Defining Inter-Cloud Architecture for Interoperability and Integration

[1]Yuri Demchenko, [1]Canh Ngo, [1,2]Marc X. Makkes, [1,2]Rudolf Strijkers, [1]Cees de Laat
[1]University of Amsterdam
System and Network Engineering Group
Amsterdam, The Netherlands
e-mail: {y.demchenko, c.t.ngo, delaat}@uva.nl

[2]TNO
Information and Communication Technology
Groningen, The Netherlands
e-mail: {marc.makkes, rudolf.strijkers}@tno.nl

Abstract—**This paper presents an on-going research to develop the Inter-Cloud Architecture, which addresses the architectural problems in multi-provider multi-domain heterogeneous cloud based applications integration and interoperability, including integration and interoperability with legacy infrastructure services. Cloud technologies are evolving into a common way to virtualize infrastructure services and to offer on-demand service provisioning. In this way, they add physical/hardware platform independency and mobility to the existing distributed computing and networking technologies. The paper uses existing standards in Cloud Computing, in particular the recently published NIST Cloud Computing Reference Architecture (CCRA) as the basis for the Inter-Cloud architecture. The proposed Inter-Cloud Architecture defines three complimentary components addressing Inter-Cloud interoperability and integration: multi-layer Cloud Services Model that combines commonly adopted cloud service models, such as IaaS, PaaS, SaaS, in one multilayer model with corresponding inter-layer interfaces; Inter-Cloud Control and Management Plane that supports cloud based applications interaction; and Inter-Cloud Federation Framework. The paper briefly presents the architectural framework for cloud based infrastructure services provisioning being developed by the authors. The proposed architecture intends to provide a basis for building multilayer cloud services integration framework and to allow optimised provisioning of computing, storage and networking resources. In this way, the proposed Inter-Cloud architecture will facilitate cloud interoperability and integration.**

Keywords-Inter-Cloud Architecture; Cloud Computing Reference Architecture; Architectural framework for cloud infrastructure services provisioned on-demand; Cloud middleware.

I. INTRODUCTION

Cloud computing technologies [1, 2] are emerging as infrastructure services for provisioning computing and storage resources on-demand in a simple and uniform way and may involve multi-provider and multi-domain resources, including integration with the legacy services and infrastructures. Cloud computing represents a new step in evolutional computing and communication technology development by introducing a new abstraction layer for general virtualisation of infrastructure services (similar to utilities) and mobility. Current developments in cloud technologies demonstrate the need to (1) develop an Inter-Cloud architecture that provides a common/interoperable environment and definition for moving existing infrastructures and infrastructure services into cloud environments and (2) integration tools to include existing enterprise and campus infrastructures. More complex use of cloud infrastructure services, such as in multi-domain enterprise environments, require new service provisioning and security models that allow on-demand provisioning of complex project and group-oriented infrastructure services across multiple providers.

Cloud based virtualisation enables easy upgrade and/or migration of enterprise application, including also the whole Information Technology (IT) infrastructure segments with automation or infrastructure management tools This brings significant cost savings compared to traditional infrastructure development and management, which requires lot of manual work. In particular, applications that use modern SOA (Service Oriented Architecture) web services platforms for services and integration benefit from cloud based infrastructure services, such as elastic scaling and on-demand provisioning. However, their composition and integration into distributed cloud based infrastructure will require a number of functionalities and services that can be jointly defined as Inter-Cloud Architecture.

This paper presents an on-going research at the University of Amsterdam to develop the Inter-Cloud Architecture (ICA). The Inter-Cloud architecture addresses the problem of (1) multi-domain heterogeneous cloud based applications integration and interoperability, including integration and interoperability with legacy infrastructure services, and (2) intra-provider infrastructure interoperability and measurability, and (3) cloud federation. The papers refers to the architectural framework for provisioning Cloud Infrastructure Services On-Demand [3] being developed by authors as a result of cooperative efforts in a number of currently running projects such as GEANT3 [4] and GEYSERS [5]. The architectural framework provides a basis for defining the proposed Inter-Cloud architecture. The presented paper significantly extends the research results initially presented as a poster paper at the IEEE CloudCom2011 Conference [6].

The remainder of the paper is organized as follows. Section II provides overview and detailed analysis of the ongoing standardisation activities at NIST and IEEE that have direct relation with and provide a basis for the proposed ICA. Section III describes a basic use case for defining ICA, and section provides motivation and defines the main components of the proposed Inter-Cloud Architecture. In Sections IV the Inter-Cloud definition and requirements are described. Section V describes the abstract model for cloud based infrastructure services provisioning. Section VI describes the Infrastructure Services Modeling Framework that provides a basis for complex infrastructure services composition and management. The paper concludes with future developments in Section VII.

II. CLOUD STANDARDISATION OVERVIEW

Two standardization activities form the basis of ICA and will be analysed in detail. One, the Cloud Computing technology and Cloud Computing Reference Architecture definition by the National Institute of Standards and Technology (NIST) and two, the IEEE standardisation activity to define Intercloud Interoperability and Federation framework. Suggestions are provided for the required extensions in the context of the proposed Inter-Cloud Architecture.

An overview of the standards that define internal cloud management, components design and communications is left out. This category of standards is well presented by DMTF, SNIA and OGF standards that correspondingly define standards for Open Virtual Machine Format (OVF) [7], Cloud Data Management Interface (CDMI) [8], and Open Cloud Computing Interface (OCCI) [9]. These standards are commonly accepted by industry and provide a basis for intra-provider infrastructure operation and services delivery to customers.

A. NIST Cloud Computing related standards

NIST is active in fostering cloud computing practices that support interoperability, portability, and security requirements that are appropriate and achievable for important usage scenarios. Since first publication of the currently commonly accepted NIST Cloud definition in 2008, NIST is leading the internationally recognised activity on defining a conceptual and standardised base in Cloud Computing. The ongoing publications of their activities create a solid base for cloud services development and offering:

NIST SP 800-145, NIST definition of cloud computing [1]

NIST SP 500-292, Cloud Computing Reference Architecture, v1.0 [2]

DRAFT NIST SP 800-146, Cloud Computing Synopsis and Recommendations [10]

NIST SP500-291 NIST Cloud Computing Standards Roadmap [11]

Draft SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing [12]

1) NIST Cloud Computing Reference Architecture (CCRA)

NIST SP 800-145 document defines Cloud Computing in the following way:

"Cloud computing is 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 promotes availability and is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling. rapid elasticity, measured Service), 3 service/provisioning models. (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)), 4 deployment models (public, private, community, hybrid clouds)."

The IaaS service model is defined in the following way:

"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of selecting networking components (e.g., host firewalls)."

Figure 1 presents a high level view of the NIST Cloud Computing Reference Architecture (CCRA), which identifies the major actors (Cloud Consumer, Cloud Service Provider, Cloud Auditor, Cloud Broker, and Cloud Carrier), their activities and functions in cloud computing. A cloud consumer may request cloud services from a cloud provider directly or via a cloud broker. A cloud auditor conducts independent audits and may contact the others to collect necessary information.

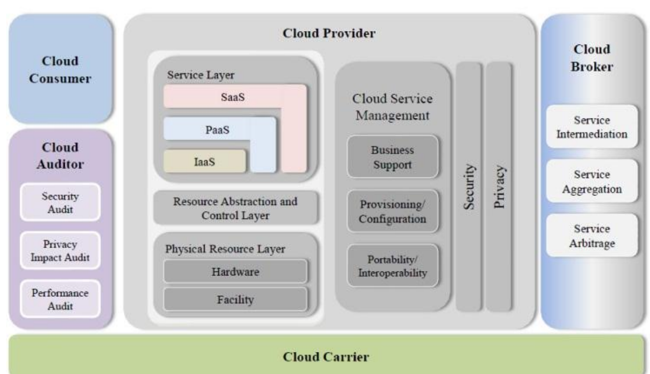


Figure 1. NIST Cloud Computing Reference Architecture (CCRA) [2]

The proposed architecture is suitable for many purposes where network performance is not critical but needs to be extended with explicit network services provisioning and management when the cloud applications are critical to network latency like in case of enterprise applications, business transactions, crisis management, etc.

2) Extending Cloud definition and CCRA for ICA

NIST CCRA and Cloud Computing definition are well suited for describing service, business, or operational relations. However, it has limited applicability for design purposes, i.e. defining basic functional components, interfaces, and layers.

The recently published CCRA includes the Cloud Carrier role, a role typical for telecom operators, which provides network connectivity as a 3rd party service. Despite the introduction of the Cloud Carrier role, there is no well-defined service model how network connectivity as a 3rd parte service be achieved. The IaaS cloud service model does not explicitly include provisioning of network services and infrastructure. One reason is that cloud computing has been developed primarily for provisioning storage and computing resources in the assumption that best-effort Internet connectivity is sufficient. However, this situation presents serious limitations for large scale use of cloud in enterprise applications that require guaranteed network connectivity QoS and low network latency in particular.

Another limitation of the current CCRA is that it is unsuitable for defining a security infrastructure and its integration with infrastructure services, which can be potentially multilayer and multi-domain.

The following extensions and improvements should be made to at least the Cloud IaaS model to meet requirements of a wide range of critical enterprise services (other service models such as PaaS, SaaS should also allow management of network related parameters):

- Define a layered cloud services model suitable for defining inter-layer and inter-service (functional) interfaces,
- Define virtualisation of resources and services as cloud features (in which virtualisation includes resource abstraction, pooling, composition, instantiation, orchestration, and lifecycle management),
- Include QoS provisioning and user / application control over QoS in the network services definition,
- Define an infrastructure service that includes the following attributes/features:
  - Topology description of computing, storage resources and their interconnection in the network infrastructure,
  - Infrastructure/topology description format that allows topology transformation operations for control and optimization (e.g., homomorphic, isomorphic, QoS, energy aware etc.).

In the context of the above definition, cloud infrastructure may include:

- Internal cloud provider infrastructure which is provided as a service, and
- External or Inter-Cloud infrastructure that can be provided by either a cloud operator or a network services provider.

In relation to business/operational aspects, the CCRA should be extended to address the following features:

- Better definition of the Cloud Carrier role, operational model and interaction with other key actors,
- Extend the set of basic roles with roles typical for telecom operators/providers as Cloud/infrastructure Operator, and split Customer role on Customer and User as representing customer organization and end-user.

B. IEEE Intercloud Working Group (IEEE P2302)

IEEE P2302 Working Group recently published a draft Standard on Intercloud Interoperability and Federation (SIIF) [13] proposing an architecture that defines topology, functions, and governance for cloud-to-cloud interoperability and federation.

Topological elements include clouds, roots, exchanges (which mediate governance between clouds), and gateways (which mediate data exchange between clouds). Functional elements include name spaces, presence, messaging, resource ontologies (including standardized units of measurement), and trust infrastructure. Governance elements include registration, geo-independence, trust anchor, and potentially compliance and audit.

However, the proposed approach has very limited scope by attempting to address a hypothetical scenario when all resources and applications will be located and run in multiple clouds and they need to be federated similar to Contend Distribution Network (CDN) [14]. The proposed architecture tries to replicate the CDN approach but doesn't address the generic problems with interoperability and integration of the heterogeneous multi-domain and multi-provider clouds.

The proposed solutions are built around extended use of the XMPP [15] as a base Intercloud protocol and introduce Intercloud Root and Exchange Hosts to support Intercloud communications, trust management and identity federation.

The proposed architecture originated from the position paper published by Cisco in 2009 [16] that tried to leverage the basic routing and messaging Internet protocols such as BGP, OSPF, XMPP to address Inter-Cloud integration and interoperability.

The limitation of the proposed architecture and approach is that it tries to closely imitate Internet approach in building hierarchical interconnected infrastructure for Internet protocol based services to support Inter-Cloud communication. But actually there is no need for such additional Inter-Cloud layer or infrastructure because cloud applications and infrastructure can use all Internet technologies directly to support intra-provider communications and user-customer-provider or inter-provider communications, given the appropriate network virtualisation and address translation technologies. Cloud technologies provide a virtualisation platform for IT and network services and allow entire infrastructure instantiation together with related protocols and core infrastructure services related to control and management functions. An extreme use case that demonstrates the capabilities of cloud technologies is to create managed virtual Internets [27] using advanced programmable networking concepts [18].

III. GENERAL USE CASES FOR ICA

The two basic use cases for Inter-Cloud architecture can be considered: large project-oriented scientific infrastructure provisioning including dedicated transport network infrastructure, and periodic semester based educational course that requires computer laboratory facilities to setup, operated and suspended till the next semester [19]. Both cases should allow the whole infrastructure of computers, storage, network and other utilities to be provisioned on-demand, physical platform independent and allow integration with local persistent utilities and legacy services and applications.

Figures 2 illustrates the typical e-Science or enterprise infrastructure that includes enterprise proprietary and Cloud based computing and storage resources, instruments, control and monitoring system, visualization system, and users represented by user clients.

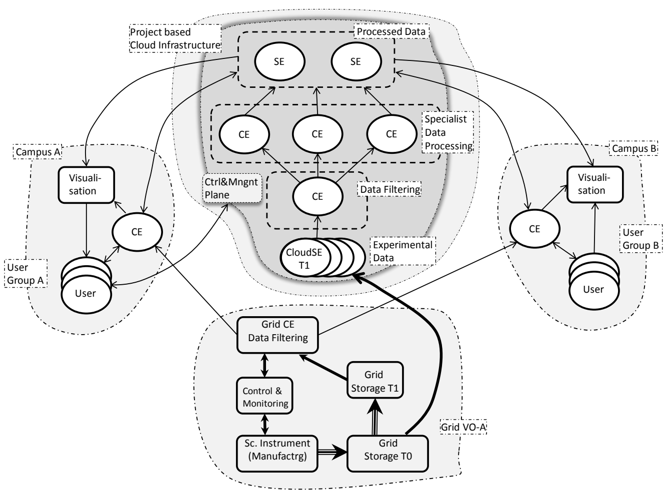


Figure 2. Project oriented collaborative infrastructure containing Grid based Scientific Instrument managed by Grid VO-A, 2 campuses A and B, and Cloud based infrastructure provisioned on-demand.

Figure 2 also illustrates a typical use case when two or more cooperative users/researcher groups in different locations want to use high performance infrastructure. In order to fulfill their task (e.g. cooperative image processing and analysis) they require a number of resources and services to process raw data on distributed Grid or Cloud data centers, analyse intermediate data on specialist applications and finally deliver the result data to the users/scientists. This use case includes all basic components of the typical e-Science research process: data collection, data mining, filtering, analysis (with special scientific applications), visualisation, and finally presentation to the users.

IV. ICA DEFINITION AND REQUIREMENTS

The developed Inter-Cloud Architecture should address the interoperability and integration issues in the current and emerging heterogeneous multi-domain and multi-provider clouds that could host modern and future critical enterprise infrastructures and applications.

The proposed ICA should address the following goals, challenges and requirements:

- ICA should support communication between cloud applications and services belonging to different service layers (vertical integration), between cloud domains and heterogeneous platforms (horizontal integration).
- ICA should provide a possibility that applications could control infrastructure and related supporting services at different service layers to achieve run-time optimization (Inter-Cloud control and management functions).
- ICA should support cloud services/infrastructures provisioning on-demand and their lifecycle management, including composition, deployment, operation, and monitoring, involving resources and services from multiple providers.

Following the above requirements, we define the subsequent complimentary components of the proposed Inter-Cloud Architecture:

(1) Multilayer Cloud Services Model (CSM) for vertical cloud services interaction, integration and compatibility;

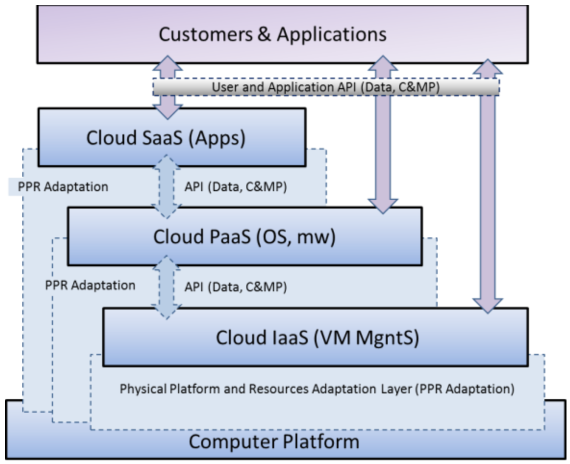
(2) Inter-Cloud Control and Management Plane (ICCMP) for Inter-Cloud applications/infrastructure control and management, including inter-applications signaling, synchronization and session management, configuration, monitoring, run time infrastructure optimization including VM migration, resources scaling, and jobs/objects routing;

(3) Inter-Cloud Federation Framework (ICFF) to allow independent clouds and related infrastructure components federation of independently managed cloud based infrastructure components belonging to different cloud providers and/or administrative domains; this should support federation at the level of services, business applications, semantics, and namespaces, assuming special gateway or federation services.

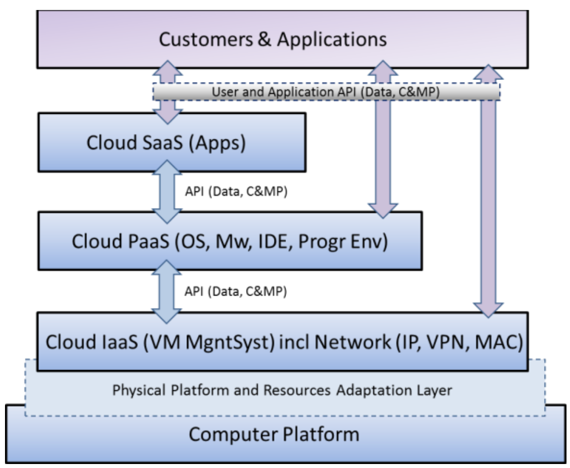
At this stage of research, we define only multi-layer Cloud Services Architecture that can be built using modern SOA technologies re-factored to support basic cloud service models as discussed below and in the following section. Future research on ICCMP will leverage User Programmable Virtualised Networks (UPVN) [20], and Internet technologies such as provided by CDN and Generalized Multi-Protocol Label Switching (GMPLS) [21]. The ICFF can be built using existing platforms for federated network access and federated identity management widely used for multi-domain and multi-provider infrastructure integration.

Figure 3 illustrates the current relation between basic Cloud service models IaaS, PaaS, SaaS that expose standards based interfaces to users, services, and applications but use proprietary interfaces to the physical provider platform. In case the application or service spans multiple heterogeneous cloud service providers, cloud services from different service models and layers will need to interact. This motivates definition of the Inter-Cloud Architecture that is depicted on Figure 3b as multilayer architecture with interlayer interfaces.

ISBN: 978-1-61208-216-5



(a) Current relation between Cloud service models



(b) current relation between Cloud service models

Figure 3. Inter-Cloud Architecture for Cloud interoperability and integration.

In the proposed Inter-Cloud layered service model, the following layers can be defined (numbering from bottom up):
(6) Customers and applications,
(5) SaaS (or cloud applications) as a top cloud layer that represents cloud applications,
(4) PaaS provides middleware services to customers and applications (6) or used as a platform for (5),
(3) IaaS provides infrastructure services to (6) or used for hosting cloud platforms (4),
(2) Cloud virtualisation and management layer (e.g. represented by VMWare as virtualisation platform, and OpenNebula, OpenStack as cloud management software),
(1) Physical hardware (e.g. physical servers, network devices).

V. ABSTRACT MODEL FOR CLOUD BASED INFRASTRUCTURE SERVICES PROVISIONING

Figure 4 below illustrates the abstraction of the typical project or group-oriented Virtual Infrastructure (VI) provisioning process that includes both computing resources and supporting network that commonly referred as infrastructure services. The figure also shows the main actors involved into this process, such as Physical Infrastructure Provider (PIP), Virtual Infrastructure Provider (VIP), Virtual Infrastructure Operator (VIO).

The required supporting infrastructure services are pictured on the left side of the picture and includes functional components and services used to support normal operation of all mentioned actors. The Virtual Infrastructure Composition and Management (VICM) layer includes the Logical Abstraction Layer and the VI/VR Adaptation Layer facing correspondingly lower PIP and upper application layer. VICM related functionality is described below as related to the proposed Composable Services Architecture (CSA).

The proposed architecture is SOA based and uses the same basic operational principles as known and widely used by SOA frameworks. Consequently, the proposed architecture also provides a direct mapping to the possible VICM implementation platforms such as Enterprise Services Bus (ESB) [22] or OSGi framework [23].

The infrastructure provisioning process, also referred to as Service Delivery Framework (SDF), is adopted from the TeleManagement Forum SDF [24] with necessary extensions to allow dynamic services provisioning. It includes the following main stages: (1) infrastructure creation request sent to VIO or VIP that may include both required resources and network infrastructure to support distributed target user groups and/or consuming applications; (2) infrastructure planning and advance reservation; (3) infrastructure deployment including services synchronization and initiation; (4) operation stage, and (5) infrastructure decommissioning. The SDF combines in one provisioning workflow all processes that are run by different supporting systems and executed by different actors.

Physical Resources (PR), including IT resources and network, are provided by Physical Infrastructure Providers (PIP). In order to be included into VI composition and provisioning by the VIP they need to be abstracted to Logical Resource (LR) that will undergo a number of abstract transformations including possibly interactive negotiation with the PIP. The composed VI need to be deployed to the PIP which will create virtualised physical resources (VPR) that may be a part, a pool, or a combination of the resources provided by PIP.

The deployment process includes distribution of common VI context, configuration of VPR at PIP, advance reservation and scheduling, and virtualised infrastructure services synchronization and initiation, to make them available to Application layer consumers.

The proposed abstract model provides a basis for ICA definition and allows outsourcing the provisioned VI operation to the VI Operator (VIO) who is from the user/consumer point of view provides valuable services of the required resources consolidation - both IT and networks, and takes a burden of managing the provisioned services.

 ISBN: 978-1-61208-216-5

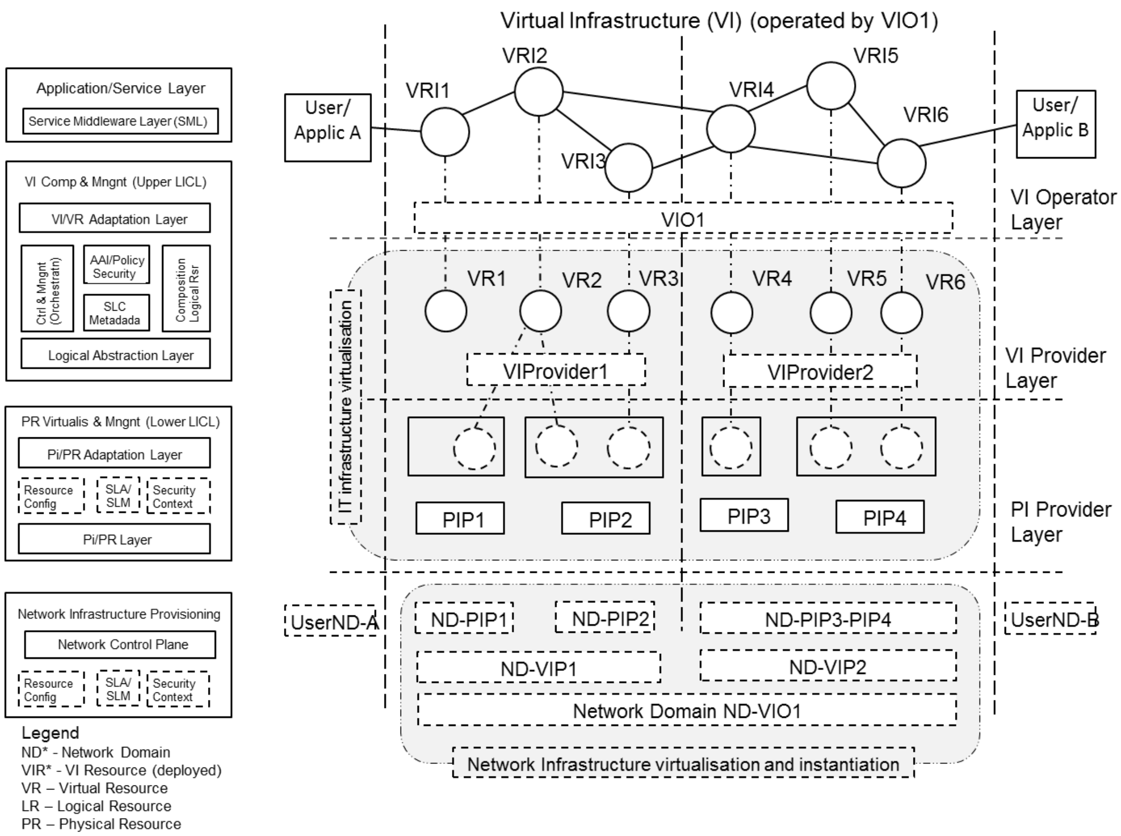


Figure 4. Main actors, functional layers and processes in on-demand infrastructure services provisioning

It is important to mention that physical and virtual resources discussed here are in fact complex software enabled systems with their own operating systems and security services. The VI provisioning process should support the smooth integration into the common federated VI security infrastructure by allowing the definition of a common access control policy. Access decisions made at the VI level should be trusted and validated at the PIP level. This can be achieved by creating dynamic security associations during the provisioning process.

VI. INFRASTRUCTURE SERVICES MODELING FRAMEWORK

The Infrastructure Services Modeling Framework (ISMF) provides a basis for virtualization and management of infrastructure services, including description, discovery, modeling, composition, and monitoring. In this paper we mainly focus on the description of resources and the lifecycle of these resources. The described model in this section is being developed in the GEYSERS project [5].

A. *Resource Modeling*

The two main descriptive elements of the ISMF are the infrastructure topology and descriptions of resources in that topology. Besides these main ingredients, the ISMF also allows for describing QoS attributes of resources, energy related attributes, and attributes needed for access control.

The main requirements for the ISMF are, that it should allow for describing Physical Resources (PR) as well as Virtual Resources (VR). Describing physical aspects of a resource means that a great level of detail in the description is required while describing a virtual resource may require a more abstract view. Furthermore, the ISMF should allow for manipulation of resource descriptions such as partitioning and aggregation. Resources on which manipulation takes place, and resources that are the outcome of manipulation are called Logical Resources (LR).

The ISMF is based on semantic web technology. This means that the description format will be based on the Web Ontology Language (OWL) [25]. This approach ensures the ISMF is extensible and allows for easy abstraction of resources by adding or omitting resource description elements. Furthermore, this approach has enabled us to re-use the Network Description Language [26] to describe infrastructure topologies.

B. *Virtual Resource Lifecycle*

Figure 5 illustrates relations between different resource presentations along the provisioning process that can also be defined as the Virtual Resource lifecycle.

The Physical Resource information is published by a PIP to the Registry service serving VICM and VIP. This published information describes a PR. The published LR information presented in the commonly adopted form (using common data or semantic model) is then used by VICM/VIP composition service to create the requested infrastructure using a combination of (instantiated) Virtual Resources and interconnecting them with a network infrastructure. In its own turn the network can be composed of a few network segments run by different network providers.

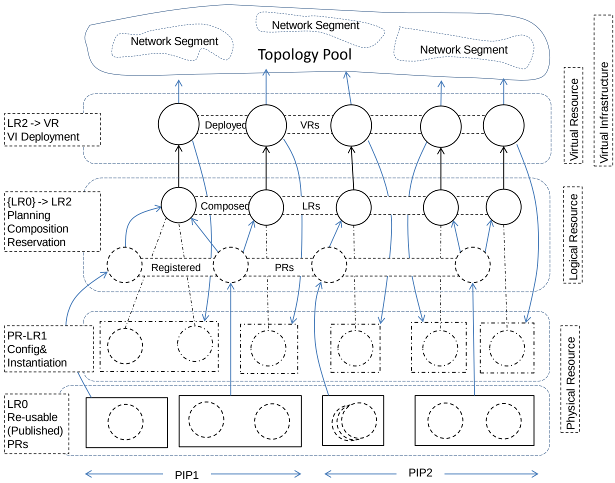


Figure 5. Relation between different resource presentations in relation to different provisioning stages.

VII. FUTURE DEVELOPMENT

The paper presents an on-going research at the University of Amsterdam to develop the Inter-Cloud Architecture (ICA) addresses the problem of multi-domain heterogeneous Cloud based applications integration and inter-provider and inter-platform interoperability.

The presented research is planned to be contributed to the Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) [27], where the authors play active role.

ACKNOWLEDGEMENTS

This work is supported by the FP7 EU funded Integrated project The Generalized Architecture for Dynamic Infrastructure Services (GEYSERS, FP7-ICT-248657) and by the Dutch national program COMMIT.

REFERENCES

[1] NIST SP 800-145, "A NIST definition of cloud computing", [online] Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] NIST SP 500-292, Cloud Computing Reference Architecture, v1.0. [Online] http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf

[3] Generic Architecture for Cloud Infrastructure as a Service (IaaS) Provisioning Model, Release 1. SNE Techn. Report SNE-UVA-2011-03, 15 April 2011. [Online] http://staff.science.uva.nl/~demch/worksinprogress/sne2011-techreport-2011-03-clouds-iaas-architecture-release1.pdf

[4] GEANT Project. [Online] http://www.geant.net/pages/home.aspx

[5] Generalised Architecture for Dynamic Infrastructure Services (GEYSERS Project). [Online] http://www.geysers.eu/

[6] Demchenko, Y., R.Strijkers, C.Ngo, M.Cristea, M.Ghijsen, C. de Laat, Defining Inter-Cloud Architecture. Poster paper. Proc. 3rd IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2011), 29 November - 1 December 2011, Athens, Greece. ISBN: 978-960-93-3482-2

[7] Open Virtualization Format (OVF), DMTF. [online] http://www.dmtf.org/standards/ovf

[8] Cloud Data Management Interface, SNIA. [online] http://www.snia.org/cdmi

[9] GFD.183 Open Cloud Computing Interface - Core [online] http://www.ogf.org/documents/GFD.183.pdf DRAFT NIST SP 800-146, Cloud Computing Synopsis and Recommendations. [online] Available: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[10] NIST SP 800-146, Cloud Computing Synopsis and Recommendations. [online] Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[11] NIST SP500-291 NIST Cloud Computing Standards Roadmap. [online] Available: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf

[12] Draft SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing. [online] Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[13] IEEE P2302 - Standard for Intercloud Interoperability and Federation (SIIF). [online] http://standards.ieee.org/develop/project/2302.html

[14] Leung, K. and Lee, Y. (2011). Content Distribution Network Interconnection (CDNI) Requirements. IETF draft, work in progress, draft-ietf-cdni-requirement-00.

[15] RFC3920 Extensible Messaging and Presence Protocol (XMPP): Core. [online] http://www.ietf.org/rfc/rfc3920.txt

[16] Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., Morrow, M., Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability. In Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on, 24-28 May 2009, Venice, Italy.

[17] J. D. Touch, Y.-S. Wang, L. Eggert, and G. G. Finn, "A virtual internet architecture," *ISI Technical Report*, Mar. 2003.

[18] R. Strijkers, M. Cristea, C. de Laat, and R. Meijer, "Application framework for programmable network control," Advances in Network-Embedded Management and Applications, pp. 37–52, 2011.

[19] Demchenko, Y., J. van der Ham, M. Ghijsen, M. Cristea, V. Yakovenko, C. de Laat, "On-Demand Provisioning of Cloud and Grid based Infrastructure Services for Collaborative Projects and Groups", The 2011 Intern. Conf. on Collaboration Technologies and Systems (CTS 2011), May 23-27, 2011, Philadelphia, Pennsylvania, USA

[20] Meijer, R. J., Strijkers, R. J., Gommans, L., and de Laat, C. (2006). User Programmable Virtualized Networks. In e-Science and Grid Computing, 2006. e-Science '06. Second IEEE International Conference on (p. 43).

[21] RFC 3945. Generalized Multi-Protocol Label Switching (GMPLS) Architecture. [online] http://www.ietf.org/rfc/rfc3945.txt

[22] D. Chappell, ENTERPRISE SERVICE BUS, O'Reilly, June 2004.

[23] OSGi Service Platform Release 4, Version 4.2. [online] Available: http://www.osgi.org/Download/Release4V42

[24] TMF Service Delivery Framework. [Online] http://www.tmforum.org /servicedeliveryframework/4664/home.html

[25] OWL 2 Web Ontology Language [online] Available: http://www.w3.org/TR/owl2-overview/

[26] J. van der Ham, F.Dijkstra, P.Grosso, R. van der Pol, A.Toonk, C. de Laat, "A distributed topology information system for optical networks based on the semantic web", Elsevier Journal on Optical Switching and Networking, Volume 5, Issues 2-3, June 2008, pp. 85-93

[27] Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG). [Online]. http://www.gridforum.org/gf/group_info/view.php?group=ISOD-RG