2012 IEEE 4th International Conference on Cloud Computing Technology and Science

Intercloud Architecture for Interoperability and Integration

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

Abstract—**This paper presents on-going research to develop the Intercloud Architecture Framework (ICAF) that addresses problems in multi-provider multi-domain heterogeneous cloud based infrastructure services and applications integration and interoperability. The paper refers to existing standards in Cloud Computing, in particular, recently published NIST Cloud Computing Reference Architecture (CCRA). The proposed ICAF defines four complementary components addressing Intercloud integration and interoperability: 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; Intercloud Control and Management Plane that supports cloud based applications interaction; Intercloud Federation Framework, and Intercloud Operation Framework. The paper briefly describes the architectural framework for cloud based infrastructure services provisioned on-demand being developed in the framework of the GEYSERS project that is used as a basis for building multilayer cloud services integration framework that allows optimized provisioning of both computing, storage and networking resources. The proposed architecture is intended to provide an architectural model for developing Intercloud middleware and in this way will facilitate clouds interoperability and integration.**

Keywords- Intercloud Architecture; Cloud Computing Reference Architecture; Multi-layer Cloud Services Model; Intercloud Control and Management Plane, Intercloud Federations Framework, Intercloud Operation Framework, Architectural framework for Cloud infrastructure services provisioned on-demand.

I. INTRODUCTION

Cloud Computing [1, 2] technologies are evolving as a common way to provide infrastructure services, resources virtualisation and on-demand provisioning. Cloud technologies bring applications and infrastructure services mobility and physical/hardware platform independency to the existing distributed computing and networking applications. The provisioned cloud based infrastructure services may involve multi-provider and multi-domain resources, including integration with the legacy services and infrastructures. In this way, clouds represent a new step in evolutional computing and communication technologies development chain by introducing a new type of services and a new abstraction layer for the general infrastructure services virtualisation to achieve distributed applications mobility. Current development of the cloud technologies demonstrates movement to developing Intercloud models, architectures and integration tools that could allow integrating cloud based infrastructure services into existing enterprise and campus infrastructures [3], on one hand, and provide common/interoperable environment for moving existing infrastructures and infrastructure services to virtualised cloud environment [4], on the other hand. More complex and enterprise oriented use of cloud infrastructure services will require developing new service provisioning and security models that could allow creating complex project and group oriented infrastructures provisioned on-demand and across multiple providers.

Cloud based applications operate as regular applications, in particular, using standard Internet protocols and platforms for services and applications interaction and management, however their composition and integration into distributed multi-provider cloud based infrastructure will require a number of functionalities and services that are jointly defined in this paper as Intercloud Architecture Framework.

This paper presents on-going research at the University of Amsterdam to develop the Intercloud Architecture Framework (ICAF) that intends to address problems with multi-domain heterogeneous cloud based applications integration and interoperability, including integration and interoperability with legacy IT (Information Technology) infrastructure services, and to facilitate interoperable and manageable inter-provider cloud infrastructures federation. The paper refers to the architectural framework for provisioning Cloud Infrastructure Services On-Demand [5] being developed by the authors as a result of cooperative efforts in a number of currently running projects such as GEANT3 [6] and GEYSERS [7], that provides a basis for defining the proposed Intercloud architecture. The presented paper significantly extends the research results initially presented as a poster paper at the IEEE CloudCom2011 Conference [8].

The remainder of the paper is organized as follows. Section II provides overview and analysis of the ongoing standardisation activities at NIST and IEEE that have a direct relation to and provide a basis for the proposed ICAF.

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

Section III describes a general use case of provisioning cloud based collaborative infrastructure that provides a motivation for defining ICAF, section IV summarises requirements and defines the main components of the proposed Intercloud Architecture. Section V describes the multi-layer Cloud Services Model, and section VI describes the main functionalities of other ICAF components. Section VII describes the abstract model for cloud based infrastructure services provisioning on-demand. Section VIII provides information about ongoing implementation of the ICAF components in the GEYSERS project. Related works are discussed in section IX, and the paper concludes with the future developments in section X.

II. CLOUD STANDARDISATION OVERVIEW

For the purpose of this paper, in this section we provide detailed analysis of the cloud related standards by National Institute of Standards and Technology (NIST) that define the Cloud Computing Reference Architecture (CCRA), IEEE standardisation activity to define Intercloud Interoperability and Federation framework, and also the ITU-T Focus Group on Cloud Computing (FG-Cloud) [9]. Suggestions are given how they can be used for the defining the general Intercloud architecture for interoperability and integration.

A group of standards that define internal cloud management, components design and communications are well presented by DMTF, SNIA and OGF standards that correspondingly define standards for Open Virtualisation Format (OVF) [10], Cloud Data Management Interface (CDMI) [11], and Open Cloud Computing Interface (OCCI) [12]. These standards are commonly accepted by industry and provide a basis for lower level cloud services interoperability; they can be directly incorporated into the proposed ICAF.

A. *NIST Cloud Computing related standards*

Since the first publication of the currently commonly accepted NIST Cloud definition in 2008, NIST is leading an internationally recognized activity on defining conceptual and standard base in Cloud Computing, which has resulted in the following documents that create a solid base for cloud services development and offering:

- NIST SP 800-145, A NIST definition of cloud computing [1]
- NIST SP 500-292, Cloud Computing Reference Architecture, v1.0 [2]
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations [13]. This recently published document provides a good overview of the basic usage scenarios in clouds, analysis of open issues and recommendations for cloud systems to comply with the general requirements to critical IT systems.

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.

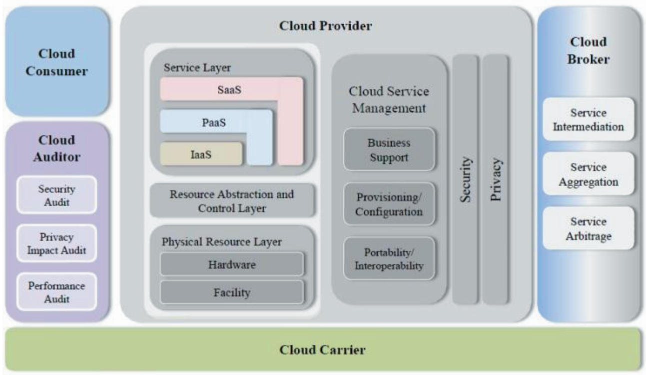

Figure 1. NIST Cloud Computing Reference Architecture (CCRA) [2]

The CCRA is suitable for many purposes where network performance is not critical but needs to be extended with explicit network services provisioning and management functions when the cloud applications are critical to network Quality of Services (QoS), in particular latency, like in case of enterprise applications, business transactions, crisis management, etc.

Despite the fact that CCRA includes Cloud Carrier as representing a typical role of the telecom operators that can provide network connectivity as a 3rd party service, there is no well-defined service model how this can be done.

The proposed in this paper ICAF uses NIST CCRA as the commonly accepted basis and defines additional functionalities that are required by heterogeneous multi-provider Intercloud services integration and interoperability, in particular, to address Intercloud network infrastructure provisioning with the optimally defined topology and guaranteed QoS. More detailed analysis of the CCRA limitations in relation to infrastructure services provisioning is provided in [14].

B. *IEEE Intercloud Working Group (IEEE P2302)*

IEEE P2302 Intercloud Working Group recently published a draft Standard on Intercloud Interoperability and Federation (SIIF) [15] that proposes 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

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

elements include registration, geo-independence, trust anchor, and potentially compliance and audit.

The proposed IEEE P2302 SIIF architecture is 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 Intercloud integration and interoperability. The document also proposes to use an approach similar to the Content Distribution Network Interconnection (CDNI) [17] but this doesn't address the generic problems with interoperability and integration of the heterogeneous multi-domain and multi-provider cloud based infrastructure.

The limitation of the proposed by IEEE P2302 architecture and approach is that it tries to closely imitate the Internet approach in building hierarchical interconnected infrastructure by adding an additional Intercloud layer to support Intercloud communications at networking and messaging levels without addressing specific problems in Intercloud integration, management and operation.

C. *ITU-T Cloud Network Infrastructure Model*

As a result of its chartered operation in 2010-2011, the FG-Cloud published the Technical Report (Part 1 to 7) **Error! Reference source not found.**that presents taxonomies, use cases, functional, cloud infrastructure and reference architecture definition, cloud security. The report also analyses the cloud technology benefits from telecommunication perspectives and discusses scenarios with inter-cloud peering, federation and brokering.

The document "Part 2: Functional requirements and reference architecture" defines the layered Cloud computing architecture that includes the following layers:

- Resources and network layer (including physical resources, pooling and orchestration, pooling and virtualisation)
- Cloud services layer (including basic cloud services IaaS, PaaS, SaaS and also Orchestration service)
- Access layer (including endpoint functions and inter-cloud functions,) where the role of network service providers is defined as to provide inter-cloud transport network
- User layer (including user functions, partner functions, administration functions).

The document "Part 3: Requirements and framework architecture of cloud infrastructure" provides well-defined general requirements to cloud infrastructure from the point of view of the telecom providers. The proposed cloud infrastructure definition is based on the convergence principle recently adopted by telecom industry that uses "one wire" concept for convergence of service traffic, storage traffic, backup traffic, and management traffic.

The document proposes the model for cloud network infrastructure that includes core transport network, intra-cloud network, and intercloud network. Issues related to network interface cards (NIC) virtualisation and virtual machines migration are discussed. The document provides suggestions for cloud network topology design and definition of the virtualised network components such as cloud switch and cloud routes.

III. General Use Cases for ICAF

The following basic use cases for Intercloud Architecture are considered: (1) Enterprise IT infrastructure migration to cloud and evolution that will require both integration of the legacy infrastructure and cloud based components, and move from general cloud infrastructure services to specialised private cloud platform services; (2) large project-oriented scientific infrastructures (capable of handling big data) including dedicated transport network infrastructure that need to be provisioned on-demand [18]; (3) IT infrastructure disaster recovery that requires not only data backup but also the whole supporting infrastructure restoration/setup on possibly new computer/cloud software or hardware platform.

The networking research area itself introduces another use case for wide spread "cloud+network" infrastructure to support small and medium scientific experiments for testing new protocols and network dynamics that are too small for super computers but too big for desktop systems. All use 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.

Figure 2 illustrates the typical e-Science or enterprise collaborative 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 and typically residing in real or virtual campuses.

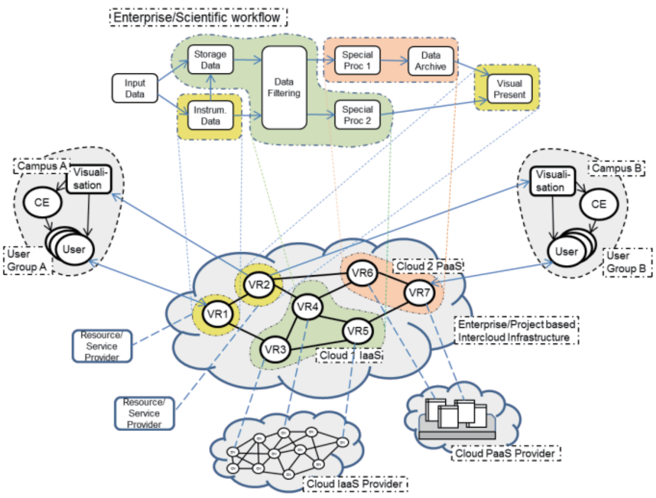

Figure 2. Enterprise or project oriented collaborative cloud based infrastructure.

The main goal of the enterprise or scientific infrastructures is to support the enterprise or scientific workflows and operational procedures related to processes monitoring and data processing. Cloud technologies allow

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

to simplify building such infrastructures and provision them on-demand. Figure 2 illustrates how an example enterprise or scientific workflow can be mapped to cloud based services and next deployed and operated as an instant Intercloud infrastructure. It contains cloud infrastructure segments IaaS (VR3-VR5) and PaaS (VR6, VR7), separate virtualised resources or services (VR1, VR2), two interacting campuses A and B, and interconnecting them network infrastructure that in many cases may need to use dedicated network links for guaranteed performance.

Efficient operation of such infrastructure will require both overall infrastructure management and individual services and infrastructure segments to interact between themselves. This task is typically out of scope of existing cloud service models and is intended to be addressed by the proposed Intercloud Architecture.

IV. ICAF REQUIREMENTS AND DEFINITION

The proposed Intercloud 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 and e-Science infrastructures and applications, including integration and interoperability with legacy campus/enterprise infrastructure.

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

- ICAF should support communication between cloud applications and services belonging to different service layers (vertical integration), between cloud domains and heterogeneous platforms (horizontal integration).
  - Be compatible and provide multi-layer integration of existing cloud service models – IaaS, PaaS, SaaS and Apps clouds
- ICAF should provide a possibility that applications can control infrastructure and related supporting services at different service layers to achieve run-time optimization (Intercloud control and management functions).
  - Common Intercloud Control Plane and signaling for better cloud services and network integration
- ICAF 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.
- Explicit/guaranteed intra- and inter-cloud network infrastructure provisioning (e.g., delivered as Network as a Service (NaaS) service model)
- Provide a framework for heterogeneous inter-cloud federation
- Facilitate interoperable and measurable intra-provider infrastructures
- Support existing cloud provider operational and business models and provide a basis for new forms of infrastructure services provisioning and operation (e.g., cloud carrier or cloud operator).

The proposed ICAF should use the rich experience of the Grid and Internet community and where possible use the tested by practice architecture patterns from Internet, SOA and Grid/OGSA, in particular, support Virtual Organisations (VO) infrastructure federation mechanisms widely used by e-Science/Grid community.

Based on the above requirements, we define the following complementary components of the proposed Intercloud Architecture:

(1) Multilayer Cloud Services Model (CSM) for vertical cloud services interaction, integration and compatibility that defines both relations between cloud service models (such as IaaS, PaaS, SaaS) and other required functional layers and components of the general cloud based services infrastructure;

(2) Intercloud 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) Intercloud 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 necessary gateway or federation services;

(4) Intercloud Operation Framework (ICOF) which includes functionalities to support multi-provider infrastructure operation, including business workflow, SLA management, accounting. ICOF defines the basic roles, actors and their relations in sense of resources operation, management and ownership. ICOF requires support from and interacts with both ICCMP and ICFF.

At this stage of research, we define in details only multi-layer Cloud Services Model that provides a basis for all other functional components and protocols definition and can be built using modern SOA technologies to support basic cloud service models. We also define the main functional components and suggest interfaces for ICCMP, ICFF and ICOF that are currently been defined for integrated IaaS infrastructure services provisioning on-demand as it is being implemented in the projects where the authors are involved. Future ICAF development will follow the implementation results in these projects to define all other components.

V. MULTI-LAYER CLOUD SERVICES MODEL (CSM)

Figure 3 illustrates the CSM layers definition and related functional components in a typical cloud infrastructure. It shows that the basic cloud service models IaaS, PaaS, SaaS that expose in most cases standard based interfaces to user services or applications, but actually use proprietary interfaces to the physical provider platform. In this respect the proposed model can be used for the inter-layer interfaces definition.

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

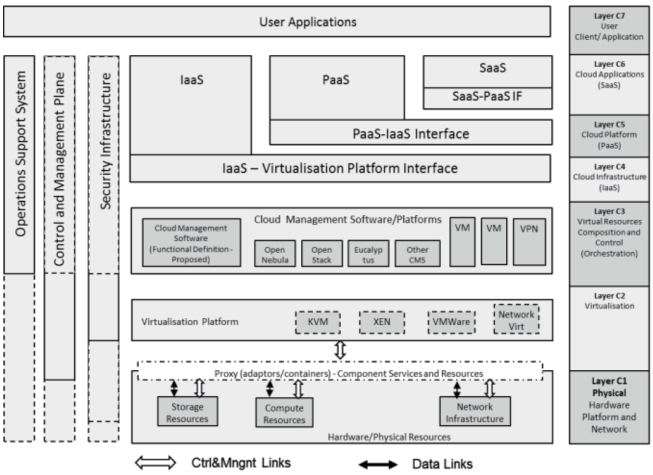

Figure 3. Reference Multilayer Cloud Services Model (CSM).

In the proposed Intercloud layered service model the following layers are defined including user client or application at the top (numbering from bottom up, see Fig. 3):

(C7) User client or application

(C6) SaaS (or cloud applications) as a top cloud layer that represents cloud applications

(C5) PaaS provided as a service or used as a platform for hosting cloud applications

(C4) IaaS provided as infrastructure or used for hosting cloud platforms or applications

(C3) Cloud virtual resources composition and orchestration layer that is represented by the Cloud Management Software (such as OpenNebula, OpenStack, or others)

(C2) Cloud virtualisation layer (e.g. represented by VMware, Xen or KVM as virtualisation platforms)

(C1) Physical platform (PC hardware, network, and network infrastructure).

Note. Layer acronyms use prefix "C" to denote their relation to clouds.

The three vertical planes or cross-layer infrastructures are defined to group related functionality in all CSM layers:

- Control and Management Plane
- Operations Support System
- Security Infrastructure.

VI. ICAF COMPONENTS

A. *Intercloud Control and Management Plane (ICCMP)*

Figure 4 illustrates a scenario where two different cloud/segments domain IaaS and PaaS need to interact allowing applications from one domain to control underlying virtualised resources and infrastructure in another domain. Upper layer interfaces are typically standardised and can use e.g. OCCI interface, while lower layer interfaces controlling internal provider virtualised and physical resources may be non-standard or proprietary. The role of ICCMP is to provide logical and functional interface between different cloud service layers running in different cloud domains. This provides another motivation for the standardisation of such interlayer interfaces; otherwise they can be implemented as part of user applications.

ICCMP supports Intercloud signalling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds.

The main functional components include

- Cloud Resource Manager
- Network Infrastructure Manager
- Virtual Infrastructure composition and orchestration
- Services and infrastructure lifecycle management (that can be also a part of the composition and orchestration layer).

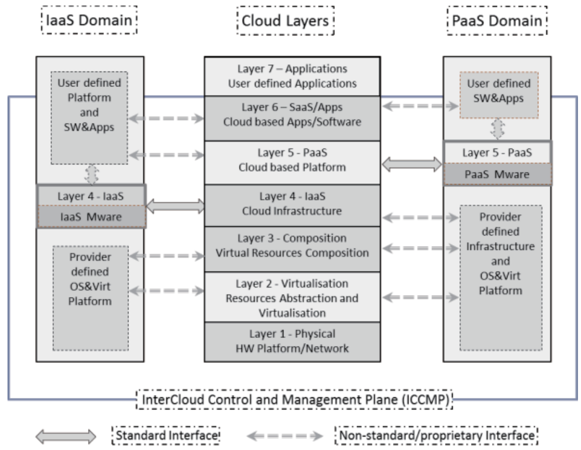

Figure 4. Example of the IaaS and PaaS cloud domains communication that uses standard interfaces and proprietary interfaces

The ICCMP Interfaces should support the following functionalities:

- Inter-/cross-layer control and signalling
- Monitoring
- Location service
- Topology aware infrastructure management
- Configuration and protocols management.

Based on the GEYSERS project implementation (see section VIII) we can suggest the GMPLS [19] as an appropriate technology for building ICCMP control plane that allows network infrastructure optimisation for the required compute and storage resources assigned to network nodes [20]. However, management functionalities will require development of new interfaces.

B. *Intercloud Federation Framework (ICFF)*

Figure 5 illustrates the main components of the federated Intercloud Architecture, specifically underlying the Intercloud gateway function (GW) that provides translation of the requests, protocols and data formats between cloud domains.

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

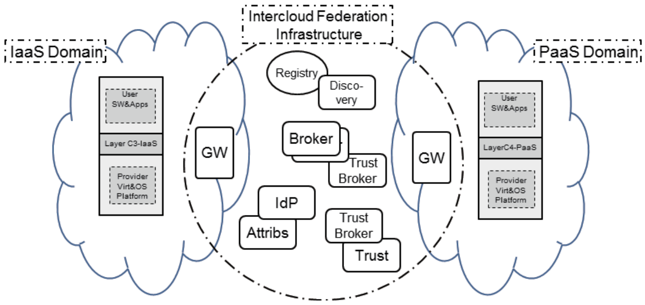

Figure 5. ICFF components

At the same time the federated inter-cloud infrastructure requires a number of functionalities, protocols and interfaces to support its operation:

- Trust and service brokers
- Service Registry
- Service Discovery
- Identity provider (IdP)
- Trust manager/router
- Attribute/namespace resolver
- Intercloud gateway and/or attribute/namespace translator.

Correspondingly, the ICFF Interfaces should support the following functionalities:

- Naming, Addressing and Translation (if/as needed)
- Publishing
- Discovery
- Attributes management
- Trust/key management

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 [21, 22, 23].

C. Intercloud Operation Framework (ICOF)

ICOF defines the main roles and actors based on the RORA model: Resource, Ownership, Role, Action, - proposed in the GEYSERS project [20]. This should provide a basis for business processes definition, SLA management and access control policy definition as well as broker and federation operation.

The main functional components include:

- Service Broker
- Service Registry
- Cloud Service Provider, Cloud Operator, Cloud (physical) Resource provider, Cloud Carrier

Suggested ICOF interfaces should support the following functionalities:

- Service Provisioning, Deployment, Decommissioning (or Termination)
- SLA management and negotiation
- Services Lifecycle and metadata management

The ICOF definition will leverage the TeleManagement Forum (TMF) standards related to eTOM and Operational Support Systems [24], Service Delivery Framework (SDF) [25]. ICOF will also evaluate an approach for market-oriented allocation of resources in clouds [26].

VII. Abstract Model for Cloud Based Infrastructure Services Provisioning

Figure 6 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 are 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 depictured on the left side of the picture and include 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 and actually implements the proposed by authors Composable Services Architecture (CSA) [27].

The infrastructure provisioning process, also referred to as Service Delivery Framework (SDF), is adopted from the TeleManagement Forum SDF [25] with necessary extensions to allow dynamic services provisioning and modification. 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 needs 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.

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

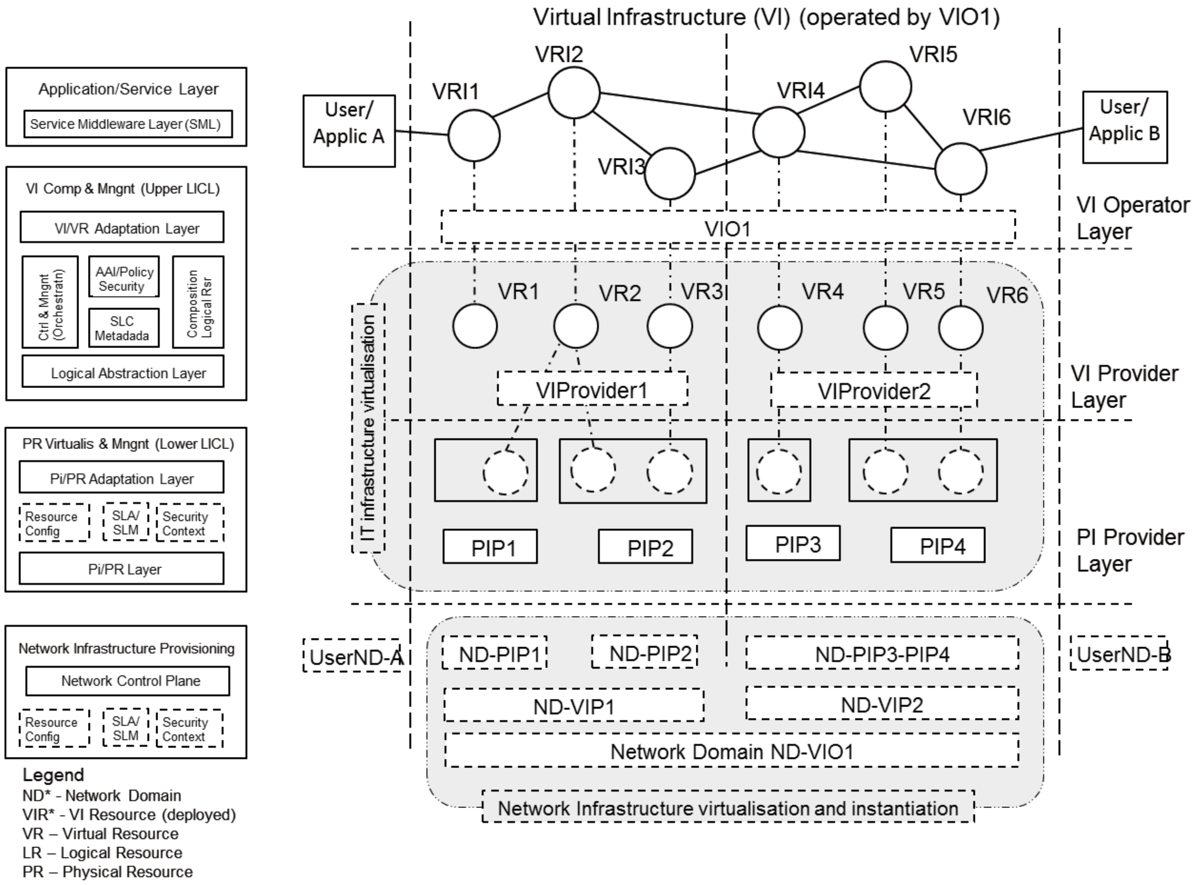

Figure 6. Main actors, functional layers and processes in on-demand infrastructure services provisioning

The infrastructure services virtualisation and composition is defined by the Infrastructure Services Modeling Framework (ISMF) described in the previous authors' work [18].

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 CSM Virtualisation and Composition layers 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.

VIII. Implementation Status and Suggestions

The GEYSERS project develops and implements an original model and architecture for the general infrastructure services virtualisation (including active network components) and provisioning optimized Network+IT infrastructure on-demand. The proposed architecture and solution include such components as (see figure 7): Logical Infrastructure Composition Layer (LICL) for infrastructure services (Network+IT) virtualisation and provisioning; enhanced Network Control Plane (NCP+) for controlling instant virtual infrastructure domains; Service Middleware Layer (SML) that actually represents the Application Layer in CSM. The project also defined an operational framework for combined network and IT services provisioning (including planning and re-planning), monitoring, SLA and services lifecycle management [20].

Figure 7 illustrates the interfaces defined in the GEYSERS architecture:

MLI - Management to LICL Interface
SLI - SML to LICL interface
NIPS UNI - NCP to LICL interface
CCI - Connection Controller Interface
LPI - LICL to PHY interface
CSSI - Common Security Service Interface.

Functional elements/layers and interfaces defined in GEYSERS project are directly mapped to the functional components and interfaces defined in the CMS, ICCMP and ICOF of the ICAF. As a part of its security architecture the project also defined the Common Security Services Interface (CSSI) and the security infrastructure for dynamically provisioned virtualised security services [28].

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

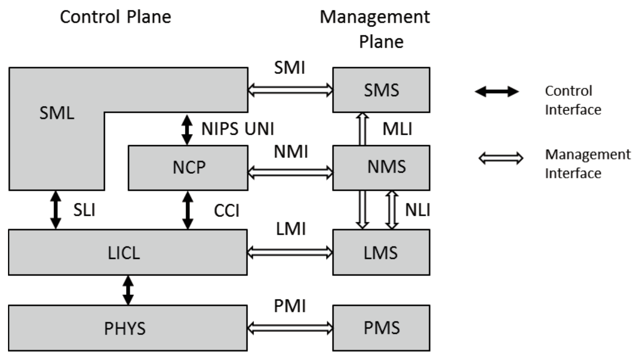

Figure 7. GEYSERS control and management architecture and interfaces.

IX. RELATED WORKS

There are not many academic researches on cloud architecture. Most of researches are focused on analysis and improvement of the general cloud architecture that is defined by NIST CCRA [2]. A few works [29-32] are trying to apply more conceptual approach to defining cloud based infrastructure services, but their scope is rather focused on one or another specific problem. Paper [29] proposes the Cloud Computing Open Architecture (CCOA) based on SOA and virtualisation and derives ten interconnected architectural models, but it doesn't go further with suggesting implementation. The position paper [30] explores an approach to describe the Intercloud operations based on the New Generation Service Overlay Network (NGSON) but the proposed solutions are rather focused on the content delivery overlay networks. Paper [31] describes the GridARS system that can provision heterogeneous performance assured virtual infrastructure over Intercloud environment, however the proposed solution is primarily focused on the optimal VM deployment and lower level underlying network communication. Paper [32] presented by Alcatel-Lucent Bell Labs provides interesting point of view of the telecom industry on adoption of cloud technologies to building cloud based telecom infrastructures what confirms the clouds potentiality to provide a basis for the complex infrastructures virtualisation and infrastructure services mobility and on-demand provisioning.

Industry research and development are mostly focused on adopting the NIST CCRA to their business practices and platforms. Good example here is the IBM Cloud Computing Reference Architecture 2.0 [33] that provides a lot of useful detail on CCRA implementation, interfaces and programming models with the IBM tools and platforms.

X. CONLUSION AND FUTURE DEVELOPMENTS

This paper presents on-going research at the University of Amsterdam to develop the Intercloud Architecture that addresses problems with multi-domain heterogeneous cloud based applications integration and inter-provider and inter-platform interoperability.

The proposed high level architecture is based on the development and implementation of its different components in a few cooperating projects such as GEYSERS, GEANT, MANTICHORE and NOVI, which experience demonstrated needs for more general approach to complex multi-provider cloud based infrastructure services.

The proposed Intercloud Architecture Framework includes the four inter-related components that address different issues in heterogeneous multi-provider, multi-cloud, multi-platforms 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; Intercloud Control and Management Plane that supports cloud based applications and infrastructure services interaction; Intercloud Federation Framework that defines infrastructure components for independent cloud domains federation; and Intercloud Operation Framework that defines functional components and procedures to support cloud based services provisioning and operation.

The proposed approach and definitions are intended to provide a consolidation basis for numerous standardisation activities in the area of Intercloud architectures by splitting concerns and using already existing and widely accepted solution where possible.

The authors are actively contributing to a number of standardisation bodies, in particular, the Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) [34], IETF on Cloud Architecture Framework definition [35]

ACKNOWLEDGEMENTS

This work is supported by the FP7 EU funded Integrated projects The Generalized Architecture for Dynamic Infrastructure Services (GEYSERS, FP7-ICT-248657), GEANT3 (FP7-ICT-238875) and by the Dutch national program COMMIT.

REFERENCES

[1] NIST SP 800-145, "A NIST definition of cloud computing", [online] 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] Rajkumar Buyya, Rajiv Ranjan, Rodrigo N. Calheiros, InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2010, Busan, South Korea, May 21-23, 2010), LNCS, Springer, Germany, 2010.

[4] Varia, J., Migrating your Existing Applications to the AWS Cloud. A Phase-driven Approach to Cloud Migration, October 2010. [Online] http://d36cz9buwru1tt.cloudfront.net/CloudMigration-main.pdf

[5] Generic Architecture for Cloud Infrastructure as a Service (IaaS) Provisioning Model. 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

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

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

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

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

[9] FG Cloud Technical Report (Part 1 to 7). [online] http://www.itu.int/en/ITU-T/focusgroups/cloud/Documents/FG-coud-technical-report.zip

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

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

[12] GFD.183 Open Cloud Computing Interface - Core [online] http://www.ogf.org/documents/GFD.183.pdf

[13] NIST SP 800-146, Cloud Computing Synopsis and Recommendations. May 2012 [online] Available: http://www.thecre.com/fisma/wp-content/uploads/2012/05/sp800-146.pdf

[14] On-Demand Infrastructure Services Provisioning Best Practices. ISOD-RG Draft Version 04,[online] draft-isod-bcp-infrastructure-v04.docx

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

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

[18] 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 International Conference on Collaboration Technologies and Systems (CTS 2011), May 23-27, 2011, Philadelphia, USA

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

[20] GEYSERS Project Deliverable 2.2 (update): GEYSERS overall architecture & interfaces specification and service provisioning workflow. [online] http://wiki.geysers.eu/images/5/55/Geysers-deliverable_2.2_update_final.pdf

[21] Defining Federated Cloud Ecosystems. Blog post by Krishnan Subramanian on October 6, 2011. [online] http://www.cloudave.com/15323/defining-federated-cloud-ecosystems/

[22] Federated Network Architectures. GEANT3 Project. [online] http://www.geant.net/Research/Future_Network_Research/Pages/FederatedNetworkArchitectures.aspx

[23] OASIS IDCloud TC, "OASIS Identity in the Cloud TC." [Online]. Available: http://wiki.oasis-open.org/id-cloud/.

[24] Draft, March 25, 2012. [online] http://www.ietf.org/id/draft-howlett-abfab-trust-router-ps-02.txtTM Forum Frameworx. http://www.tmforum.org/frameworx/1911/home.html

[25] TR139, Service Delivery Framework (SDF) Overview, Release 2.0. http://www.tmforum.org/TechnicalReports/TR139ServiceDelivery/34303/article.html

[26] R. Buyya, C.S. Yeo, S. Venugopal: Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. HPCC 2008: 5-13

[27] Demchenko, Y., C. Ngo, P. Martнnez-Julia, E. Torroglosa, M. Grammatikou, J. Jofre, S. Gheorghiu, J.A. Garcia-Espin, A.D. Perez-Morales, C. de Laat, GEMBus based Services Composition Platform for Cloud PaaS. The European Conference on Service-Oriented and Cloud Computing (ESOCC2012), 19-21 September, 2012, Bertinoro, Italy. (Accepted paper).

[28] Ngo, C., P.Membrey, Y.Demchenko, C. de Laat, Security Framework for Virtualised Infrastructure Services Provisioned On-demand. Proc. 3rd IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2011), 29 November - 1 December 2011, Athens, Greece. ISBN: 978-0-7695-4622-3

[29] Zhang, Liang-Jie, Qun Zhou, CCOA: Cloud Computing Open Architecture, Proc. IEEE International Conference on Web Services (ICWS2009), 6-10 July 2009. ISBN: 978-0-7695-3709-2

[30] Shan, C., C.Heng, Z.Xianjun, Inter-Cloud Operations via NGSON, IEEE Communications Magazine, Volume 50, Issue 1, January 2012

[31] Takefusa, A., H.Nakada, R.Takano, T.Kudoh,Y.Tanaka, GridARS: A Grid Advanced Resource Management System Framework for Intercloud, Proc. 3rd IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2011), 29 Nov - 1 Dec 2011, Athens, Greece.

[32] Bosch, P., A.Duminuco, F.Pianese,T.L.Wood, Telco Clouds and Virtual Telco: Consolidation, Convergance, and Beyond, Proc. Symposium on Integrated Network Management, 2011 IFIP/IEEE, 23-27 May 2011.

[33] Cloud Computing Reference Architecture 2.0, IBM CC RA team. [online]https://share.confex.com/share/117/webprogram/Handout/Session9261/CCRA_2.0.pdf

[34] 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

[35] Cloud Reference Framework. Internet-Draft, version 0.3, June 27, 2012. [online] http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-03.txt

978-1-4673-4510-1/12/$31.00 ©2012 IEEE