The Path to Cloud Federation through Standardization

Robert B. Bohn[1], Ranganai Chaparadza[2], Muslim Elkotob[3], Taesang Choi[4]

Abstract — This paper describes the efforts of the NIST Cloud Computing Program in the development of understanding the federated cloud concept through the creation of a reference architecture, cooperation with the IEEE and resulting in the publication IEEE 2302-2021 Standard for Intercloud Interoperability and Federation (SIIF). Standards for cloud federation continue to show their growing importance due to the fact that cloud federation standards, mechanisms/techniques such as APIs, are the enablers for ICT assets and resource sharing by diverse stakeholders who can immensely benefit from the federations in creating new business models and even to test complex technologies and scenarios that can only be achieved through distributed and federated ICT assets. The growing industry requirement on Testbeds Federations benefits from Cloud Federation Standards and APIs (Application Programming Interfaces) a lot when Testbeds are implemented as Clouds, hence the recent creation of an ITU-T Focus Group on Testbeds Federations for IMT-2020 and Beyond (FG-TBFxG) under the parent ITU-T SG11 on Testing related topics is bound to benefit a lot from IEEE Cloud Federation Standards and APIs in its envisaged deliverables.

Index Terms— NIST Cloud Computing Program; IEEE 2302-2021 Standard for Intercloud Interoperability and Federation (SIIF); Cloud Federation through Standardization, ITU-T Focus Group on Testbeds Federations for IMT-2020 and Beyond (FG-TBFxG); Testing Federated Autonomic Management & Control Use Case for Federated Testbeds

I. Introduction

The NIST [2] Cloud Computing Program (NCCP) was formed in May 2010 with the purpose to foster and to ensure the secure and effective adoption of cloud computing into the USG by examining the high-priority strategic requirements in security, interoperability and portability. It carried that out by examining the current technological landscape to determine the relevant standards, guidance and technology that are needed to satisfy the requirements.

Recognizing the significance and breadth of the emerging cloud computing trend, NIST designed its program to support accelerated US government adoption, as well as leverage the strengths and resources of government, industry, academia, and standards organization stakeholders to support cloud computing technology innovation.

Standards are critical to ensure cost-effective and easy migration, to ensure that mission-critical requirements can be met, and to reduce the risk that sizable investments may become prematurely technologically obsolete. Standards are key to ensuring a level playing field in the global marketplace.

In September 2011, The NIST Definition of Cloud Computing was published as NIST SP 800-145 (Mell & Grance, 2011). It describes cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of three service models, and four deployment models and five essential characteristics**.** The three service models, Software as a Service (SaaS). Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are familiar by now. The 4 possible cloud deployment models they describe are: private cloud, public cloud, community cloud and hybrid cloud.

The essential characteristics of cloud computing are those traits that are expected to be demonstrated in order to fit the model. The 5 characteristics follow:

- *On-demand self-service* - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- *Broad network access* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

[1]Robert B. Bohn: NIST: robert.bohn@nist.gov
[2]Ranganai Chaparadza: ETSI AFI & IPv6Forum: ran4chap@yahoo.com
[3]Muslim Elkotob Vodafone, ETSI AFI: muslim.elkotob@vodafone.com
[4]Taesang Choi: ETRI: choits@etri.re.kr

- *Rapid elasticity* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

NIST published a “USG Cloud Computing Standards and Technology Roadmap” (NIST SP 500-293, Sept 2014) which identified the highest priority level requirements in security, interoperability and portability to further adopt cloud computing into the government. The roadmap primary focus on interoperability, portability, and security requirements does not preclude the need to address reliability, maintainability, performance, accessibility and other essential requirements.

These requirements were developed in collaboration with a series of cloud computing public working groups in reference architecture and vocabulary, security, use cases and standards. Each working group had two co-chairs, one from NIST and one from industry. In summation, there were over 300 participants in these groups.

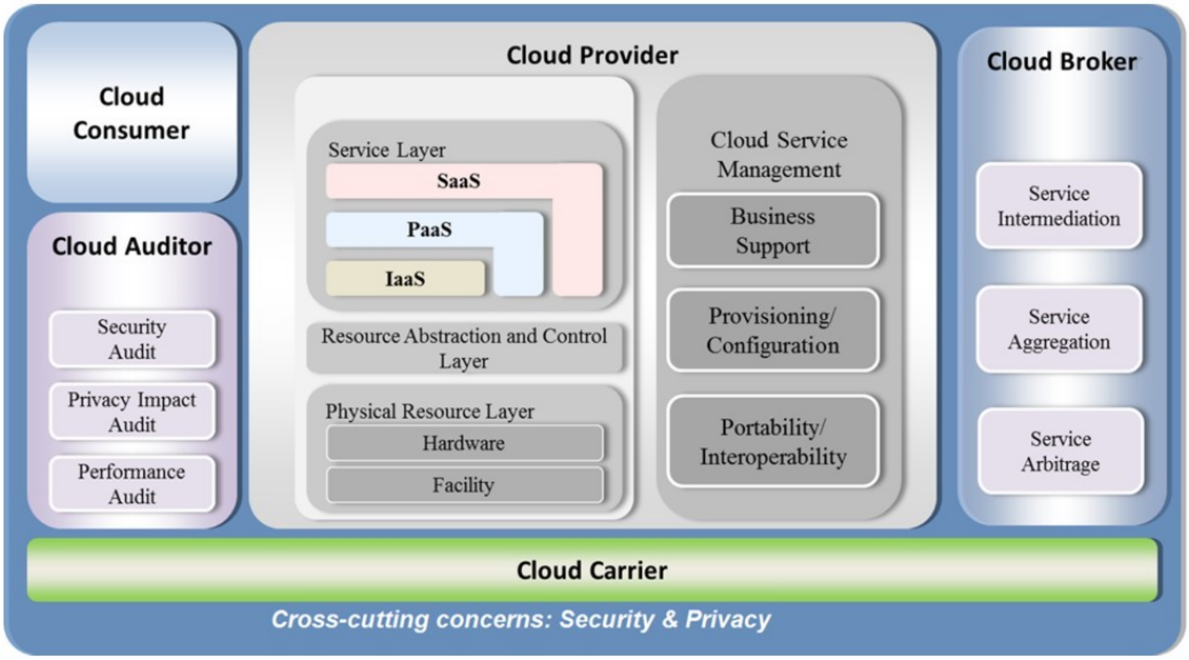

Figure 1: ***NIST Cloud Computing Reference Architecture (from NIST SP 500-293)***

The USG Cloud Computing Technology Roadmap requirements which are identified as high priorities to further USG Cloud Computing Technology Adoption are:

- *Requirement 1*: International voluntary consensus-based standards (interoperability, performance, portability, and security standards)
- *Requirement 2*: Solutions for High-priority Security Requirements, technically de-coupled from organizational policy decisions (security standards and technology)
- *Requirement 3*: Technical specifications to enable development of consistent, high-quality Service-Level Agreements (interoperability, performance, portability, and security standards and guidance)
- *Requirement 4*: Clearly and consistently categorized cloud services (interoperability and portability guidance and technology)
- *Requirement 5*: Frameworks to support seamless implementation of federated community cloud environments (interoperability and portability guidance and technology)
- *Requirement 6*: Updated Organization Policy that reflects the Cloud Computing Business and Technology model (security guidance)
- *Requirement 7*: Defined unique government regulatory requirements and solutions (accessibility, interoperability, performance, portability, and security technology)
- *Requirement 8*: Collaborative parallel strategic “future cloud” development initiatives (interoperability, portability, and security technology)
- *Requirement 9*: Defined and implemented reliability design goals (interoperability, performance, portability, and security technology)
- *Requirement 10*: Defined and implemented cloud service metrics (interoperability, performance, and portability standards)

<u>**Note:**</u> The order in which the requirements are listed does not imply relative importance.

The Reference Architecture and Vocabulary PWG produced a high-level reference architecture for cloud computing and published as NIST SP 500-292 (2011). This is an actor/role-based model which is also technology neutral. The initial input to this model was the definition of cloud computing. This model will be referred to as the CCRA in the remainder of the document.

This conceptual model describes the actors in a cloud computing environment and the roles that are assigned to them. There are 5 actors: A Cloud Consumer, Cloud Provider, Cloud Auditor, Cloud Carrier and a Cloud Broker. This model describes cloud computing without stipulating or mandating any specific technological solution which is important to an open marketplace. A vocabulary for cloud computing was also developed with this model as way to give the stakeholders a standard way of communicating the topics and themes in cloud computing. This way everybody has an equivalent starting point in which to guide further discussions.

The next section will describe the efforts of the NCCP and the IEEE in the development and approach to addressing Requirement 5 - Frameworks to support seamless implementation of federated community cloud environments by developing a high-level reference architecture, vocabulary and an IEEE standard.

II. NCCP and IEEE Collaboration on Cloud Federation

As shown above, Requirement 5 is concerned with frameworks to support seamless implementation of federated community cloud environments. The federated cloud model is related to the community cloud model in that the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. The keys to federation are how a User A can find services or resources from Service Provider B, how Service Provider B can manage its discoverability, and how can Service Provider B validate User A's credentials and make access decisions to use their cloud resources. This is identified in the figure below in which the Identity Provider A must be able to communicate with Service Provider B. The numbers in the figure (1-6) show the normal path of how a user is typically authenticated and authorized on a system using an identity provider who communicates the appropriate identity information so the Service Provider can complete the request.

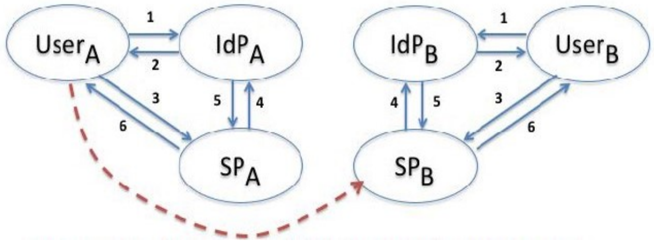

Figure 2: ***Federated authentication and authorization***

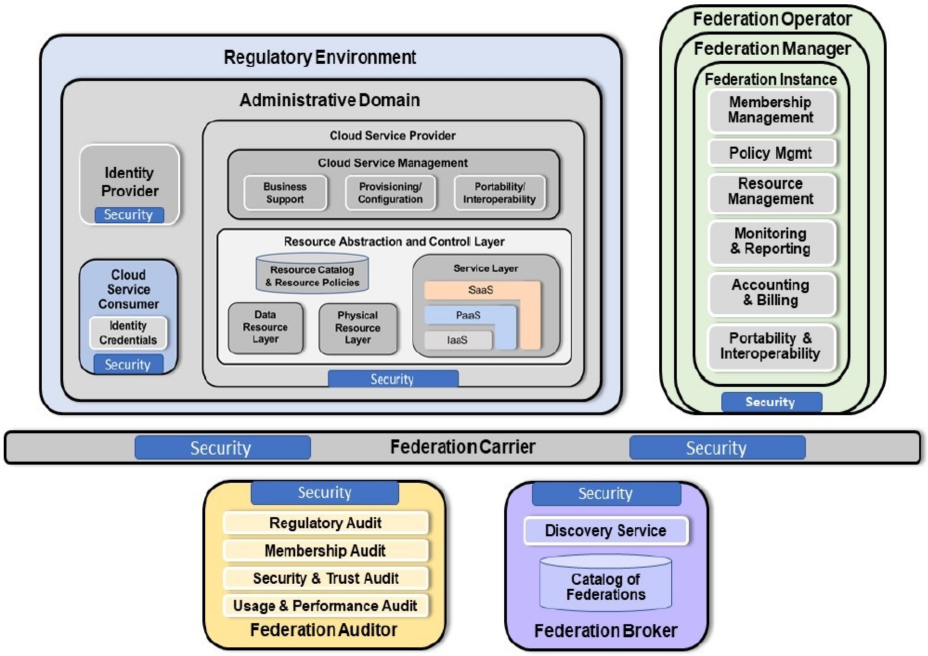

Figure 3: ***NIST Cloud Federation Reference Architecture (NIST SP 500-332)***

In mid-2017, the IEEE and NCCP agreed to collaborate on the development of the federated cloud model. In this arrangement, the NCCP public working group was charged with the development of a reference architecture and a vocabulary for cloud federation and the IEEE would use that output to develop a standard in the IEEE-P2302 working group. This arrangement followed a feedback system in which the NCCP was able to deliver concepts and add to the discussion of the P2302 and it was able to give feedback to the NCCP team.

This collaboration resulted in the publication of a NIST Cloud Federation Reference Architecture (CFRA) in February 2020 as NIST SP 500-332. This model has many similarities to the original cloud computing reference model from NIST SP 500-292. For example, this CFRA is also an actor/role-based model for the same reasons the original CCRA was. It is important to ensure that it is a technology neutral model.

There are many similarities in the actors in this model and the CCRA. The notable additions to this model are the explicit identification of regulatory environments, administrative domains, an identity provider and the Federation Operator/Manager/Instance.

When 2 entities decide to federate their cloud infrastructure, one can consider this interaction as a 3-plane model where the planes are identified as a “Trust Federation Plane”, “Federation Management Plane” and a Federation Usage Plane. The Trust Plane is the initial phase in which the two Site Administrators decide to create a federation and by doing so need to establish a trust of some design. Once each Site Admin deploys a Federation Manager (FM), they can set up a secure communication pathway to interact. The trust models and the security design were not prescribed in the model in order to allow for technological innovation and flexibility. This is necessary since the FMs must exchange information concerning the management of federations that is valid and trusted. The Site Admins also populate the Federation with the necessary information about the users, policies and services. Finally, when “up and running”, the federation logically consists of users and services from either site. These users can discover and use those services. That discovery and use is governed by the specific policies that are associated with those services for this federation.

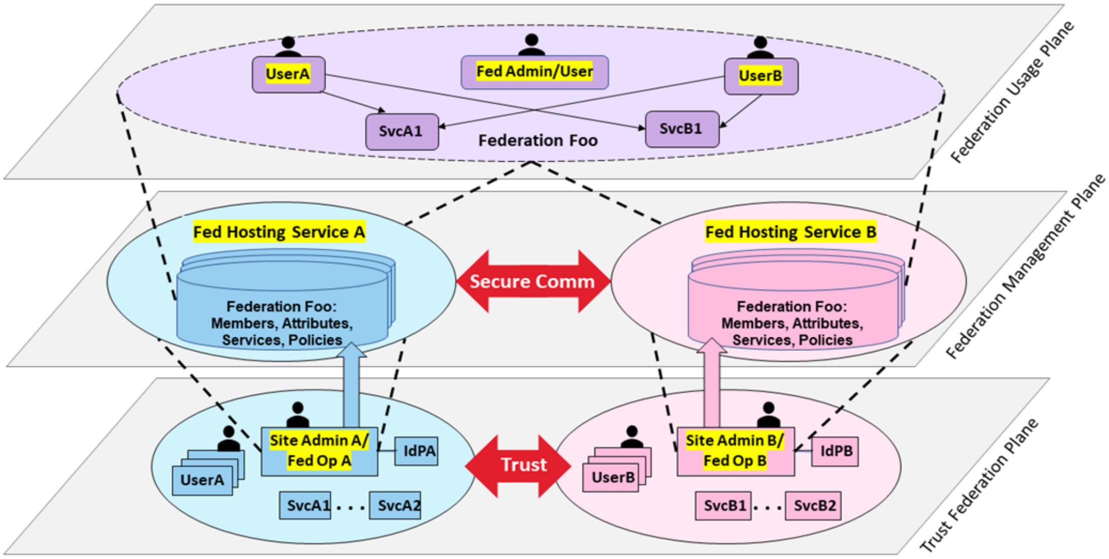

Figure 4: ***3-Plane Model of Cloud Federation***

III. IEEE 2302-2021 Standard for Intercloud Interoperability and Federation

The IEEE P2302 working group was able to use this conceptual description in the creation of its own standard which was published in December 2021. The Project Authorization Request for P2302 states the purpose of the standard to create an economy amongst cloud providers that is transparent to users and applications, which provides for a dynamic infrastructure that can support evolving business models. The scope is to define the topology, functions, and governance for cloud-to-cloud interoperability and federation.

The working group was able to identify a series of potential deployments for a federation in which they can be peer-to-peer (as shown above) or operate in a 3rd party centralized trust deployment in which one site does the deployment of the federation hosting service. In this description, the federation hosting service will need the ability to communicate with the users (members of the federation), the federation operator and other federations (if necessary) through a series of endpoints and APIs. In this way, the FHS model developed by the P2302 is essentially a set of communicating API gateways. The 3 APIS developed here are the FHS Operator API, FHS Member API and finally the FHS-FHS API which allows 2 Federation Hosting Services to communicate.

Using the small deployments described in the standard, one can build up much larger federations. The range of possible Cloud Federation deployments is large. They can vary from the small, informal arrangements all the way through to large industrial sized federations which need to consider automation, legal frameworks, auditing, and billing. The 2302-2021 standard describes the different levels of potential federation, with Level 1 as the core functions for a base federation. Level 2 begins to incorporate accounting functions as billing and auditing. Level 3 federations start to consider legal and compliance agreements. Finally, Level 4 federations focus on automation of these tasks.

IV. The value of the ITU-T Focus Group (FG-TBFXG) On Testbeds Federations for 5G & Beyond

Federation in general and federated testbeds in particular form a key part of the success of CSPs (Communication Service Providers) and other stakeholders to leverage their assets, monetize on their investments, and position themselves in their ecosystem of 5G and beyond in which everything is evolving very dynamically. Federated testbeds bring sustainability in fostering environments for quick innovations and testing of complex technologies and use cases, and for enabling quicker time to market for products and services. Federated testbeds, enabled as a turnkey service such as testbed-as-a-service (TaaS), bring a lot of value to research use cases and industrial use cases. Yet, Standards have been lacking in this increasingly very important area of testbeds federations and interoperability. Standards are the enablers for interoperability and further benefits. Therefore, it is important to note that research communities and the industry (solutions vendors/suppliers, CSPs, enterprises, and standards development organizations (SDOs)/Fora) all have roles to play in this desired ecosystem that should be built around the Testbeds Federations Reference Model recently standardized by ITU-T (under ITU-T Q.4068 [4]) both now and into the future in the era of disaggregation of ICT networks, 5G and beyond, as well the shift towards software in services, assets, etc. One of the Use Cases for Testbeds Federations for 5G and Beyond that is of interest to CSPs is Testing of Federated Autonomic (Close-Loop) Management and Control operations for networks and services by ETSI GANA (Generic Autonomic Networking Architecture) Knowledge Plane (KP) Platforms [5] in 5G Multi-Operator Scenarios [3].

In order to reinforce the work in ITU-T SG11 on Testbeds Federations, a special Focus Group was created in 2021 (had its kick-off meeting in 2022) under the parent ITU-T Study Group 11, called ITU-T Focus Group on Testbeds Federations for IMT-2020 and Beyond (FG-TBFxG) [1]. The FG-TBFxG is now working on a set of deliverables and is encouraging all various stakeholders impacted by Testbeds for 5G & Beyond to join the activities. It consists of three working Groups defined as follows (more details are found at the Focus Group Website [1]):

- **WG1**: ***Use Cases, Applications and Industry Demand, Business Models*** → this Working Group focuses on the ecosystem perspective combining stakeholders engaged in Federation scenarios, on the business value in Testbeds Federations and the underlying use cases, as well as the industry and verticals perspectives with respect to Federation.
- **WG2**: ***Testbeds as a Service*** → this Working Group has as a key target to expose different assets and make them available to services that are dynamically composed to serve collaboration and value-adding purposes primarily via Federation.
- **WG3**: ***APIs, Reference Model Instantiations*** → this Working Group works on developing a blueprint reference model for Testbeds Federations, including instantiations of this Reference Model in different scenarios. Furthermore, key building blocks and enablers for Testbeds Federations such as APIs and Reference Points are being specified and worked on in this working Group. One of APIs that have great potential to be used in Testbeds Federations is the Cloud Federations API defined by IEEE Std 2302™-2021.

Acknowledgement: This work was *Partially* supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Ministry of Trade, Industry and Energy (MTIE) (No., P0019809: Building Enablers for Multi Industry Sectors Collaborative Federated Testbeds, as a Foundation (Distributed Open Platform) for Cross-Industry End-to-End Services Innovation and Delivery Agility in the 5G & Beyond)"

REFERENCES

[1] "ITU-T ETSI IEEE Joint SDOs Brainstorming Workshop on Testbeds Federations for 5G & Beyond: Interoperability, Standardization, Reference Model & APIs" (www.itu.int/go/BTF4-5G) that took place 15-16 March 2021; ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) (www.itu.int/go/fgtbf).

[2] National Institute of Standards and Technology https://www.nist.gov/

[3] ETSI Work Item: Core Network and Interoperability Testing (INT); Description of Test Requirements and Approach for E2E Federated Testbeds: Description of Test Requirements and Approach for E2E Federated Testbeds. With an Example Use Case of Testing Federated Autonomic Management and Control (AMC) operations (e.g. by GANA) Components Within and Across Multiple 5G Network Operators. https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=59577

[4] ITU-T Q.4068 : Open application program interfaces (APIs) for interoperable testbed federations: https://www.itu.int/rec/T-REC-Q.4068-202108-P

[5] ETSI TS 103 195-2 (published by ETSI in May 2018): Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: *An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management*

[6] The NIST Defn of CC-
Mell, P, and Grance, T. "The NIST Definition of Cloud Computing." NIST Special Publication, 800-145, (2011).

[7] The NIST Cloud Computing Reference Architecture –
Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D.NIST Cloud Computing Reference Architecture: NIST Special Publication 500-292, (2012).

[8] US Government Cloud Computing Technology Roadmap-
Badger L, Bernstein D, Bohn R, de Vaulx F, Hogan M, Iorga M, Leaf D, Mao J, Messina J, Mills K, Simmon E. US Government Cloud Computing Technology Roadmap, NIST Special Publication 500-293, (2014).

[9] The NIST Cloud Federation Reference Architecture-
Lee, C. A., Bohn, R. B., & Michel, M. The NIST Cloud Federation Reference Architecture, NIST Special Publication, 500-332. (2020).

[10] IEEE 2302-2021 Standard for Intercloud Interoperability and Federation (2021)

[11] IEEE's Cloud Continuum (**2**,2022). This can be downloaded from: https://ieeecs-media.computer.org/media/marketing/cloud-continuum/cc-vo2-no1.pdf