Creating a Sustainable Federation of Cloud-Based Infrastructures for the Future Internet

The FIWARE Approach

Yahya Al-Hazmi
Technische Universität Berlin, Germany
yahya.al-hazmi@tu-berlin.de

Alexander Willner
Technische Universität Berlin, Germany
alexander.willner@tu-berlin.de

Brian Pickering
IT Innovation Centre, Southampton, UK
jbp@it-innovation.soton.ac.uk

Alaa Alloush
Technische Universität Berlin, Germany
alaa.alloush@tu-berlin.de

Thomas Magedanz
Fraunhofer FOKUS, Berlin, Germany
thomas.magedanz@fokus.fraunhofer.de

Silvio Cretti
CREATE-NET, Trento, Italy
silvio.cretti@create-net.org

ABSTRACT

The remarkable success of cloud computing has change the way services and applications are implemented and offered not least because of the flexibility and scalability that such an environment can offer. Cloud federation has tremendous potential for the industry as an effective way to increase the capacity of resources and diversity of offerings while keeping costs relatively low. Yet cloud federation is still in its infancy, with different approaches being introduced, either in terms of architectural design or the availability of test facilities. This paper introduces the FIWARE approach for federating multiple cloud-based infrastructures targeting different fields related to Future Internet and Smart-Cities innovative developments. Sustainability is considered in the focus of our approach. In addition to the traditional cloud services, the FIWARE federation mainly offers a set of general-purpose platform functions and services that are available through open (public and royalty-free), vendor-independent APIs supporting open innovation and extended with further facilities (e.g. sensing and Software-Defined-Networking (SDN) capabilities) advancing the market with smart infrastructures. We present federated infrastructure sustainability considerations along with the FIWARE federation architecture design that is implemented and deployed within a federation of 17 cloud-based infrastructures distributed across Europe.

Categories and Subject Descriptors

C.2.1 [**Computer Systems Organization**]: COMPUTER-COMMUNICATION NETWORKS—*Network Architecture and Design*; C.2.4 [**Computer Systems Organization**]: COMPUTER-COMMUNICATION NETWORKS—*Distributed Systems*; D.2.12 [**Software**]: SOFTWARE ENGINEERING—*Interoperability*

General Terms

Design, Management, Economics

Keywords

Sustainable Marketplace, Cloud Federation, Future Internet, Application Development

1. INTRODUCTION

The wide adoption of the Cloud Computing paradigm has changed the way services and applications are implemented and offered. Computing resources are available according to a subscription utility service model. It provides virtualized resources in a pay-as-you-go fashion over the Internet and from a business perspective, it is widely viewed as an economical model for renting technical resources[1].

For the industry the interconnection of multiple cloud sites embodies a number of business opportunities. The increased variety and capacity of available service offerings preclude the usage of multiple clouds in order to achieve better Quality of Service (QoS), reliability and flexibility. Further, depending on single Compute Cloud service makes it hard to implement adequate responsiveness and usability to clients distributed worldwide.

However, the federation and interoperation of Compute Clouds are still under active research. While a number of Standards Developing Organizations (SDOs) are working on standards such as Open Cloud Computing Interface[2] (OCCI), Cloud Infrastructure Management Interface[3] (CIMI), Cloud Data Management Interface[4] (CDMI) or Topology and Orchestration Specification for Cloud Applications[5] (TOSCA) that complement and compete with each other, they do not cover the interconnection of administrative independent infrastructures. Therefore, over 20 proposals[6] have been proposed to approach the Intercloud concept.

TRIDENTCOM 2015, June 24-25, Vancouver, Canada

DOI 10.4108/icst.tridentcom.2015.259747

In this paper, we introduce the approach developed within the Future Internet Public Private Partnership[7][1] (FI-PPP) Future Internet Core Platform[8][2] (FIWARE) program for federating multiple cloud-based infrastructures. This approach focuses on building a sustainable pan-European federation of cloud-based test infrastructures for open innovation developments offering a large number of general-purpose, vendor-independent platform functions and services, called Generic Enablers (GEs), in different fields within the context of Future Internet (FI) and Smart Cities Innovation.

The main contribution of this paper is on the evaluation of available and selected federation models as well as the introduction of the methodology followed in FIWARE federation aiming at longer-term sustainability of the federation. Besides analysing the benefits for different stakeholders, which they see as significant for their own business plans, we have considered most pertinent and relevant features from some research projects focused on assessments of the potential social and economic impact and sustainability impact. Furthermore, this paper presents the description of the FIWARE federation architecture. This federation has been validated by a deployment of 17 infrastructures distributed across Europe through the FIWARE Lab[3]. An infrastructure in FIWARE Lab terminology is referred to with a node, however, in this paper we will use the term infrastructure.

The rest of the paper is structured as follows. Sec. 2 gives an overview on the related work. In Sec. 3 different federation models are being analyzed and based on this, the FIWARE approach for creating its sustainable federated infrastructure is presented in Sec. 4. Following this approach the federation architecture is introduced along with several architectural principles in Sec. 5. Further, we shed light on the benefits and offerings of FIWARE Lab federation in Sec. 6. Finally, the paper is concluded together with an outlook in Sec. 7.

2. RELATED WORK

The Cloud Computing paradigm [9] has been attracting the interest of the Information Technology (IT) industry since at least 2007 and has been viewed as an important economical model for renting technical resources [1, 10].

As a result, a number of specifications have been established within several SDOs. For example one of the first standards was the OCCI that was defined within the Open Grid Forum (OGF). Similar to the OCCI, the Distributed Management Task Force (DMTF) worked on the CIMI in conjunction with Open Virtualization Format (OVF) packaging format. To manage data in the cloud the Storage Networking Industry Association (SNIA) defined the CDMI. Further, the Organization for the Advancement of Structured Information Standards (OASIS) has defined the Cloud Application Management for Platforms (CAMP) specification in addition to the TOSCA that allows the definition of complex platform independent service topologies and their orchestration.

However, these standards do not cover the federation and interoperation of administrative independent cloud sites[11]. As a result, the term Intercloud[6] was coined in 2007 and well over 20 designs for interoperability architectures have been proposed[12] and a taxonomy and survey of already existing architectures was published in 2012[6] and 2014[13].

As highlighted in [14] simultaneous with the first academic publications also several SDOs have been formed to define Intercloud[6] Computing architectures. Among others, this includes the European Grid Infrastructure (EGI) Federated Cloud Task Force in Europe to deploy a testbed to evaluate the integration of several approaches; the Global Inter-Cloud Technology Forum (GICTF) in Japan to define Intercloud architecture requirements[15]; the National Institute of Standards and Technology (NIST) in the US formed a Federated Community Cloud working group; the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Focus Group on Cloud Computing has published a reference architecture[16]; the IEEE has formed the working group Standard for Intercloud Interoperability and Federation[17] (P2302); and the Internet Engineering Task Force (IETF) is working on their Cloud Reference Framework[18].

One overarching goal in the context of federated e-infrastructures is the establishment of a self-sustainable operation. According models and strategies have been been analyzed since many years for example in the Future Internet Research and Experimentation[19][4] (FIRE) context. Starting 2007 within the Pan-European Laboratory[20] (Panlab) project several relevant deliverables[21, 22] have been produced and a FIRE Office[23] was planned to be established. About 7 years later, still within the Federation for FIRE[24] (Fed4FIRE) project a paper on the sustainability of federated FI facilities has been published[25] that itself is mainly based on the work conducted in the Federated IT Service Management[26] (FedSM) project. In parallel the Coordination and Support Action (CSA) Coordination and Integration of FIRE Activities in Europe[5] (CI-FIRE) is analyzing the current state of self-sustainability approaches to build a generic framework for testbeds. Further, within the European Institute of Innovation and Technology Information and Communication Technology Labs[27] (EIT ICT Labs) context the Fanning out Testbeds-as-a-Service for the EIT ICT[28] (FanTaaStic) project is focusing on commercial offerings for Small and Medium Enterprises (SMEs) based on FIRE infrastructures.

3. FEDERATION MODELS

Many cloud federations exist that differ in their approaches, models and the used tools and interfaces. Operation is an important and critical aspect of any federation. Different kinds of federation models exist and are differently operated. For FIWARE federation, the taken approach and models have to fulfill its requirements and objectives.

FIWARE federation aims at federating cloud-based infrastructures offering resources to the developers of FI applications, services and trials. These infrastructures typically

[1] http://fi-ppp.eu
[2] http://fi-ware.org
[3] https://lab.fiware.org
[4] http://ict-fire.eu
[5] http://ci-fire.eu

offer traditional cloud resources as well as deploy instances of FIWARE Generic Enablers (reusable, generic services important for application development in several fields, like: data analytics, context-based message brokering, Internet of Things (IoT) gateways, and many more). In addition, infrastructures may also provide further advanced facilities (e.g. sensors generating Smart-Cities orientated data, Wi-Fi, SDN-enabled facilities, etc.).

To identify the most suitable approach that fits FIWARE federation need, we have explored the federation framework defined by the FedSM project. This framework was chosen for two reasons: *Simplicity* as it promotes a viewpoint of clearly and simply identifying federation operation beyond technical descriptions; *Relevance* as it is developed alongside Grid infrastructure federations that are in many aspects similar to cloud federations like the FIWARE one.

According to FedSM, the three main actors in a federation are the **user** (any one requiring offered services or resources), **federation member** (infrastructure provider), and **federator** (the individual or component controlling and/or managing the result of federating individual members). These actors can interact in one of three different ways in order to utilize a service:

- **Certification.** The user interacts directly with the federation member.
- **Loose.** Part of the service interaction involves the user interacting with federation services before interacting directly with the federation member.
- **Integrated.** All interaction is between the user and the federator.

According to these three ways of interactions, five federation models are to be discussed.

- **Invisible Coordinator.** The federation acts as certification or validation authority. The federator defines membership rules, and checks compliance of members that work to comply with the rules and seeks certification from the federator. Users find infrastructures via other channels (e.g. search engines, marketplaces, etc.) and request services.
- **Advisor.** The federator advises federation members on how to promote their capabilities through federation. Users describe their required services to the federator that advises them on where to find the needed capabilities in forms of recommendations. Users then decide which federation members to engage with.
- **Matchmaker.** The federator advises federation members on how to promote their capabilities (offerings along with terms and conditions) through federation. Users describe their required services to the federator that matches requests from users to capabilities / offerings from infrastructures, and thus performs resource allocation (reservations) on behalf of the users.
- **One-Stop-Shop.** The federation provides a channel for the federation members to advertise services and resources. Users describe their required services to the federator that performs resource allocation (reservations) on behalf of the users, monitors the usage (based on monitoring data received from the respective infrastructures), and provides billing. Users pay the federator who is the initial point of contact. However, federation members still able to bill one another.
- **Integrator.** The federation is responsible for all interactions with users. They interact with the federation searching for offerings, describe required resources. The federator reserves, and then invokes them at the proper time. Billing and payment are done by the federator.

The invisible coordinator and advisor models relate directly to the one-stop-shop and matchmaker models. An advisor or matchmaker model implies a looser integration of resources and partners whereby the federator provides support to enable resource identification by potential users and resource exploitation at the resource provider site. Such a matchmaker role corresponds to the looser integration model in the third part of Fig. 1. An invisible coordinator or one-stop-shop by contrast increases the control and support offered by the federator in running and managing resource utilization. This one-stop-shop role reflects the tighter integration model in Fig. 1. Offering both loose and tight integration models is an important benefit of FIWARE offerings.

Making a decision on the most suitable model among these models is not a trivial task. FIWARE choice is made taking into account the sustainability strategies as well as requirements of diverse types of stakeholders, in particular i) use-case projects (that represent the developers of future applications and services) in different domains (e-health, gaming, environmental, etc.), ii) different infrastructures participating in FIWARE federation, and iii) FIWARE enablers [29].

The most appropriate federation model adopted in FIWARE is a **hybrid federation model** covering aspects of the **one-stop-shop** model (a common advertising channel for infrastructures where users choose which services/resources they want to use) and the **integrator** model (the federator decides which services/resources will be used). Whether the user or the federation decides which resources will be allocated depends on the type of services/resources. Example, conventional data resources are allocated by FIWARE Lab (the federation) and accessed in a unified way under common terms by users (the **integrator** model can be applied), but non-conventional resources (e.g. sensor networks) are advertised by the federator and negotiated with the federation members and accessed directly.

The federation models discussed so far concern the ways different parties in a federation collaborate and technically interact with each other. However, business models are also of major interest. As long as cloud paradigm closely matches FIWARE federation, the typical business models proposed for cloud services are concerned. In this perspective, among those eight types of cloud business models classified in [30], FIWARE approach adopts the *One-stop Resources and Services* model, which is suitable for multiple stakeholders who can bring mutual benefits through collaboration. However, each stakeholder can check the proper business model according to the characters of its business. For instance, in accordance with its business size, a federation member may choose a *Service Provider and Service Orientation* model (public cloud) or *Support and Service Contracts* model (provide solutions for private domains such as SMEs), or even join an *All-In-One Enterprise Cloud* model as a part of a broader and flexible ecosystem. Technology and service providers and developers can join any of these models as a part of FIWARE ecosystem that is also open to support further models.

The selected models will have implications for the technical architecture but also business planning. In short, the technical architecture will need to provide integration points at different levels and be flexible enough either to provide functional capabilities or to be able to interface with one or more of those capabilities at infrastructure level (see Sec. 5.2). In respect of business planning, this is dealt with in the following section on sustainability.

4. FEDERATED INFRASTRUCTURE SUSTAINABILITY

Defining sustainability is not necessarily straight forward. Whereas most refer to the Triple Bottom Line (TBL) [31], i.e. social, economic and environmental factors, there are still others who would prefer a return to the original environmental protection emphasis, whilst acknowledging the significance of technical and cultural legacies [32]. Whatever the specific definition or focus wished to be applied, it is however more than clear that evaluating and tracking sustainability are essential parts of the business and technical planning processes [31].

For FIWARE federation, providing cloud computing facilities to FI application and service developers, there is already benefit in terms of TBL: the federation offers support to the wider community, optimizing and sharing resource efficiently, and via virtualization remains portable across physical environments [33]. In addition, though, as we describe in this section, technical as well as commercial planning has been done via direct engagement with the appropriate stakeholders [31]. By way of introduction, Fig. 1 summarizes how we've gone about it: starting with the identification of those stakeholders most relevant to the provision of FI federated resources, as well as engaging directly with them, we sought to identify their highest priority concerns and challenges and to build a structured and flexible offering which would encourage those stakeholders to invest in its long term future, even when public funding had gone.

Developing and supporting the broader community is recognized as an integral part of any sustainability plans [31, 32, 33, 34]. For FIWARE federation, this began early on with an analysis of those directly and indirectly relevant to the FI ecosystem, including direct contributors, potential users and groups such as potential sponsors (see 1 in Fig. 1): these included the developers of FI services and applications, the owners of the federated infrastructures as well as the federator; externally, end users, developers, sponsors and intermediaries. The first step was to identify all the potential challenges, and begin to develop a federated offering around it, supporting multiple federation models. Recognizing the challenges and implementing features to accommodate them is not enough, though. We had to prioritize them in discussion with the internal and external stakeholders (see 2 in Fig. 1) [31, 34].

Stakeholders identified and ranked the challenges and concerned in different functional and non-functional areas as referred in table 1:

Federation	Market development	Ensuring future (economic) growth
	Changing requirements	Keeping up with shifting market needs
	Personnel and Administration	Managing the federation
	Updates	Ensuring ongoing technical capabilities
	Legal constraints	Respecting regulatory context
	Customer support	Engagement with users
	Maintenance	Ensuring continuity of service
Partnership	Trust	Developing and maintaining relationships
	Maintaining market share	Protecting financial security
	Privacy	Protecting all assets
Member	Capacity	Providing basic capabilities
	Infrastructure	
	New technology	
Joint	Licensing	Ensuring compliance
	Other	Miscellaneous

Table 1: Concern of challenges in functional and non-functional areas

Stakeholder priorities map well onto the various dimensions of sustainability outlined in the literature. But more importantly for the federation is the fact that identifying where the responsibility lies (with the *federation* itself, in *partnership* between the federator and federation members, or with the *members* themselves) is significant information to be fed back into the design and packaging of the overall federation offering.

As Fig. 1 part 3 shows, the federation has developed a number of different variants. In terms of federation itself (see by comparison models in Sec. 3), infrastructures wishing to join the federation can choose just how much of the responsibility for meeting the challenges identified is assumed by the federator: if the burden remains with the infrastructure provider, then a loose federation model such as *matchmaker* is appropriate: the federator simply acts as a recommender service for resource consumers. By contrast, and equally possible, a tighter integration may be more suitable with the federator assuming more control over things like maintenance, meeting changing requirements and provisioning service updates; in that case a *one-stop-shop* model is more appropriate. Underlying both though is a functional and institutional flexibility which facilitates adaptation in the creation of value to all interested parties [31, 33, 34].

With more of a broader community focus though ([31, 34]), it can also support others running similar services by providing know-how and experience in the deployment of the technologies as well as to allow for *ad hoc* connection of specialized resource as a one-off or in response to particular needs. This level of flexibility in service offering bodes well for the future, along with the willingness to share functional and non-functional responsibilities between federator and federation members. In direct consequence, what began as an equal public-private investment, 60% of current members (Fig. 1 part 4), including software developers, infrastructure providers and general support personnel will continue with the federation: for the others it is simply a matter of funding.

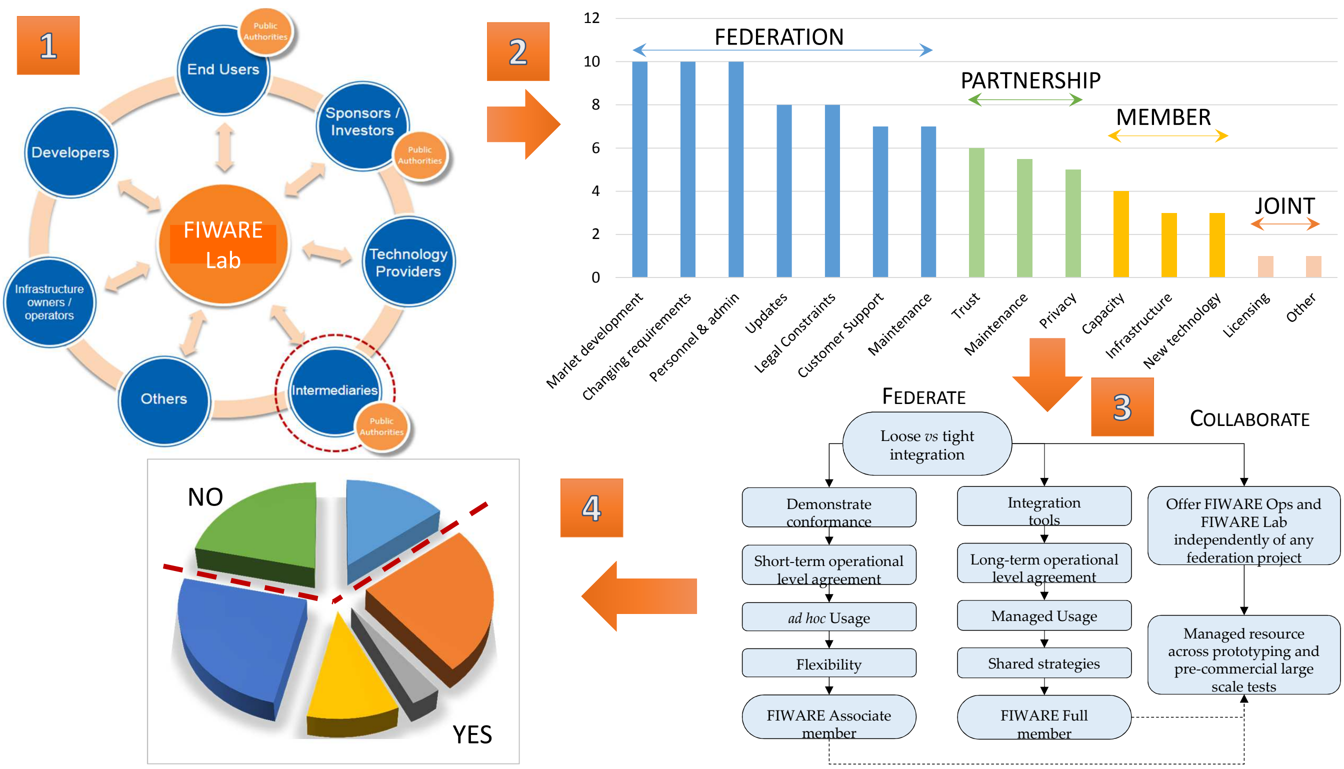

Figure 1: Planning for federation sustainability (starting with the identification of the most relevant stakeholders (1) and FI socio-economic challenges (2), then developing different federation variants (3), and infrastructure and non-infrastructure continuation beyond the public funding (4))

For the federation of infrastructures discussed in this paper, the business treatment, and not least with a view to long-term sustainability, has been focused on the identification and engagement with key stakeholders to prioritize their challenges and shape federation service offerings that would encourage the building of an on-going community and its support. In moving forward, the priority is really about keeping the value identified going [31, 33, 34] and encouraging the broader community to take over responsibility: for FIWARE, it's now about the assets of the present providing well-being for future generations [32].

5. FEDERATION ARCHITECTURE

Taking into account the sustainability considerations discussed in Sec. 4, this section presents several architectural principles to build a sustainable federated infrastructure. In addition, it introduces the federation architecture adopted in FIWARE federation.

5.1 Design Principles

The architecture is designed following a set of principles. It adheres the significant five cloud computing characteristics defined in [9]:

- **On-demand self-service.** The architecture allows automatic resource provisioning without requiring human interaction. This is achieved in FIWARE Lab through a couple of GEs that facilitate automatic deployments, presented in [35].
- **Broad network access.** Services are accessible over the network through standard mechanisms using any device (smart phones, laptops, tablets, etc.). Users can request services and resources through FIWARE Lab Portal that is accessible from any device. Services are also accessible via TCP/IP and HTTP compatible standards, in particular via RESTful Application Programming Interfaces (APIs).
- **Resource pooling.** Offering a large number of heterogeneous virtual and physical resources. Allowing also specifying location at a higher level of abstraction (e.g. country, city, or data center). FIWARE Lab serves multiple developers at the same time in forms of isolated tenants. The physical resources are shared across virtual ones (i.e. assigned to the active ones).
- **Rapid elasticity.** Supporting auto-scaling up or down of resources for a given application. Scalability and elasticity are supported in both automatic and manual manner using a special GE called FIWARE Cloud Hosting as well the monitoring system [36].
- **Measured service.** Automatically control and optimize resource usage, supported with suitable monitoring and reporting capabilities [36].

Furthermore, the design also adheres the heterogeneous cloud deployment best practices presented in [37]. Among those principles the major ones are:

- **User-centricity.** It is at the heart of the design. Well-designed services and user interfaces are keys to deliver best user experience. FIWARE Lab enables through its interfaces a uniform access to the offered services.

- **Simplicity.** Federation of heterogeneous environments may require complex solutions to automate some processes. However, this could impact delivery time and service quality. Therefore, some processes might need to be managed manually in an initial phase to reduce time-to-market, rather than designing with full functionality. FIWARE Lab hides the heterogeneity from users allowing automatic deployments of services/resources (through the (Platform-as-a-Service) PaaS Manager [35]) and unified access to different services.

- **Reusability.** Avoid developing new solutions from scratch but rather reuse as much as possible among a plethora of cloud-related solutions that are available off the shelves and capable of support the creation of cloud based infrastructures. The used and offered services in FIWARE Lab are based on FIWARE GEs whose concept addresses by definition the reusability.

- **Service dependability.** Service availability is one of the key attributes for a service to be defined dependable. It should be careful planned taking into account associated costs [38]. The architecture aims at delivery dependable services, focusing more on availability (each infrastructure should ensure service availability regardless the availability of other infrastructures), reliability, safety and transparency attributes. FIWARE Lab architecture avoids any single point of failure so that its main services (like identity manager, portal, security proxy, etc.) are provided in high availability.

- **Flexibility.** The architecture has to be flexible to the dynamic changes in terms of new requirements (from FI application developers) as well as the integration of new infrastructures (joining the federation). In this sense modularity and service orientation are fundamental principles. FIWARE Lab architecture is modular and its components expose interfaces used for external access and for communications among each other.

- **Compatibility.** Suitable APIs should be vendor independent and as much as possible compatible with available reference and defacto standards. FIWARE Lab architecture includes adaptation layers for allowing legacy systems to become part of the federation [36].

FIWARE Lab federation management architecture is designed for a robust and sustainable deployment. It is designed in a way to avoid possible technical complications on the deployment of the federation management components as well as to ensure fulfilling both functional and non-functional requirements. For instance, on the one hand, having all the FIWARE Lab federation services and repositories (e.g. monitoring, security, cloud portal) distributed on all the participating infrastructures can complicate a lot the management of the federation (think in particular to the synchronization problems among the different infrastructures). On the other hand, having all the federation management components on just one infrastructure does not assure high availability.

Again, as aforementioned, an infrastructure in FIWARE Lab architecture is referred to with a node, but in this paper we use the term infrastructure instead.

The architecture distinguishes therefore between two types of infrastructures participating in FIWARE Lab federation: *master* and *slave*. The *master* infrastructure is the one where, in addition to the features deployed on the slave infrastructure, the centralized parts of the federation services (i.e. the components needed to manage the federation) are deployed whilst the *slave* infrastructure is the one where only the software needed for deploying and managing user resources and services is installed.

5.2 The Architecture

FIWARE Lab federation architecture is illustrated in Fig. 2, where the lower part contains the architecture and the components deployed on each infrastructure (both master and slave), and the upper part contains the architecture and components deployed only on the master infrastructures. Before discussing the individual architecture components, it is to be noticed that most of these components are based on FIWARE GE implementations that are all available online through the FIWARE Catalogue[6]. That means that FIWARE Lab federation is mainly built using some FIWARE GEs, however instances of these GEs and more other GEs are offered through FIWARE Lab for users (FI application developers).

Each FIWARE Lab infrastructure (both master and slave) includes three main functional groups, where each comprises a set of components which are in charge of enabling:

- **Cloud computing**: the setup of a cloud computing environment based on OpenStack[7] using the Infrastructure-as-a-Service (IaaS) Data Center Resource Management (DCRM) GE that wraps OpenStack and, together with the OpenStack Neutron (Quantum), local SDN Controller (connected to the one at the master infrastructure), Open vSwitch[8] and OpenFlow Switches[9] components, provide all the services required for the IaaS management system. In addition, each virtual machine (VM) is equipped with the Software Deployment and Configuration (SDC) Manager GE client, connected to the SDC Manager GE that exists only in the master infrastructure, in order to deploy different products and GE implementations deployed by the users.

- **Monitoring functionalities**: collecting data from physical devices, network devices, VMs and services used by several federation components such as Service Level Agreement (SLA) Manager, info graphics and status pages, FI application developers, etc. Monitoring data is collected from different sources and provided through adapters in a common, context format using the Open Mobile Alliance's Next Generation Service Interface (NGSI) Adapter [38] which is part of the Monitoring GE.

[6] http://catalogue.fi-ware.org/
[7] http://openstack.org
[8] http://openvswitch.org/
[9] http://archive.openflow.org/wp/documents/

- **Security functionalities**: the Identity Management GE together with the Security Proxy (the OpenStack Keystone Proxy[10]), and Access Control GE provide both authentication and authorization services for each infrastructure.

In addition to these components, a master infrastructure contains the following functional groups as well:

- **User oriented services and tools**: provides a view on all the facilities offered by FIWARE Lab. A set of services and tools are available:
  - The Federation Manager governs the registration of a new infrastructure to the federation.
  - The Resource Catalogue and Recommendation Tool is oriented to find the right services offered by the federation.
  - The Interoperability Tools verify the interoperability and compatibility of developed software with FIWARE GEs based on some rules.
  - The SLA Manager handles the SLA negotiation.
  - The Portal (Marketplace) provides a single entry point and graphical user interfaces (GUIs) for all these tools offering a sort of marketplace for all the services provided by the federation.
- **Services and tools supporting the setup, deployment and operation of the federation:** provides the functionalities to deploy the software required to install the cloud hosting management of a FIWARE Lab infrastructure and its operation. These include the following components:
  - The Infrastructure Toolbox aims at providing an automated installation of the IaaS Management System (OpenStack, DCRM and the Local SDN Controller), the components enabling monitoring functionalities and the component enabling security functionalities.
  - The Deployment and Configuration Adapter (DCA), the PaaS Manager GE, the SDC Manager GE and the Network Controller provide functionalities for the deployment of FIWARE technologies (GEs) and the offered third parties products on the different infrastructures and for setup the network connectivity among different VMs. Readers can refer to [35] for more details.
  - The Scalability Manager GE implements elasticity and scalability rules. It includes a set of rules that are defined by each PaaS (a tenant in OpenStack) administrator and allows taking decisions based on monitoring information provided by the monitoring system.
  - The Context Broker (CB) and Big Data GEs support the monitoring functionalities at the federation layer. NGSI adapters notify monitoring data to the Publish/Subscribe based CB that stores the data in a Hadoop[11] based Big Data platform for a scalable and distributed storage. The Big Data GE exposes a RESTfull interface that is used by its users. Monitoring data is also displayed to users through the Monitoring GUI that is integrated into the Portal.
  - The Help Desk represents a problem tracking system. It implements a workflow defined for processing user requests and providing user support.
- **Federation security tools**: The security solution comprises the Security Monitoring GE that gathers security monitoring data from remote probes and possible local proprietary IdM systems, and the Security Dashboard that is integrated into the Portal and provides a GUI to display security information and alerts users in the case of security problems.

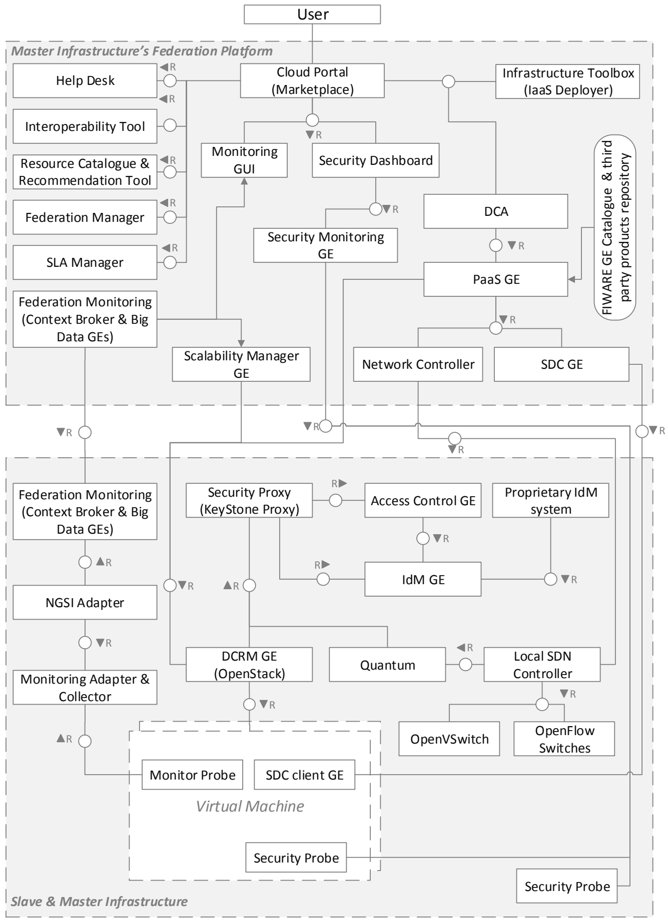

Figure 2: FIWARE Lab Federation Architecture

An infrastructure in FIWARE Lab federation is any infrastructure that mandatory offers i) capacity to host FIWARE GEs for building FI applications, and ii) connectivity to Internet and to the network interconnecting all infrastructures participating in FIWARE Lab federation, and optionally offers iii) additional capacities such as sensing environment,

[10] http://wiki.openstack.org/wiki/Keystone/Federation/Blueprint

[11] http://hadoop.apache.org

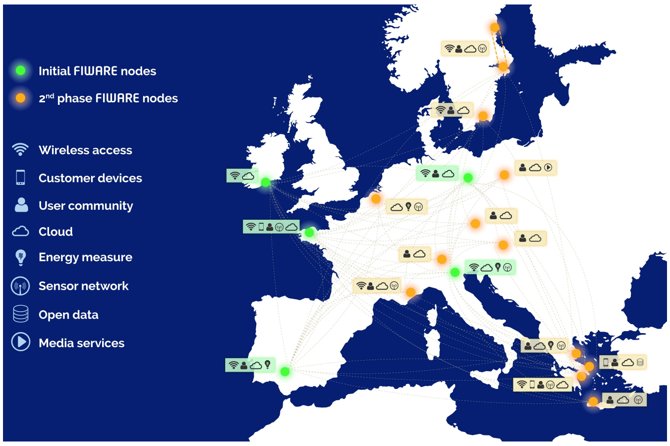

Figure 3: Overview on the current FIWARE Lab federated infrastructures

advanced wireless connectivity, and smart city data sets, iv) services to developers like support, backup, etc., and v) access to end-user communities. The current implementation of FIWARE Lab federation includes seventeenth infrastructures distributed across Europe (as shown in Fig. 3) and interconnected based on a layer-3 Multi-Domain Virtual Private Network provided by GÉANT[12]. These infrastructures have different capacities and all together offer over 3,000 computing cores with 16TB of RAM and 750TB of storage capacity.

6. FIWARE OFFERING AND BENEFITS

This section gives an overview on the multi-fold benefits and offering provided by FIWARE Lab federation for its stakeholders. Its flexible architecture and the wide range of diverse technologies provided by the participating infrastructures, makes FIWARE Lab the most suitable environment for Open Innovation[39] where various communities can meet and influence each other. In the paper, we focus only on three main stakeholders among those discussed in Sec. 4.

6.1 Infrastructure providers

One of the attractive features of FIWARE Lab architecture is that it allows infrastructures to easily join and leave the federation as well as fast and simply deploy the entire management software in short time and automated way.

Having sustainability in the focus of our approach, the software required to operate any infrastructure willing to participate in FIWARE Lab federation is offered through FIWARE Ops. FIWARE Ops is a collection of tools (the federation architecture components presented in Sec. 5.2) that ease the deployment, setup and the operation of FIWARE Lab infrastructure. FIWARE Ops tools support four management operations:

- **Deployment**: The Infrastructure Toolbox facilitates the deployment of a new infrastructure by deployment of basic cloud hosting GEs, monitoring adapters and configuring the federation APIs and end points.

[12]http://www.geant.net

- **Federation management**: The Federation Manager allows new infrastructures to register in FIWARE Lab and to test the successful registration. The deployed resources in each infrastructure are available through the Cloud Portal and the capacity of each infrastructure is displayed in the info graphics.

- **Connectivity management**: The Network Controller supports the connectivity of different services composing an application using SDN techniques. It enables the connection of virtual private networks across different infrastructures and the management of their topologies, without the need to expose public ports over the Internet.

- **Service offer management**: Due to the diverse offering of the federated infrastructures, FIWARE Ops offers tools to facilitate the deployment of GEs such as the DCA. In combination with the PaaS Manager GE, it allows federators to deploy in a batch way GEs, simplifying the setup of an infrastructure and their registration in the GE Catalogue. Registered services can also be tested for interoperability and compliancy within respect their APIs and expected behavior using the Interoperability Tool. Through the Security Dashboard also allows for checking security leaks in FIWARE Lab infrastructures.

Through joining the FIWARE Lab federation, infrastructure owners gain numerous benefits such as:

- Being part of the wide user base of the European FI ecosystem.

- Have access to the specific solutions and technologies developed by FIWARE and offered via its catalogue, to a much richer and more diverse set of resources, and to technologies and capabilities not available locally.

- Gain valuable experience and know-how via collaboration and interaction with diverse and large communities.

- Gain economic benefits starting with being able to collaborate and build out new business and business relationships outside of the home market (i.e. across Europe), continuing with effectively gaining new customers, strengthening infrastructure owners' position and value offering to their existing customers.

6.2 Technology and service providers

FIWARE Lab is enriched by diverse enabling technologies in different fields. Although the traditional cloud resources (e.g. VMs) are still offered to the users, but the strength and the unique offer of FIWARE Lab is the innovative general-purpose platform functions and services (GEs) in different fields within the context of FI and Networking as well as Smart Cities. FIWARE Catalogue includes over 80 GE implementations that can be applied in the fields of IoT, Healthcare, Transports, Energy & Environments, Media & Content, Manufacturing & Logistics, and Social & Learning. These GEs are offered by different technology providers in form of open and vendor-independent APIs extended with advanced FI facilities like sensor-enabled environments, SDN-enabled infrastructures, seamless access anywhere, anytime and from any device (Wi-Fi, 2G, 3G, 4G, etc.), and more.

Technology providers can build their technologies in any field and provide them in forms of GEs through FIWARE Catalogue. These can be used by different application developers who can provide significant feedbacks to the technology providers. They can accordingly enhance their solutions.

6.3 Application developers

The combination of a rich set of GEs and a federation of infrastructures offering access to a range of emerging technologies and a large pool of physical resources with a Europe-wide geographic coverage. Application developers can take advantage of these offerings to build distributed applications with high-availability set-up and QoS control across the different used infrastructures. They can build and deploy their applications in any form of the three traditional cloud services models, namely Software-as-a-Service (SaaS), PaaS, or IaaS to develop new applications.

FIWARE federation ecosystem provides the basis for more efficient and faster innovations through providing testing environment suitable for SMEs, guarantee large scale validation of new technologies, enabling competitive testing via offering various locations and networks, providing solutions to localize data storage and suitable place for the implementation of new services, protocols and solutions. Indeed, adopting FIWARE approach leads to reduce the time-to-market for new services and technologies, minimize related risks, provide experimentation facilities as needed for conducting testing in complex, controllable, real-world and large-scale environment.

6.4 Summary

The presented offers can be used through a set of showcase demonstrations divided into three groups. First group directly supports the value proposition in demonstrating the benefits of being part of the federation as well as how to interact with the broader ecosystem. Second, supports some of the target markets in relevance to mobility, smart cities, and so forth. The last group gives SMEs a clear indication of what needs to be done to reap the benefits of FIWARE offerings. Indeed, these showcases are shaped from a business perspective as well as purely technical demonstration, so that they provide glimpses of long-term perspectives. Each showcase has been documented to capture the experience gained. But in addition, they are demonstrated in a series of related YouTube videocasts.

7. CONCLUSION AND FUTURE WORK

This paper has introduced the FIWARE cloud federation approach that takes into account sustainability considerations in the focus of the architecture design and offering models.

Diverse federation models have been analyzed and the most suitable ones fit to the context of the FIWARE needs and offerings are adopted in building its sustainable federated cloud-based infrastructure. We have presented the sustainability procedure followed by the FIWARE approach along with the federation management architecture that are implemented and deployed in a federation of 17 infrastructures distributed across Europe through FIWARE Lab.

This paper presented several sustainability guidelines and considerations followed in FIWARE federation. This includes many FI social and economic aspects as well as architectural principles to build a community-based, trustworthy ecosystem allowing stakeholders from various relevant communities to meet, interact and share experience. Furthermore, services and resources are used in a secure, transparent and interoperable manner, supported with user-friendly tools as well as self-assessment capabilities (e.g. self-monitoring). In addition to these considerations, versatile benefits and offerings have been discussed that attract various stakeholders to be part of (or to continue in) the federation.

The potential for sustainability is significantly enhanced through the technical capabilities of FIWARE, but also the ecosystem which has grown up around it. In consequence, the federated infrastructure resource does not exist in a vacuum: from a technology perspective, it provides a set of utilities for service and application development, as well as tools for deployment; beyond that, the ecosystem provides access to potential users and sponsors with interest in the success of FI applications and services. In addition, it forms part of a strategic investment and development initiative at EU level. Other offerings tend to be more focused on individual areas, such as scientific research, and lack the ecosystem to provide experience and support development.

FIWARE Lab federation aims at advancing the global competitiveness of the European economy offering currently 80 million euros of direct funding, mentoring and networking to over 1,000 startups and small enterprises. It also aims at extending its federation with similar large-scale infrastructures.

Acknowledgments

The research work has received funding from the European Union's FP7 grant agreement no. 604590 XIFI Project. The authors would like to thank the project partners for their contribution, especially Daniel Nehls, Federico M. Facca, Eunsook E. Kim and Maurizio Cecchi.

References

[1] G. Lewis. "Basics about cloud computing". In: *Software Engineering Institute Carniege Mellon University, Pittsburgh* (2010).

[2] T. Metsch and A. Edmonds. "Open Cloud Computing Interface–Infrastructure". In: *Standards Track, no. GFD-R in The Open Grid Forum Document Series, Open Cloud Computing Interface (OCCI) Working Group, Muncie (IN).* Open Grid Forum (OGF). 2010.

[3] DMTF. *Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol.* Sept. 2012.

[4] Storage Networking Industry Association (SNIA). *Cloud Data Management Interface (CDMI) Std. 1.0.* Tech. rep. Storage Networking Industry Association (SNIA), 2010.

[5] D. Palma and T. Spatzier. *Topology and Orchestration Specification for Cloud Applications (TOSCA) Version 1.* Nov. 2013.

[6] N. Grozev and R. Buyya. "Inter-Cloud Architectures and Application Brokering: Taxonomy and Survey". In: *Software: Practice and Experience* 44.3 (2012), pp. 369–390.

[7] D. Havlik et al. "From Sensor to Observation Web with environmental enablers in the Future Internet". In: *Sensors* 11.4 (Jan. 2011), pp. 3874–907.

[8] A. Glikson. "FI-WARE: Core Platform for Future Internet Applications". In: *4th Annual International Conference on Systems and Storage*. Haifa, 2011.

[9] P. Mell and T. Grance. *The NIST definition of cloud computing*. Tech. rep. NIST, 2011.

[10] D. Villegas et al. "Cloud federation in a layered service model". In: *Journal of Computer and System Sciences* 78.5 (2012), pp. 1330–1344.

[11] L. Mei, W. K. Chan, and T. H. Tse. "A tale of clouds: Paradigm comparisons and some thoughts on research issues". In: *Asia-Pacific Services Computing Conference (APSCC)*. IEEE. 2008, pp. 464–469.

[12] M. P. Papazoglou. "Cloud blueprints for integrating and managing cloud federations". In: *Software Service and Application Engineering*. Springer, 2012, pp. 102–119.

[13] A. N. Toosi, R. N. Calheiros, and R. Buyya. "Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey". In: *ACM Computing Surveys (CSUR)* 47.1 (2014), p. 7.

[14] Y. Demchenko et al. "Intercloud Architecture Framework for Heterogeneous Cloud based Infrastructure Services Provisioning On-Demand". In: *International Conference on Advanced Information Networking and Applications*. IEEE, 2013.

[15] Technical White Paper. *Technical Requirements for Supporting the Intercloud Networking*. Tech. rep. GICTF, Apr. 2012.

[16] ITU-T Focus Group on Cloud Computing. *Part 2: Functional Requirements and Reference Architecture*. Tech. rep. Version 1.0. TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, Feb. 2012.

[17] D. Bernstein and V. Deepak. *Draft Standard for Intercloud Interoperability and Federation (SIIF)*. Tech. rep. IEEE P2303, 2014.

[18] B. Khasnabish et al. *Cloud Reference Framework*. Internet-Draft draft-khasnabish-cloud-reference-framework-02. Internet Engineering Task Force (IETF), 2014.

[19] A. Gavras et al. "Future Internet Research and Experimentation: The FIRE Initiative". In: *ACM SIGCOMM Computer Communication Review* 37.3 (2007), pp. 89–92.

[20] A. Gavras et al. "Pan European Laboratory for Next Generation Networks and Services". In: *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TRIDENTCOM)*. IEEE, 2006, pp. 436–441.

[21] A. Gavras et al. *Deliverable D2.1: Legal Framework (Version 2)*. Tech. rep. Panlab, 2008, pp. 1–34.

[22] J.-C. Imbeaux et al. *Deliverable D2.1: Vision for a Pan-European Laboratory (Version 2)*. Tech. rep. Panlab, 2007, pp. 1–52.

[23] J. Crowcroft et al. "Towards a collaboration and high-level federation structure for the FIRE Facility". In: *Working Group on modular federation of FIRE Facilities* (2009).

[24] W. Vandenberghe et al. "Architecture for the Heterogeneous Federation of Future Internet Experimentation Facilities". In: *Future Network and Mobile Summit (FNMS)*. Lisboa, Portugal, 2013, pp. 1–11.

[25] J. Van Ooteghem et al. "Sustaining a federation of Future Internet experimental facilities". In: *International Telecommunications Society (ITS) conference* (2014).

[26] O. Appleton. *D3.1: Business models for Federated e-Infrastructures*. Tech. rep. FedSM, 2012.

[27] T. Heger and U. Bub. "The EIT ICT Labs - Towards a Leading European Innovation Initiative". In: *it - Information Technology* 54.6 (2012), pp. 288–295.

[28] A. Willner et al. "FanTaaStic: Sustainable Management of Future Internet Testbed Federations". In: *6th International Workshop on Management of the Future Internet (ManFI)*. Krakow, Poland: IEEE/IFIP, 2014.

[29] S. Cretti et al. *Deliverable D1.4: Analysis of UC, Infrastructures and Enablers Version 2*. Tech. rep. XIFI, 2014, pp. 1–45.

[30] V. Chang et al. "A categorisation of cloud computing business models". In: *10th International Conference on Cluster, Cloud and Grid Computing*. IEEE/ACM. 2010, pp. 509–512.

[31] C. A. Poveda and M. G. Lipsett. "An integrated approach for sustainability assessment: the Wa-Pa-Su project sustainability rating system". In: *International Journal of Sustainable Development & World Ecology* 21.1 (2014), pp. 85–98.

[32] T. Kuhlman and J. Farrington. "What is sustainability?" In: *Sustainability* 2.11 (2010), pp. 3436–3448.

[33] H. S. A. Nawi et al. *Sustainability Criteria Model*. Tech. rep. A Field Study of ICT4D Project, 2013.

[34] R. R. Harmon and N. Auseklis. "Sustainable IT services: Assessing the impact of green computing practices". In: *Portland International Conference on Management of Engineering & Technology (PICMET)*. 2009, pp. 1707–1717.

[35] T. Zahariadis et al. "FIWARE Lab: Managing Resources and Services in a Cloud Federation supporting Future Internet Applications". In: *7th International Conference on Utility and Cloud Computing*. 604590. London, UK: IEEE/ACM, 2014.

[36] Y. Al-Hazmi et al. "Unified representation of monitoring information across federated cloud infrastructures". In: *26th International Teletraffic Congress (ITC)*. IEEE. 2014, pp. 1–6.

[37] Technical White Paper. *Seven design principles for building a converged cloud*. Tech. rep. HP, Apr. 2013.

[38] M. Bauer et al. "The context API in the OMA next generation service interface". In: *14th International Conference on Intelligence in Next Generation Networks (ICIN)*. IEEE. 2010, pp. 1–5.

[39] H. W. Chesbrough. *Open innovation: The new imperative for creating and profiting from technology*. Harvard Business Press, 2003.