, Sustainability, and Security Architectural Enhancements.

with global sustainability. The amount of CO_2 generated by ICTs, which includes data centers, networks, and end-user equipment, has been assessed. According to GeSI — Global Enabling Sustainability Initiative, the contribution of ICT is about 1.25 Mton of CO_2 per year [42]. Despite the increasing number of computing devices, this number has been gradually decreasing due to actions regarding the energy efficiency of the equipment and its operation. In this sense, the deployment of network slices optimizes computing and network resources through their virtualization. However, it requires more complex functions and management. Therefore, energy efficiency has to be targeted at different stages of the slice life cycle, including slice preparation, commissioning, and operation, which have varying energy demands. Beyond that, tenants in the ICT business may explicitly require specific sustainability (*e.g.*, clean/renewable energy

sources) and energy efficiency indicators due to their commitments to users and investors adherent to the Environmental, Social, and Governance (ESG) principles [43].

The SFI2 architecture works toward a sustainable and energy-efficient network slicing process, addressing features aligned with cloud computing and general data centers' equivalent policies. As a general policy, service providers' resource allocation, including slice deployments, should always favor the least energy consumption, ideally coming 100% from renewable sources [44].

The design of the SFI2 architecture addresses a perspective that energy (in terms of electricity power) is a resource as essential and scarce as computational resources. For instance, this perspective allows one to approach energy usage the same way as CPU usage. Therefore, SFI2 adopts resource allocation strategies considering the energy usage of the final

system, aiming to reduce it as much as possible. While also ensuring that slice requirements are attended to. Moreover, the energy-as-a-resource perspective enables SFI2 to follow policies and guidances considering the energy sources (*e.g.*, renewable, non-renewable).

The SFI2 architecture endorses state-of-the-art policies and methods to achieve energy efficiency for distributed systems, focusing on strategies for resource allocation. In this direction, we list the following strategies considered in the SFI2 architecture:

- Building network routes/paths aiming to reduce the communication cost;
- Enforcing efficient computational resource allocation;
- Applying local solutions to increase energy efficiency (*e.g.*, switches with appropriate technology, sleep-mode mechanisms); and
- Prioritizing allocating resources from providers using renewable energy.

From a conceptual-architectural perspective, SFI2 adopts such strategies by improving some of the fundamental slice life cycle components, namely, resource marketplace and slice builder (Fig. 2). The resource marketplace is in charge of grouping all the available resources required to build a virtual network by sliced resources, indicating the available resources and their description (*e.g.*, type of resource, resource owner, price per hour, flag for renewable energy usage, available amount). In this sense, the resource marketplace serves as a menu for computational resource selection fitting the tenant's requirements.

The slice builder module uses machine learning to analyze the resource list available in the marketplace, looking for an optimal decision on the resource selection for the slice deployment on domains towards a virtual network deployment. A rating scheme favors the resource providers showing better Power Usage Effectiveness (PUE), greater renewable consciousness, and the lowest communication cost (in terms of geographical distance and number of hops). The slice instantiation module is then responsible for performing the actual deployment task.

C. SECURITY ENHANCEMENTS

Security is often overlooked or even neglected in network testbed research, which primarily focuses on its physical and functional aspects. The reason for that is perhaps the same that led the Internet architecture to bring on security at a later phase. Testbed architects' academic mindset usually assumes the legitimate use of its resources and focuses on delivering facilities rather than preventing or protecting them against misuse. However, for 5G security, several prominent bodies, such as NGMN, are concerned with this issue and are making recommendations to be considered at the design stage of network slicing [13]. Conversely, the SFI2 security challenge is how to handle the integration of testbed architectures originally built with only minor security capabilities.

The proposal for SFI2 architecture with security enhancements is illustrated in Fig. 2. Firstly, we must present a clear definition of security in the context and scope of the SFI2 architecture, since the term can be taken by its diverse meanings. Slicing frameworks operate over complex domains of resources, each of which bears its vulnerabilities and special features regarding security. In addition, the more performance decoupling among slices sharing a given physical infrastructure is promoted, the better is a network slicing solution [45]. This implies that multiple slices over a shared infrastructure can coexist without much interference among them, assuring isolation, and, thus integrity.

So, through a synthetic definition, we define security via five primary requirements: Confidentiality, Integrity, Availability, Authentication, and Authorization [46], [47]. And these requirements should be considered along different phases of a slice life cycle.

As stated earlier, the slicing life cycle is composed of 4 main phases: preparation, commissioning, operation, and decommissioning [15]. The literature identifies inherent vulnerabilities in each phase [14]. Among the main contributions of the SFI2 architecture, one is to consider such vulnerabilities and propose architecturally-embedded solutions against multiple attack vectors throughout the slice life cycle.

Table 2 presents the slice life cycle phases and attack categories that can impact them. We use the marker ● to denote the attack accomplishment on the slicing life cycle; otherwise, we use ○ where the attack class does not impact the slicing life cycle. Different attack classes may target distinct life cycle phases, as follows:

- Impersonation: Attack that attempts to bypass authentication and authorization procedures. It is an attempt by an unauthenticated and/or unauthorized user to make a request to the system and to be attended by it;
- Traffic Injection: It is the insertion of foreign - unusual or invalid - traffic to the components of the architecture aiming at generating greater consumption of bandwidth on the network and increased processing on servers and switches. This class of attack is related to the Denial-of-Service class, and it is mostly intended to compromise availability;
- Denial-of-Service (DoS): This is an attempt to make a service unavailable to legitimate users, temporarily or indefinitely. It can occur in a variety of forms, the most prominent being the flooding of resources with superfluous requests and injection of foreign traffic;
- Tampering: This is the unauthorized interference over code, data, or physical device of a system intended to modify or manipulate it. Integrity is the first requirement affected by this attack, which can even lead to service unavailability;
- Eavesdropping: This is the attack that attempts to access information in the communications between communicating entities by capturing data. Such kind of attack impacts the confidentiality and even the integrity of the targets.

TABLE 2. Attack Categories and Network Slicing Phases.

Attack Categories	Preparation	Commissioning	Operation	Decommissioning
Impersonation	●	●	●	●
Traffic Injection	●	●	●	●
Denial-of-Service (DoS)	●	○	●	○
Tampering	●	●	●	●
Eavesdropping	●	●	●	○
Reply Attacks	●	○	○	○
Interfaces Monitoring	●	●	●	●

- Reply Attacks: This type of attack aims to capture access control information previously sent from one entity to another and its subsequent retransmission with the intention of producing an unauthorized effect or gaining unauthorized access. In this way, the goal of the attack is to perform operations originating from legitimate users, targeting, for example, to affect the availability and integrity requirements;
- Interfaces Monitoring: This attack targets the interfaces of a system, e.g.: northbound and southbound, aiming to control the interfacing components. It impacts the confidentiality requirement at first since it captures any and all information. After that, other malicious activities can be performed.

The impersonation attack (Table 2) can be performed at all stages of a slice's life cycle. To prevent this attack, the SFI2 architecture provides, as presented in Fig. 2, an element called IAM (Identity and Access Management). This element is responsible for the management of the identity of the involved parts as well as for the control of access to services and resources. The IAM performs identity authentication and access authorization in the SFI2 architecture, for the experimenter/tenant of the architecture as well as for all elements that compose SFI2. It aims to ensure that all elements that interact or provide service to SFI2 are authenticated and operations are authorized.

The traffic injection attack (Table 2) can also be performed at all stages of the life cycle. The SFI2 architecture mitigates the risk of suffering from such a class of attack by blocking any and all traffic coming from the network external to the architecture's network. In addition, all elements of the SFI2 architecture will only accept traffic generated by the architecture elements themselves. This blocking will be accomplished with firewall rules and also for the controls of the IAM.

The DoS attack, as shown in Table 2, can be executed in the preparation and operation phases. During the preparation phase, the attack may intend to deny the tenant - which is also the experimenter - the ability to request the slice creation. Therefore, the API/Portal of the SFI2 architecture must be equipped with mechanisms that prevent or mitigate this attack. To this purpose, SFI2 uses IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) mechanisms combined with packet filtering. In addition, this architecture element can be provided with high scalability and also with

autoscale mechanisms [48]. While in the operation phase, the goal of the DoS attack is to deny the slice service to the experimenters/tenants on the SFI2 architecture. To prevent this attack, the SFI2 architecture uses IDS/IPS mechanisms and packet filtering on slice accesses.

The tampering attack can be performed in all phases of the slice life cycle. For this attack, the SFI2 architecture only changes information or code of any element by a token generated for this purpose by the IAM. Thus, the user/element that wants to make any change must request a token from the IAM, while the element that will receive the change must check with the IAM if the token presented is a valid token.

The eavesdropping attack can be performed in the preparation, commissioning, and operation phases. To avoid this attack, it is a requirement in the SFI2 architecture to use cryptography between the communication pairs. The exchange of the cryptographic key must be performed at the moment of authentication of the elements with the IAM. The use of cryptography by all elements of the architecture also aims to prevent the attack on monitoring interfaces, which can reach all phases of the slice life cycle.

In the SFI2 architecture, each new request from a user or an element of the architecture to another element must be made using a token. In this way, a new token will be generated for each new request. This creation and control of the tokens are executed by the IAM. This functionality aims to prevent reply attacks.

Additionally, the SFI2 slicing database component (Fig. 2) is provided with mechanisms to ensure the integrity of the information stored in this database. For this, any insertion or removal of data from the database must be authorized by the IAM. In addition, the database itself must be equipped with redundancy to maintain the persistence of the slices' information.

Finally, as a security mechanism, the SFI2 architecture, as presented in Fig. 2, has a specific database, called "SFI2 Security Database", in which all the logs of security-related incidents and activity are stored. This database is used for auditing and also as an input to machine learning algorithms, to learn about new attacks and to suggest mitigation methods.

The attacks and solutions discussed above are in the context of the architecture domain. Thus, in addition to attacks related to the slice life cycle, there are security issues internal to the slice and in communication between the multiple slices. Some of these security issues are mitigated by a
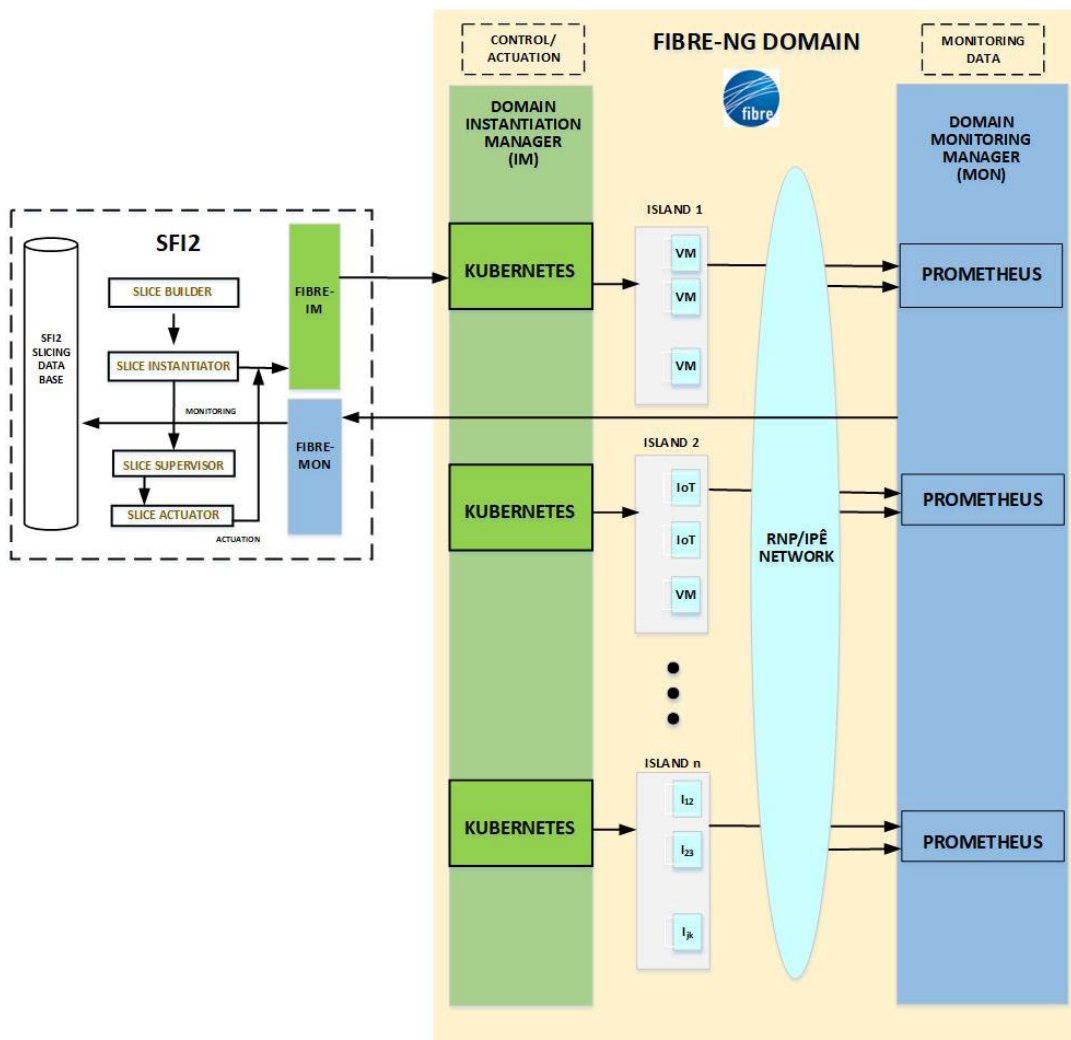
FIGURE 3. SFI2 Architecture Instantiation and Deployment in FIBRE-NG Domain.

single point of access to the architecture/slice. That is, the experimenter and end-user use the same environment for management, configuration, and access to the slice. In this way, the SFI2 architecture can have access control and insert security levels. It is assumed that an experiment can request end-to-end communication, including being a request on the slice template at creation time. With the single point of access, this request from the experimenter can be met with the integration of the endpoint device (the gateway) and how the end client connects to that gateway (e.g. VPN). So, as these issues are pertinent, they will be discussed soon, with the current SFI2 architecture being an experimental system, with security updates focused on the slice life cycle.

V. SFI2 INSTANTIATION AND DEPLOYMENT OVER EXPERIMENTAL NETWORK DOMAINS

This section illustrates how SFI2 reference architecture is instantiated and deployed over a specific experimental network domain and highlights how the reference architecture

addresses multi-domain and multi-technology aspects when integrating multiple experimental networks.

One of the contributions of the SFI2 project is its capability to integrate existing experimental testbeds scattered around different institutions (universities, research centers, non-governmental institutions, and others) into a single, multi-domain experimental testbed. Each integrated testbed will run an instance of its domain management components so that SFI2 experimenters can book resources like containers, virtual machines, bare metal, and IoT devices in these instances. The SFI2 orchestrator handles these resources to provide network slicing on top of SFI2 target domains.

Fig. 3 illustrates the physical and logical elements, modules, and components involved in the instantiation of the SFI2 reference architecture for the FIBRE-NG experimental domain [7].

The FIBRE-NG domain is an experimental network composed of islands hosting resources (VMs, containers, and bare metal) for experimentation and the IPÊ network [49]. The islands are physically located in universities and research
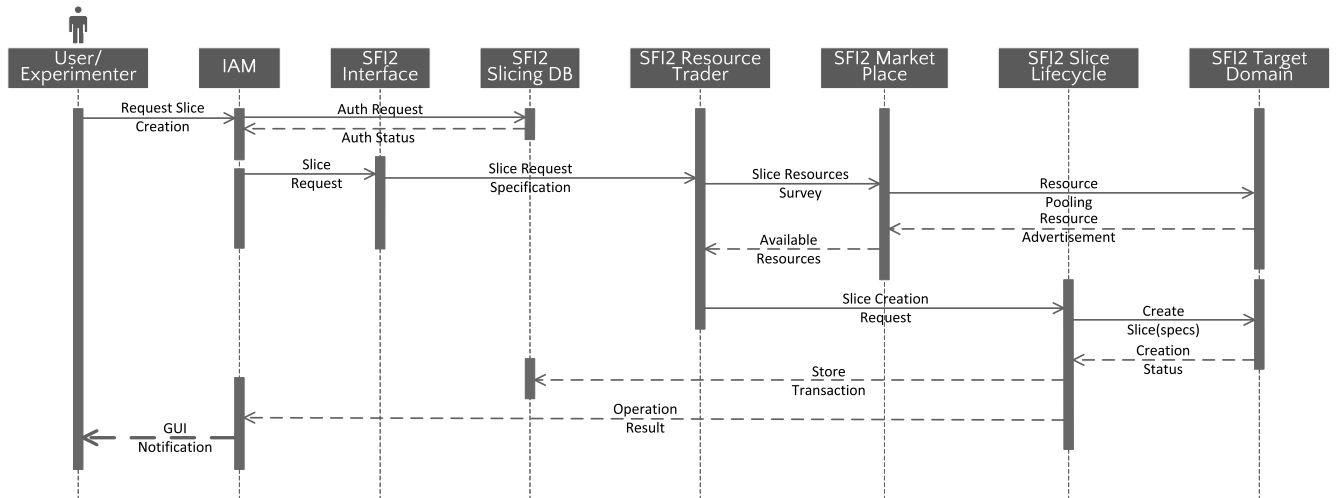
FIGURE 4. Slicing Creation Flow Interactions.

centers scattered in Brazil from north to south, and the IPÊ network provides the necessary network interconnection among islands to support running distributed experiments. FIBRE-NG has 18 active islands, allowing an experimenter to set up and run distributed experiments on a geographically extensive real network. Regarding technology, the FIBRE-NG supports container deployment based on Kubernetes [50] and has a monitoring infrastructure based on Prometheus [51] for its geographically distributed islands and the IPÊ interconnection network.

At this point, it is essential to highlight that the FIBRE-NG experimental network has independent setup and experiment running support for experimenters [52]. As such, the SFI2 instantiation and deployment in the FIBRE-NG domain is an additional alternative to configuring resources for experimentation. SFI2 slicing over the FIBRE-NG will complement and add new resources and benefits to FIBRE-NG users by incorporating ML-native optimization, energy-efficient resource utilization, and slicing-tailored security functionalities. Beyond that, the integration with other experimental domains will allow experimenters to allocate services, platforms, 5G functions, and IoT device resources hosted by other experimental domains.

As illustrated in Figure 3, the SFI2 deployment over the FIBRE-NG experimental network uses a domain interface manager (DOM-IM) based on Kubernetes (FIBRE-IM) to allocate and deallocate slicing resources such as VMs, containers, and bare-metal in the FIBRE-NG islands.

The SFI2 resource orchestrator (Figure 3) enhances and takes precedence over the FIBRE-NG Kubernetes orchestration stream to handle the management and lifecycle of network slices. Accordingly, slice instantiation is achieved through the Kubernetes-aware FIBRE-IM, a DOM-IM module customized for this specific domain. The modular DOM-IM approach of the SFI2 architecture agnostically facilitates the integration of distinct experimental

domains. Since SFI2 has ML-native optimization features, slice supervision may dynamically reconfigure slices in the FIBRE-NG domain using the FIBRE-IM or, in any other domain, making use of its specific DOM-IM. In general, the SFI2 resource orchestrator has specialized functions such as deployment in target domains with heterogeneous virtualization technology, full-stack monitoring requirements, and specific configurations for enabling inter-domain isolation.

The domain monitoring interface of SFI2 (DOM-MON) (Figure 3) is the abstraction used to agnostically monitor the components involved in the creation, operation, and management of slices. In the context of the FIBRE-NG domain deployment, the FIBRE-MON module is the element that interfaces SFI2 modules with the Prometheus FIBRE-NG native monitoring system. FIBRE-MON module allows the monitoring of the islands, allocated virtual machines, bare-metal, and the interconnection backbone provided by the IPÊ network.

When integrated through the SFI2 reference architecture, other experimental testbeds will provide different resources like IoT and drones on the SFI2 marketplace. For example, an experimental testbed focusing on 5G may provide resources related to the 5G Core and the 5G Radio interface. In contrast, a cloud testbed may provide common platforms as a service or even machine learning such as Jupyter notebooks and compute-intensive applications such as Apache Spark and Apache Kafka.

The resource heterogeneity inherently existing in multi-domain and multi-technology experimental networks poses challenges over the current state-of-the-art slicing orchestration, especially because end-to-end network service has stringent requirements. The SFI2 architecture addresses these challenges by adopting natively intelligent orchestration, as illustrated in the discussed FIBRE-NG instantiation and deployment.
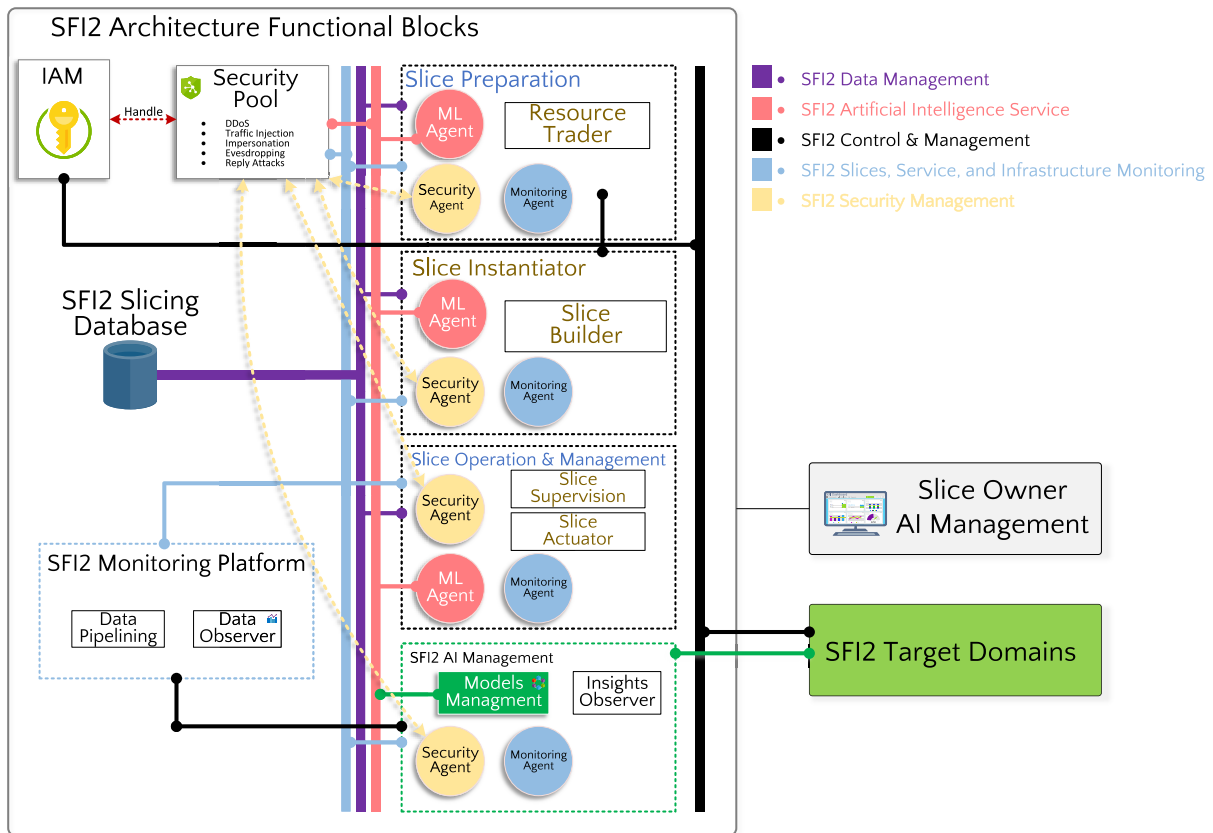
FIGURE 5. Security Enhancement for SFI2 Reference Architecture.

VI. EXPERIMENTAL ASSESSMENT

Aiming to validate our architectural enhancements, we propose a two-fold experimental scenario to assess the functionalities of our slicing orchestration architecture. This testing scenario showcases how AI techniques are essential for secure, sustainability-aware network slicing architectures.

Our experimental flow follows Fig. 4, which depicts the deployment flow diagram of network slicing through the SFI2 Architecture. Initially, we outline the enhancements in security within slice orchestration architectures achieved through the utilization of native and distributed machine learning agents within the architectural blocks. Subsequently, we discuss the advancements in the context of sustainability.

A. SECURITY

We built an experimental scenario to evaluate the security enhancement of the SFI2 Architecture that combines Machine Learning (ML) techniques with a distributed security approach oriented to the life cycle of the network slice. Fig. 5 represents with more detail the conceptual blocks of the SFI2 Architecture. It highlights the network slice orchestration and security blocks that are the Identity and Access Management (IAM) and Security Pool. The SFI2 Architecture has different data, control, and management planes for the different services and architectural blocks.

The SFI2 Security Management plane is responsible for security control and enforcement in the functional blocks of the SFI2 Architecture. In this security control plane, asynchronous interaction exists between it and all the available blocks of the SFI2 Architecture. The IAM Block is responsible for the authentication and authorization of users and the functional blocks that make up the SFI2 Architecture. IAM interacts with the Security Pool, enabling the architecture manager or the owner of the network slice to use the necessary security mechanisms for its deployment.

Our architectural framework can deal with the following security threats: DDoS, traffic injection, impersonation, tampering, eavesdropping, reply Attacks, and interface monitoring. The current literature regarding slicing architectures does not cover these security aspects widely. We use a distributed security mechanism natively integrated with the functional blocks of the architecture. The interaction between the security mechanisms with the ML-Agents distributed throughout the architecture and its functional blocks is responsible for this distributed approach. An ML-Agent works alongside the slicing orchestration blocks enabling them to apply predictions, forecasting, and classification on demand, acting as an Application Programming Interface (API) of ML services for the architecture block. Thus, an ML-Agent in Slice Preparation acts differently from the ML-Agent present in the Slice Instantiation block.
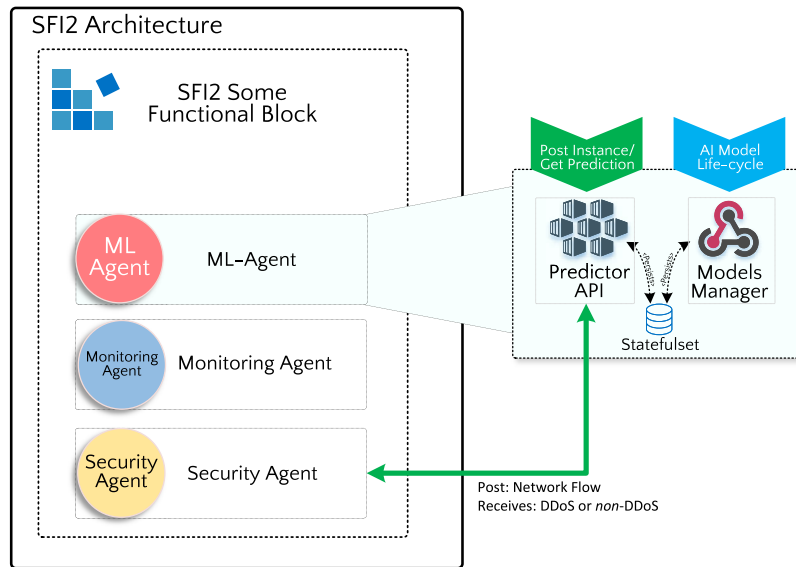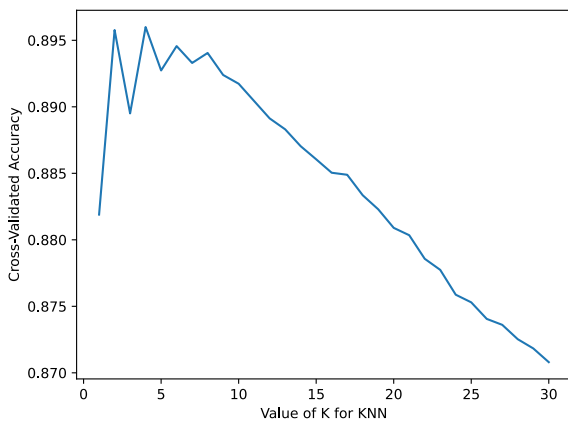
FIGURE 6. ML-Agent Specification and Functionalities.

FIGURE 7. K-Nearest Neighbors (KNN) for Distributed Denial of Service (DDoS) Attacks Prediction.

with native Artificial Intelligence (AI) and security. For this, as Fig. 6, we take a functional block of the architecture and exploit its roles and interfaces of the ML-Agent. ML-Agent provides two types of services, one is provided by the Predicor API which comprises of an API which takes data as input and returns a ML prediction as a response. The other functionality of the AI-Agent comes through the AI Model Life-Cycle, which is where the AI-Agent interacts with the SFI2 AI Management (Fig. 5) to insert, remove or update models from ML accordingly.

In this experiment, using SFI2 AI Management, we trained some ML models with a DDoS dataset in order to finally have an accurate ML model capable of responding to a given network flow if deals with DDoS and or benign traffic. At the end of the training, the model was exported and loaded into the AI-Agent through the ML-Agent's AI Model Life-Cycle interface. At this point, the Security Agent can query the Predictor API, providing a sample of the network flow and receiving as a response the classification of the network flow according to whether the profile is DDoS or benign.

2) DATASET

For that, we trained several ML models using the AI Management block considering the DDoS-2019 [54] dataset. This dataset contains packets representing DDoS attacks in raw *pcap* format. Thus, using the FlowMeter [55], a flow sampling tool, which is a time-based features extractor tool, we train our ML algorithms on these collected flows. The flows that the tool extracted contain more than 80 time-based features with many DDoS attacks, making it possible to apply ML algorithms to extract patterns from these features. Furthermore, once we train the models through SFI2 AI Management, it is possible to export the trained model to the ML-Agents that are distributed throughout the architecture to

The SFI2 AI Management Block is where the architecture manager and the network slice owner manage the AI services the architecture supports. Thus, the selection of an AI service for each ML-Agent, as well as the training of the ML algorithm, takes place in this functional block [53]. Additionally, the architecture provides the SFI2 Monitoring Platform block, which monitors each component of the architecture and the orchestration services that run on top of it. Thus, to validate the distributed security mechanism that the SFI2 Architecture brings, we evaluated the empowering of DDoS Defense in the architecture blocks. This security mechanism aims to empower the functional blocks of the architecture against DDoS attacks that can lead to its instability or unavailability.

1) EXPERIMENTAL SCENARIO

We propose the experimental scenario in Fig. 6 to functionally validate our hypothesis of building a slicing architecture

TABLE 3. Accuracy for DDoS Attacks Classification.

Algorithm	Accuracy	Training Time (seconds)
KNN	94%	0.026
Random Forest	92%	4.379
SVM	93%	36.920
MLP	95%	542.661

carry out predictions, forecasting, and classifications for the functional blocks they require.

Each architectural block contains a mechanism for sampling packets and classifying them according to DDoS traffic class, using FlowMeter technology. Thus, we train ML algorithms considering the following traffic classes: Benign, DoS-DNS, DoS-MSSQL, DoS-NetBIOS, DoS-SNMP, DoS-UDP, Syn, TFTP, and UDP-lag which are malign. For training the ML models we use the strategy of dividing the dataset 80% for training and 20% for testing. In our training strategy, we use the following ML algorithms: KNN, Random Forest, Decision Tree, and Multilayer Perceptron (MLP). The objective of this experiment is to validate the onboarding SFI2 Architecture block with ML capabilities in order to classify whether certain traffic refers to DDoS attacks or is benign. For this, we use the training time and accuracy metrics to measure how capable ML-Agents are of detecting DDoS Attacks against the functional blocks of the architecture.

3) RESULTS AND DISCUSSION

Thus, we train all ML algorithms considering the dataset and present their accuracies according to Table 3. According to Table 3, we confirmed that MLP produces the best accuracy among its peers. However, it requires a significantly higher training time than its peers. On the other hand, KNN performed well in terms of accuracy while taking the least amount of time to train.

Furthermore, we dived into behavior KNN algorithm to classify DDoS Attacks to measure how their accuracy changes depending on the choice of K. For this, we performed cross-validation using and made several separations of training and testing to evaluate the model in various sampling scenarios. Thus, we vary the K from 1 to 30 and measure its accuracy according to Fig. 7. As this is cross-validation, for each K, we obtained average accuracies for ten (10) different executions, and according to Fig. 7 with $K = 4$, we obtained the best accuracy of the model, with an average of 0.895. Subsequently, as the value of K increases, accuracy drops slightly.

Thus, after training the ML models, they can be distributed and activated by the ML-Agents along the functional blocks of the SFI2 Architecture to empower these blocks of DDoS attacks that can compromise or disable their operation. Furthermore, it is imperative to point out that attacks vary over time, requiring improvement of the model that ML-Agent uses. After verifying a DDoS attack, the functional block can make some decisions regarding the originator of the malicious traffic, such as dropping the traffic from one of the origins.
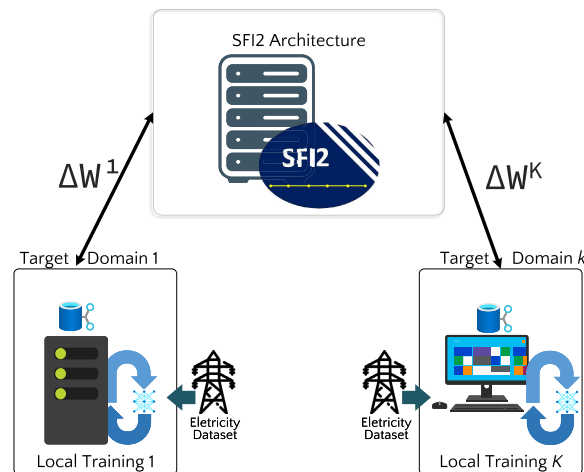
FIGURE 8. Experimental Setup for Sustainability of SFI2 Reference Architecture.

B. SUSTAINABILITY

We built an experimental scenario to validate the architectural enhancement proposed in SFI2, especially regarding sustainability. Thus, according to Fig. 8, we consider two different target domains that deliver network slices with specific purposes. These target domains have specific energy sources, so we built a forecasting scenario for electricity consumption in each target domain using the distributed learning paradigm.

We validate our enhancement suitability with Convolutional Neural Network (CNN), specifically Long Short-Term Memory (LSTM) for energy forecasting in each target domain using the SFI2 AI Management block. After training each ML model, they are appropriately distributed to the ML-Agent using each domain as shown in Figure 5. After then, the SFI2 architecture can handle energy consumption forecasting.

To validate the forecasting capability of the distributed training, we used the Mean Squared Error (MSE) metric that measures the difference between the forecast and the actual in a time series. For the proposed experimental scenario, we used the well know neural network the LSTM [56].

1) DATASET

In Fig. 8, we have a representation of two target domains containing different datasets referring to electricity consumption. The first dataset refers to the Duquesne Light Company's electricity consumption. It contains the multivariate time series of the electricity consumption of the city of Pittsburg, containing the interval December 2005 to January 2018 [57]. The second, Steel Industry Energy Consumption Dataset, refers to the electricity consumption of the steel sector in South Korea, containing the record of consumption from January 1, 2018, to December 30, 2018, and the consumption of kWh [58].

Thus, the SFI2 resource orchestrator interacts with the two target domains that locally proceed with local data training. We divide the two datasets to 80% for training and 20% for
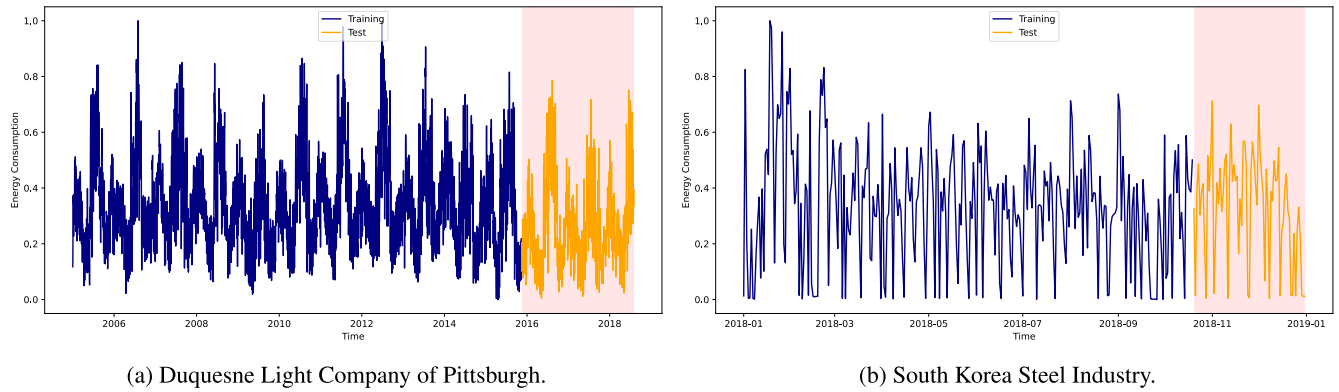
(a) Duquesne Light Company of Pittsburgh.

(b) South Korea Steel Industry.

FIGURE 9. Electricity Consumption – Dataset Division.

(a) Training Loss Behavior of Target Domain 1.

(b) Training Loss Behavior of Target Domain 2.

FIGURE 10. Training Loss Behavior of Target Domains.

(a) Energy Forecasting Test in Target Domain 1.

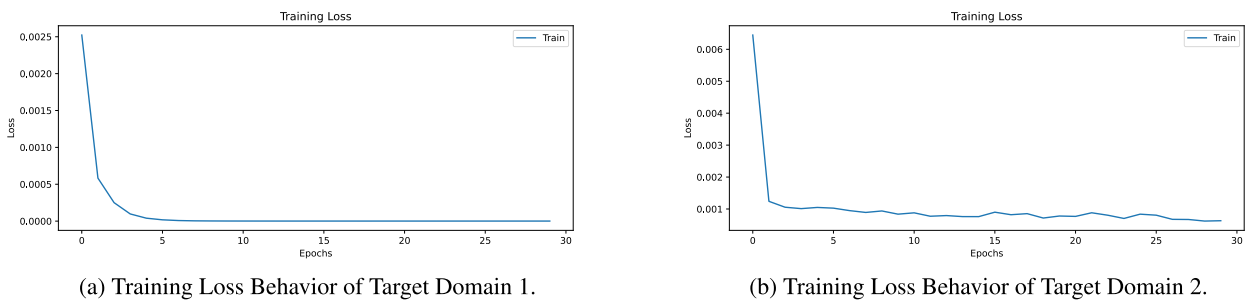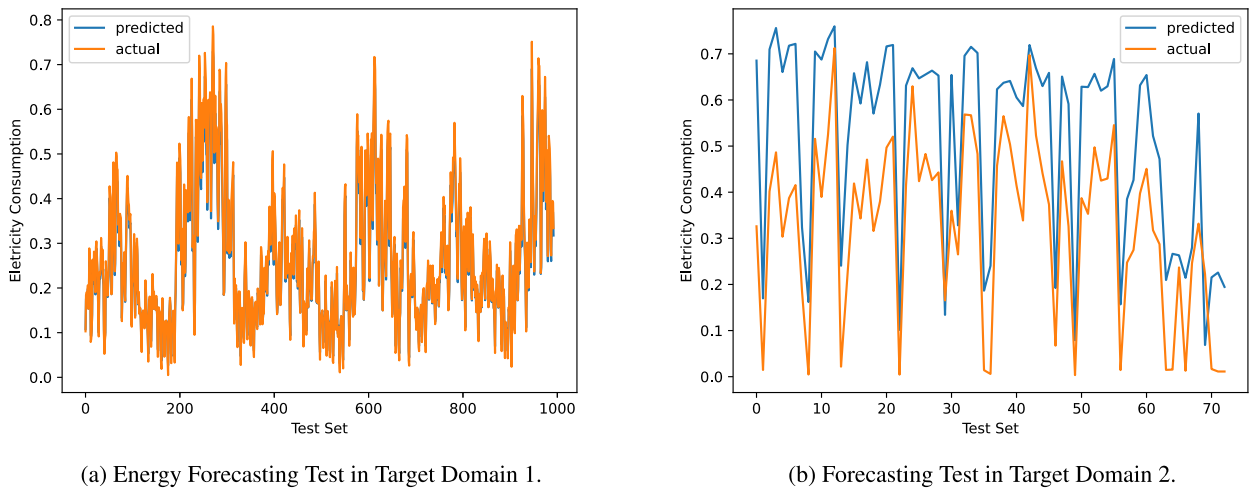(b) Forecasting Test in Target Domain 2.

FIGURE 11. Energy Forecasting Performance Test of SFI2 Reference Architecture.

testing according to Fig. 9, and we consider a 30-day window for future forecasting in the test set. For reproducibility purposes, we let open the dataset and code artifacts available at https://github.com/romoreira/SFI2-Energy-Sustainability.

2) RESULTS AND DISCUSSION

We performed experiments in the proposed scenario to verify the suitability of distributed training for the sustainability use case. Thus, each target domain trained an CNN for forecasting time series and reported the model weights to the central model stored by SFI2 Architecture. In addition, we recorded a global MSE of 0.0014 on average, which means that the global model's error received the weights of the target domains trained locally with the electricity consumption datasets. Thus, Fig. 10 depicts the generalization and learning capacity of the model. Given the behavior of the graph, it is suggestive of admitting that the neural network in each target domain was able to learn appropriately due to the descending of the Loss metric.

In addition, we evaluated the ability of the SFI2 Slicing Reference Architecture global model to forecast the electricity consumption of those target domains. We randomly tested the global model using some tested target domains. According to Fig. 11, distributed learning shows promising results for forecasting electricity consumption in future slicing architectures. We estimated the difference between the actual and the predicted in the forecasting process. The electricity consumption forecast was very accurate, according to its behavior in the time series graph between the actual and predicted curves Fig. 11. The error rate is low such that the time series follow similar behavior for both target domains 1 and 2. Our investigation opens up opportunities for further investigation into how sustainability initiatives move toward built-in AI-capabilities in network slicing architectures.

Our sustainability enhancement opens up research opportunities especially considering our distributed artificial intelligence approach. Forecasting target domain energy consumption allows the SFI2 Architecture to ponder its network slicing decisions against the energy constraints of each target domain. Our security-oriented and AI-native architecture fosters a high customization level of slicing architecture.

VII. FINAL CONSIDERATIONS

The new SFI2 network slicing reference architecture fills an existing gap resulting from the diversity of NS architecture's target domains by integrating multi-domain and multi-technology experimental network infrastructures. The experimental network integration is enhanced by embedding machine learning native optimizations, energy-efficient slicing, and slicing-tailored security functionalities. An essential architectural design aspect is that although the SFI2 instantiation and deployments were focused on integrating Brazilian experimental testbeds (FIBRE-NG, CloudNEXT, FUTEBOL, FIWARE, 5GINFIRE, and NECOS), the agnostically defined domain and monitoring interfaces (DOM-IM and DOM-MON) allow instantiation to distinct experimental domains. Moreover, the generic embedded enhancements (ML-native optimization, energy efficiency, and tailored security functions) will enable the use of the SFI2 reference architecture in domains other than the experimental ones.

Beyond technical achievements and enhancements, the SFI2 reference architecture significantly benefits the research community by fostering the utilization of currently available and deployed experimental testbeds. The gains are twofold, with enhancements to the current infrastructures and simultaneously allowing the reuse of the infrastructures with additional value. In practice, the achieved gains mean having more extensive resources (VMs, 5G functions, IoT, and others) for experimenters by integrating the infrastructures.

The SFI2 architecture contributes to the network slicing state-of-the-art in various ways. Initially, the SFI2 architecture focuses on integrating experimental networks and allowing the creation, operation, and decommissioning of independent and isolated slices on distinct experimental network domains, fulfilling an existing research gap. These results in reusing available infrastructures, thus reducing capital expenditure (CAPEX) and operational expenditure (OPEX) for the institutions involved with the integrated experimental networks. Additionally, slicing in the SFI2 architecture incorporates significant global values and principles by adopting a sustainability-aware dynamic resource discovery and leasing for multi-domain experimental networks.

Besides, the modular and agnostic design characteristics of the SFI2 main interface modules with the experimental domains through DOM-IM and DOM-MON, together with the embedded ML-native optimizations and slice-tailored security functions, push the network slicing paradigm to the level of functionalities required by current and future users and applications.

Several research opportunities lie ahead using the proposed architecture. First, it is necessary to extend SFI2 to support a more significant number of experimental and possibly operational networks. We expect to face new challenges as we include new domains and technologies in a multi-domain scenario. Second, the ML selection for each optimization task is challenging, extending and evaluating different approaches. In this context, the training datasets, i.e., data collection and labeling for each domain and technology, should be investigated and enhanced for slice-as-a-service.

Finally, the SFI2 architecture allows for advancing new research challenges. For example, providing comprehensive security tests to prevent zero-day attacks is critical. Moreover, tests of reconfiguration of slices considering the elasticity of resource allocation according to demand and sustainable approaches are desirable for future architecture versions. In resource allocation, testing and guaranteeing the isolation of network slices created as services is also essential.

REFERENCES

[1] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984.

[2] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.

[3] Z. Mlika and S. Cherkaoui, "Network slicing with MEC and deep reinforcement learning for the Internet of Vehicles," *IEEE Netw.*, vol. 35, no. 3, pp. 132–138, May 2021.

[4] Y. Wu, H. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1175–1211, 2nd Quart., 2022.

[5] Z. Yuan and G. Muntean, "AirSlice: A network slicing framework for UAV communications," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 62–68, Nov. 2020.

[6] G. N. Dias, J. F. Rezende, L. N. Ciuffo, I. Machado, F. D. O. Silva, T. C. de Brito, F. F. Redigolo, J. S. B. Martins, L. N. Sampaio, and A. J. G. Abelem, "SFI2—Slicing future internet infrastructures project," in *Proc. Global Exp. Future Internet (GEFI)*, Coimbra, Portugal, Nov. 2019, pp. 1–3.

[7] A. Abelem, M. Stanton, I. Machado, M. Salvador, L. Magalhaes, N. Fernandes, S. Correa, K. Cardoso, C. Marcondes, J. Martins, J. Monteiro, T. Carvalho, and J. Rezende, "FIT@ BR—A future internet testbed in Brazil," in *Proc. APAN Netw. Res. Workshop*, Aug. 2013, pp. 1–8.

[8] C. Both, R. Guimaraes, F. Slyne, J. Wickboldt, M. Martinello, C. Dominicini, R. Martins, Y. Zhang, D. Cardoso, R. Villaca, I. Ceravolo, R. Nejabati, J. Marquez-Barja, M. Ruffini, and L. DaSilva, "FUTEBOL control framework: Enabling experimentation in convergent optical, wireless, and cloud infrastructures," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 56–62, Oct. 2019.

[9] Atmosphere. (2019). *CloudNext Testbed—Atmosphere*. [Online]. Available: https://www.atmosphere-eubrazil.eu/cloudnext-testbed

[10] C. T. Oliveira, R. Moreira, F. d. O. Silva, R. S. Miani, and P. F. Rosa, "Improving security on IoT applications based on the FIWARE platform," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 686–693.

[11] A. P. Silva, C. Tranoris, S. Denazis, S. Sargento, J. Pereira, M. Luís, R. Moreira, F. Silva, I. Vidal, B. Nogales, R. Nejabati, and D. Simeonidou, "5GinFIRE: An end-to-end open5G vertical network function ecosystem," *Ad Hoc Netw.*, vol. 93, Oct. 2019, Art. no. 101895. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870518309387

[12] S. Clayman, A. Neto, F. Verdi, S. Correa, S. Sampaio, I. Sakelariou, L. Mamatas, R. Pasquini, K. Cardoso, F. Tusa, C. Rothenberg, and J. Serrat, "The NECOS approach to end-to-end cloud-network slicing as a service," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 91–97, Mar. 2021.

[13] NGMN. (2016). *5G Security Recommendations Package #2: Network Slicing*. [Online]. Available: https://www.ngmn.org/wp-content/uploads/Publications/2016/160429_NGMN_5G

[14] F. Salahdine, Q. Liu, and T. Han, "Towards secure and intelligent network slicing for 5G networks," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 23–38, 2022.

[15] 3GPP. (2021). *Management and Orchestration;Concepts, Use Cases and Requirements (Release 17)*. Accessed: Jun. 20, 2022. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/28_series/28.530/

[16] J. Ordonez-Lucena, P. Ameigeiras, L. M. Contreras, J. Folgueira, and D. R. López, "On the rollout of network slicing in carrier networks: A technology radar," *Sensors*, vol. 21, no. 23, p. 8094, Dec. 2021.

[17] X. Shen, J. Gao, W. Wu, K. Lyu, M. Li, W. Zhuang, X. Li, and J. Rao, "AI-assisted network-slicing based next-generation wireless networks," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 45–66, 2020.

[18] W. Guan, H. Zhang, and V. C. M. Leung, "Customized slicing for 6G: Enforcing artificial intelligence on resource management," *IEEE Netw.*, vol. 35, no. 5, pp. 264–271, Sep. 2021.

[19] *D3.1: NECOS System Architecture and Platform Specification*, document D3.1, NECOS Project, UPC, Spain, Oct. 2018. [Online]. Available: http://www.maps.upc.edu/public/NECOS%20D3.1%20final.pdf

[20] F. Debbabi, R. Jmal, and L. C. Fourati, "5G network slicing: Fundamental concepts, architectures, algorithmics, projects practices, and open issues," *Concurrency Comput. Pract. Exper.*, vol. 33, no. 20, Oct. 2021, Art. no. e6352.

[21] *Next Generation Protocols (NGP); E2E Network Slicing Reference Framework and Information Model*, ETSI Group, Sophia Antipolis, France, document NGP 011, 2018.

[22] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Netw.*, vol. 34, no. 2, pp. 186–194, Mar. 2020.

[23] M. Chahbar, G. Diaz, A. Dandoush, C. Cérin, and K. Ghoumid, "A comprehensive survey on the E2E 5G network slicing model," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 1, pp. 49–62, Mar. 2021.

[24] *Applying SDN Architecture to 5G Slicing*, Open Networking Foundation, Palo Alto, CA, USA, document TR-526, Apr. 2016.

[25] *Framework of Network Virtualization for Future Networks*, Telecommunication Standardization Sector of ITU-T, Geneva, Switzerland, document ITU-T Y.3011, 2012.

[26] A. Napolitano, A. Giorgetti, K. Kondepu, L. Valcarenghi, and P. Castoldi, "Network slicing: An overview," in *Proc. IEEE 4th Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2018, pp. 1–4.

[27] C. J. Bernardos, O. Dugeon, A. Galis, D. Morris, C. Simon, and R. Szabo, "5G exchange (5GEx)—Multi-domain orchestration for software defined infrastructures," in *Proc. Eur. Conf. Netw. Commun.*, Paris, France, Jul. 2015, pp. 1–5.

[28] G. Xilouris, S. Kolometsos, C. Xilouris, J. F. Hidalgo, S. Siddiqui, A. Rocha, S. Castro, F. Vicens, and J. Martrat, "Devops based service orchestration in 5G virtualised networks–SONATA project demo," in *Proc. IEEE Conf. Netw. Softwarization (NetSoft)*, Jul. 2017, pp. 1–3.

[29] I. Afolabi, A. Ksentini, M. Bagaa, T. Taleb, M. Corici, and A. Nakao, "Towards 5G network slicing over multiple-domains," *IEICE Trans. Commun.*, vol. E100.B, no. 11, pp. 1992–2006, 2017.

[30] A. M. Escolar, J. M. A. Calero, and Q. Wang, "Scalable software switch based service function chaining for 5G network slicing," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[31] L. Briguglio, P.-J. Nesse, A. Di Giglio, C. Occhipinti, P. Durkin, and I. Markopoulos, "Business value and social acceptance for the validation of 5G technology," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Sep. 2021, pp. 132–137.

[32] L. Vignaroli, M. Gramaglia, M. Fuentes, A. Casella, R. Odarchenko, L. Natale, B. Altman, and F. D'Andria, "The touristic sector in the 5G technology era: The 5G-TOURS project approach," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2020, pp. 1–6.

[33] I. Mesogiti, "5G-VICTORI: Future railway communications requirements driving 5G deployments in railways," in *Proc. Artif. Intell. Appl. Innov. (AIAI)*, Jun. 2021, pp. 21–30.

[34] Li, Xi, A. Garcia-Saavedra, X. Costa-Perez, C. J. Bernardos, C. Guimarães, K. Antevski, J. Mangues-Bafalluy, J. Baranda, E. Zeydan, D. Corujo, P. Iovanna, G. Landi, J. Alonso, P. Paixão, H. Martins, M. Lorenzo, J. Ordonez-Lucena, and D. R. López, "5Growth: An end-to-end service platform for automated deployment and management of vertical services over 5G networks," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 84–90, Mar. 2021.

[35] R. Moreira, P. F. Rosa, R. L. A. Aguiar, and F. D. O. Silva, "NASOR: A network slicing approach for multiple autonomous systems," *Comput. Commun.*, vol. 179, pp. 131–144, Nov. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421002917

[36] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019.

[37] *5G End to End Key Performance Indicators (KPI) (Release 17)*, document TS 128.554, version 17.8.0, ETSI, Sophia Antipolis, France, 3GPP, Oct. 2022.

[38] S. Kukliński and L. Tomaszewski, "Key performance indicators for 5G network slicing," in *Proc. IEEE Conf. Netw. Softwarization (NetSoft)*, Jun. 2019, pp. 464–471.

[39] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, N. Zhang, X. S. Shen, and W. Zhuang, "AI-native network slicing for 6G networks," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 96–103, Feb. 2022.

[40] N. M. Nasir, S. Hassan, and K. M. Zaini, "Evolution towards 6G intelligent wireless networks: The motivations and challenges on the enabling technologies," in *Proc. IEEE 19th Student Conf. Res. Develop. (SCOReD)*, Nov. 2021, pp. 305–310.

[41] A. Domeke, B. Cimoli, and I. T. Monroy, "Integration of network slicing and machine learning into edge networks for low-latency services in 5G and beyond systems," *Appl. Sci.*, vol. 12, no. 13, p. 6617, Jun. 2022.

[42] A. Strategy, "SMARTer2030: ICT solutions for 21st century challenges," Global eSustainability Initiative (GeSI), Brussels, Brussels-Capital Region, Brussels, Belgium, Tech. Rep. 3, 2015, vol. 3.

[43] A. Bassen and A. M. M. Kovács, "Environmental, social and governance key performance indicators from a capital market perspective," in *Proc. Wirtschafts-Und Unternehmensethik*. Cham, Switzerland: Springer, 2020, pp. 809–820.

[44] N. Khattar, J. Sidhu, and J. Singh, "Toward energy-efficient cloud computing: A survey of dynamic power management and heuristics-based optimization techniques," *J. Supercomput.*, vol. 75, no. 8, pp. 4750–4810, Aug. 2019.

[45] Z. Kotulski, T. W. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Towards constructive approach to end-to-end slice isolation in 5G networks," *EURASIP J. Inf. Secur.*, vol. 2018, no. 1, pp. 1–23, Dec. 2018.

[46] V. A. Cunha, E. da Silva, M. B. de Carvalho, D. Corujo, J. P. Barraca, D. Gomes, L. Z. Granville, and R. L. Aguiar, "Network slicing security: Challenges and directions," *Internet Technol. Lett.*, vol. 2, no. 5, Sep. 2019, Art. no. e125.

[47] J. Wang, *Computer Network Security: Theory and Practice*, 1st ed. Berlin, Germany: Springer, 2009.

[48] J. H. G. M. Corrêa, E. A. Sousa Jr., I. E. Fonseca, V. Nigam, M. R. N. Ribeiro, and R. S. Villaça, "Selectivity and autoscaling as complementary defenses for DDoS protection to cloud services," in *Proc. IEEE 8th Int. Conf. Cloud Netw. (CloudNet)*, Nov. 2019, pp. 1–3.

[49] V. Zanotelli, G. Comarela, R. Villaca, and M. Martinello, "Caracterização e previsão de falhas em serviços de conectividade: Uma aplicação à rede ipê," in *Proc. Anais do 39th Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Porto Alegre, RS, Brasil: SBC, 2021, pp. 141–154.

[50] P. Raj, S. Vanga, and A. Chaudhary, "Kubernetes architecture, best practices, and patterns," in *Cloud-Native Computing: How to Design, Develop, and Secure Microservices and Event-Driven Applications*. Hoboken, NJ, USA: Wiley, 2023, pp. 49–70.

[51] N. Sukhija and E. Bautista, "Towards a framework for monitoring and analyzing high performance computing environments using kubernetes and prometheus," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov.*, Aug. 2019, pp. 257–262.

[52] R. N. P. Rede Nacional de Pesquisa. (2022). *FIBRE—Future Internet Brazilian Environment for Experimentation*. [Online]. Available: https://www.fibre.org.br/

[53] R. Moreira, J. S. B. Martins, T. C. M. B. Carvalho, and F. d. O. Silva, "On enhancing network slicing life-cycle through an AI-native orchestration architecture," in *Proc. Adv. Inf. Netw. Appl.*, L. Barolli, Ed. Cham, Switzerland: Springer, 2023, pp. 124–136.

[54] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–8.

[55] A. H. Lashkari, A. Seo, G. D. Gil, and A. Ghorbani, "CIC-AB: Online ad blocker for browsers," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2017, pp. 1–7.

[56] M. Sundermeyer, R. Schlüter, and H. Ney, "LSTM neural networks for language modeling," in *Proc. Interspeech*, Sep. 2012, pp. 194–197.

[57] M. Bilal, H. Kim, M. Fayaz, and P. Pawar, "Comparative analysis of time series forecasting approaches for household electricity consumption prediction," 2022, *arXiv:2207.01019*.

[58] D. Dua and C. Graff. (2017). *UCI Machine Learning Repository*. [Online]. Available: http://archive.ics.uci.edu/ml

JOBERTO S. B. MARTINS (Life Senior Member, IEEE) received the Ph.D. degree in computer science from Université Pierre et Marie Curie (UPMC), Paris, in 1986. He was a Postdoctoral Researcher with ICSI—Berkeley University, in 1995, and Postdoctoral Senior Researcher with Paris Saclay University, France, in 2016. He has been an International Professor with Hochschule für Technik und Wirtschaft des Saarlandes (HTW), Germany, since 2004, and Université d'Evry, France. He is currently a Full Professor in computer science with Salvador University (UNIFACS) and the Director of NUPERC and IPQoS research groups. His research interests include network slicing, resource allocation, machine learning, software-defined networking, smart grids, and smart city. He is also a key speaker, a teacher, and an invited lecturer at various international congresses and companies in Brazil, USA, and Europe.

TEREZA C. CARVALHO is currently an Associate Professor with Escola Politécnica, University of São Paulo (USP), and a Visiting Professor with Université Paris 1 Panthéon-Sorbonne. She has been the Founder and a general Coordinator with the Laboratory of Sustainability on ITC (LASSU), since 2010, and the Center for Reuse and Discard of Informatics Residuals (CEDIR-USP), since 2009. She is also a former Assessor with CTI—USP (Information Technology Coordination), from 2010 to 2013, and the Director of CCE-USP (Electronic Computing Center), from 2006 to 2010. She was a Sloan Fellow with the Massachusetts Institute of Technology (MIT), in 2002. She has been coordinating international and national research and development projects, since 2000, in green computing, cloud computing, IT energy efficiency, IT governance, digital technologies applied to the Amazon production chains, waste electrical and electronic equipment (WEEE), future internet, scientific DMZ, and security. She holds several international patents.

RODRIGO MOREIRA received the B.S. degree from the Federal University of Viçosa, in 2014, and the M.S. degree and the Ph.D. degree in computer science from the Federal University of Uberlândia, Brazil, in 2017 and 2021, respectively. He is currently a Professor with the Federal University of Viçosa. His research interests include future internet, the quality of service, cloud computing, network function virtualization, software-defined networking, and edge computing.

CRISTIANO BONATO BOTH is currently a Professor with the Applied Computing Graduate Program, University of Vale do Rio dos Sinos (UNISINOS), Brazil. He coordinates research projects funded by H2-1.52-1.5 EU-Brazil, CNPq, FAPESP, and RNP. His research interests include wireless networks, next-generation networks, softwarization, and virtualization technologies for telecommunication networks.

ADNEI DONATTI received the Bachelor of Technology degree and the M.Sc. degree in applied computing from Santa Catarina State University (UDESC). He is currently pursuing the Ph.D. degree with the University of São Paulo (USP). He is also working with resource allocation for network slicing on the SFI2 project. His research interests include cloud computing, distributed systems, and computer networks.

JOÃO H. CORRÊA received the B.Sc. degree in computer networks from the Federal Institute of Paraíba (IFPB), in 2015, the M.Sc. degree in computer science from the Federal University of Paraíba (UFPB), in 2017, and the Ph.D. degree in computer science from the Federal University of Espírito Santo (UFES), in 2021. He is currently an Assistant Professor with the Federal University of Ceará (UFC). His current research interests include computer networks, software-defined networks, network security, and cloud computing.

JOSÉ A. SURUAGY (Member, IEEE) received the Graduate degree in electrical engineering from the Federal University of Pernambuco (UFPE), in 1979, the master's degree in electrical engineering from the University of São Paulo (USP), in 1982, and the Ph.D. degree in computer science from the University of California at Los Angeles (UCLA), in 1990. Has experience in computer science, focusing on telecomputing, acting on the following subjects: computer networks, measurement, quality of service, and performance evaluation. In 2014, received the "Computer Network Brazilian Symposium Distinguished Premium" for his scientific contributions in the areas of computer networks and distributed systems, for his participation in the symposium activities, and for his services that benefitted that community. Currently, he is a Full Professor and a Researcher with Centro de Informática, UFPE.

SAND L. CORRÊA received the bachelor's degree in computer science from the Federal University of Goiás (UFG), in 1994, the M.Sc. degree in computer science from the State University of Campinas (Unicamp), in 1997, and the D.Sc. degree in informatics from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio), in 2011. Since 2010, she has been an Associate Professor with the Institute of Informatics, UFG.

ANTONIO J. G. ABELEM (Member, IEEE) received the Ph.D. degree in computer science from the Catholic University of Rio de Janeiro (PUC-Rio), in 2003. He is currently a Full Professor with the Computer Science Faculty, University of Pará (UFPA), Belém, Pará. He is also an Associate Member and a member of the Board of the Brazilian Computer Society (SBC). He coordinates the Research Laboratory in Computer Network and Multimedia Communication (GERCOM) from which participates and coordinates several national and international projects. In 2020, he was a Visiting Professor with the University of Massachusetts (UMass), Amherst, MA, USA, where he carried out research on quantum networks. His research interest includes networking.

MOISÉS R. N. RIBEIRO received the B.Sc. degree in electrical engineering from Instituto Nacional de Telecomunicações, Brazil, in 1992, the M.Sc. degree in telecommunications from Universidade Estadual de Campinas, Brazil, in 1996, and the Ph.D. degree from the University of Essex, U.K., in 2002. In 1995, he joined the Department of Electrical Engineering, Federal University of Espírito Santo. He was a Visiting Professor with the Photonics and Networking Research Laboratory, Stanford University, from 2010 to 2011. His research interests include fiber optic communication and sensor devices, systems, and networks.

JOSÉ-MARCOS S. NOGUEIRA (Member, IEEE) received the B.S. degree in electrical engineering and the M.S. degree in computer science from Universidade Federal de Minas Gerais (UFMG), Brazil, in 1979, and the Ph.D. degree in electrical engineering/computing from the University of Campinas, in 1985. He is currently a Full Professor (nowadays collaborator retired) in computer science with UFMG. He held a postdoctoral researcher position with UBC, Canada, and had a sabbatical year with universities Pierre et Marie Curie (Paris 6) and Evry Val D'Essonne, France. His research interests include computer, management, wireless sensor, mobile and vehicular, programmable, and security networks. He chaired/headed many activities with UFMG (department, graduate, and undergraduate), where he has been for few months the Dean and the Vice-Dean. He heads the Brazilian multi partner's project PORVIR-5G. He served as the Chair/Co-Chair in several OCs and TPCs. He is a member of diverse editorial boards. In 2015, he was awarded the Computer Network Community Highlight Award.
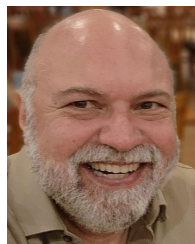
LUIZ C. S. MAGALHÃES received the M.Sc. degree in informatics from Pontifícia Universidade Católica do Rio de Janeiro (PUC-RJ), in 1993, and the Ph.D. degree in computer science from the University of Illinois at Urbana–Champaign, in 2005. He is currently a Professor with the Telecommunications Engineering Department, Universidade Federal Fluminense (UFF), Niterói, Rio de Janeiro. His research interests include mobile computing, transport protocols, and large scale infrastructure.
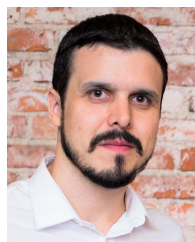
JULIANO WICKBOLDT received the M.Sc. and Ph.D. degrees in computer science from the Federal University of Rio Grande do Sul (UFRGS), Brazil, in 2010 and 2015, respectively. He is currently an Associate Professor with UFRGS. He was an Intern with the NEC Laboratories Europe, Heidelberg, Germany, between 2011 and 2012. In 2015, he was a Visiting Researcher with the Waterford Institute of Technology, Ireland. His research interests include softwarized networking, the IoT, and 5G technologies.

TIAGO C. FERRETO (Member, IEEE) received the Ph.D. degree in computer science from the Computer Science Department, Pontifical Catholic University of Rio Grande do Sul (PUCRS), Brazil, in 2010. He is currently an Associate Professor in computer science with PUCRS, where he is also the Head of Research Group on Networking, Infrastructure, and Cloud Computing (GRIN) and High-Performance Computing Laboratory (LAD). His research interests include cloud and edge computing, IT infrastructure management, computer networks, high-performance computing, and big data. He received the Sandwich Ph.D. Internship from TU-Berlin, Germany (2007–2008).
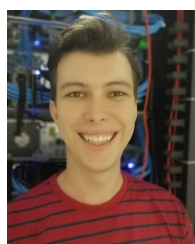
RICARDO MELLO received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Federal University of Espírito Santo (UFES), Brazil, in 2015, 2018, and 2020, respectively. He is currently an Assistant Professor with the Electrical Engineering Department, UFES. His Ph.D. thesis dealt with practical aspects of cloud robotics research and his research resulted recently in a book published in Springer's STAR series. His research interests include cloud robotics, networked systems, autonomous systems, and human–robot interaction.

RAFAEL PASQUINI (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer engineering from the State University of Campinas, in 2006 and 2011, respectively. From 2015 to 2017, he was a Visiting Researcher with the Department of Network and Systems Engineering (NSE), KTH Royal Institute of Technology. Since 2011, he has been an Associate Professor and leads the Distributed Systems and Networks (DSN) research group with the Department of Computer Science, Federal University of Uberlândia. His research interests include network management, the slicing of softwarized infrastructures, machine learning, cloud computing, and software-defined networks.

MARCOS SCHWARZ received the B.Sc. degree in computer science from Santa Catarina State University (UDESC), in 2011, and the M.S. degree in computer engineering from the University of São Paulo (USP), in 2014. He is currently the Research and Development Manager of Brazilian Research and Education Network (RNP). Since 2014, he has been with the Research and Development Team and projects in cyber-infraestructures, involving advanced internet, network performance monitoring, dynamic circuit networks, and orchestration in SDN and cloud-native.

JOSÉ F. DE REZENDE (Member, IEEE) received the Ph.D. degree in computer science from Université Pierre et Marie Curie, in 1997. He was an Associate Researcher with Université Pierre et Marie Curie, in 1997. Since 1998, he has been an Associate Professor with the Federal University of Rio de Janeiro. His research interests include distributed multimedia applications, QoS in the internet, mobile networks, wireless communication, and experimental platforms.

LEOBINO N. SAMPAIO (Member, IEEE) received the Ph.D. degree in computer science from the Federal University of Pernambuco (UFPE). He was a Visiting Researcher with the Computer Science Department, University of California at Los Angeles (UCLA), USA. He is currently an Associate Professor with the Computing Department (DCC), Federal University of Bahia (UFBA). His current research interests include future internet architectures and network performance evaluation.

KLEBER V. CARDOSO received the degree in computer science from Universidade Federal de Goiás, in 1997, and the M.Sc. and Ph.D. degrees in electrical engineering from COPPE, Universidade Federal do Rio de Janeiro, in 2002 and 2009, respectively. He is currently an Associate Professor with the Institute of Informatics, Universidade Federal de Goiás (UFG), where he has been a Professor and a Researcher, since 2009. In 2015, he spent his sabbatical with Virginia Tech, USA. In 2020, he was with the Inria Saclay Research Center, France. His research interests include wireless networks, SDN, virtualization, resource allocation, and performance evaluation.

DANIEL F. MACEDO received the B.Sc. and M.Sc. degrees in computer science from the Federal University of Minas Gerais (UFMG), Brazil, in 2006, and the Ph.D. degree in computer science from Université Pierre et Marie Curie-ParisVI, in 2009. He is currently an Associate Professor with the Computing Department (DCC), UFMG. He has productivity in research scholarship (Bolsa PQ—CNPq) level 2. He was a Postdoctoral Researcher with UFMG. His research interests include wireless networks, network management, and autonomic networks.

FLÁVIO DE OLIVEIRA SILVA (Member, IEEE) received the Ph.D. degree from the University of São Paulo, in 2013. He is currently a Professor with the Faculty of Computing, Federal University of Uberlândia (UFU). He has had several papers published and presented at conferences worldwide. His research interests include future networks, the IoT, network softwarization (SDN and NFV), future intelligent applications and systems, cloud computing, and software-based innovation. He is a member of ACM and SBC. He is a reviewer of several journals and a member of TCPs at several IEEE conferences.

● ● ●