Intercloud Architecture Framework for Heterogeneous Multi-Provider Cloud based Infrastructure Services Provisioning

[1]Yuri Demchenko, [1,2]Marc X. Makkes, [1,2]Rudolf Strijkers, [1]Canh Ngo, [1]Cees de Laat

[1] University of Amsterdam, the Netherlands

[2] TNO, the Netherlands

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 (CSM) that combines commonly adopted cloud service models, such as IaaS, PaaS, SaaS, in one multilayer model with corresponding inter-layer interfaces including also access and delivery infrastructure layer; Intercloud Control and Management Plane (ICCMP) that supports cloud based applications interaction; Intercloud Federation Framework (ICFF), and Intercloud Operation Framework (ICOF). The paper provides general definition of the ICFF, its generic components and interfaces. 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 provides a basis for CSM and ICCMP implementation allowing optimized provisioning of 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: 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

1. INTRODUCTION

Cloud Computing [NIST SP 800-145 ; NIST SP 500-292] 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 [Buyya et al. 2010], on one hand, and provide common/interoperable environment for moving existing infrastructures and infrastructure services to virtualised cloud environment [Varia 2010], 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.

This research 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.

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 [SNE-IaaS 2011] being developed by the authors as a result of cooperative efforts in a number of currently running projects such as GEANT3 [GEANT] and GEYSERS [GEYSERS], that provides a basis for defining the proposed Intercloud architecture. The presented paper updates and significantly extends the research results initially presented at the IEEE CloudCom2012 Conference [Demchenko et al. 2012].

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. 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, section VI describes the ICCMP and ICOF components, and section VII provides definition and describes the main functionalities of the ICFF component. Section VIII describes the basic use cases for cloud/intercloud federation and the main functional components of the ICFF. Section IX describes the abstract model for the cloud based infrastructure services provisioning on-demand. Section X provides information about ongoing ICAF implementation in the GEYSERS project. Related works are discussed in section XI, and the paper concludes with the future developments in section XII.

2. CLOUD STANDARDIZATION 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) [ITU-T Cloud]. 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) [DMTF OVF], Cloud Data Management Interface (CDMI) [SNIA CDMI], and Open Cloud Computing Interface (OCCI) [GFD.183]. 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.

2.1 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 [NIST SP 800-145]
- NIST SP 500-292, Cloud Computing Reference Architecture, v1.0 [NIST SP 500-292]

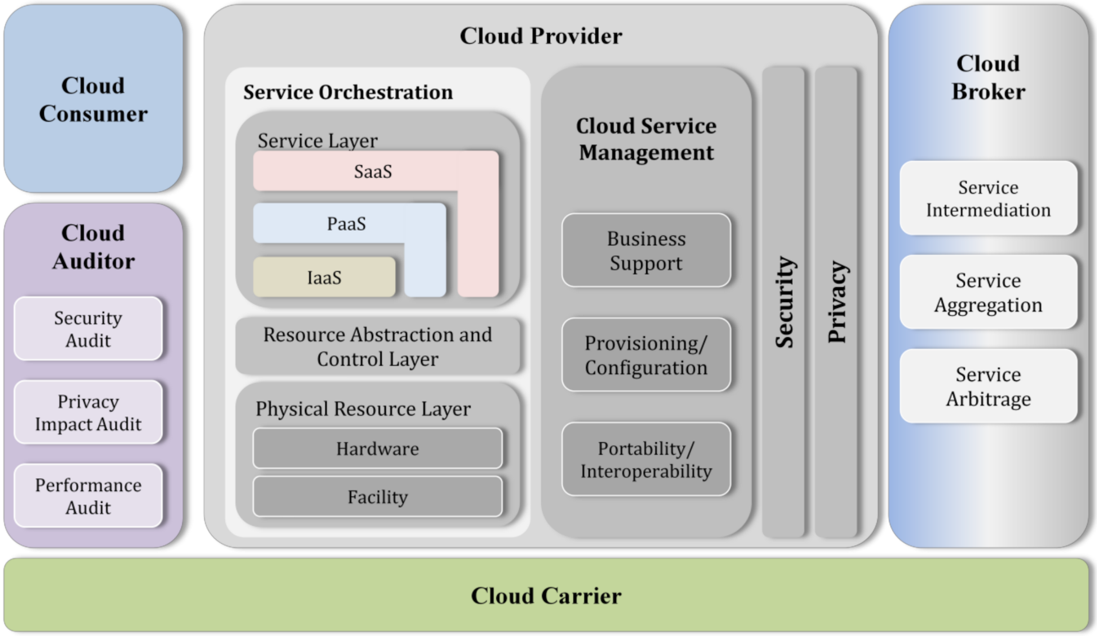

Figure 1. NIST Cloud Computing Reference Architecture (CCRA)

- NIST SP 800-146, Cloud Computing Synopsis and Recommendations [NIST SP 800-146 2012]. 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.

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 [ISOD BCP].

2.2 IEEE Intercloud Working Group (IEEE P2302)

IEEE P2302 Intercloud Working Group recently published a draft Standard on Intercloud Interoperability and Federation (SIIF) [IEEE P2302] 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 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 [Bernstein et al. 2009] 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) [Leung and Lee 2011] but this doesnt 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.

2.3 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) [ITU-T Cloud] 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.

3. 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 the integration of the legacy infrastructure with cloud based components, as a first step, and in the second stage progressive transfer from general cloud infrastructure services to specialised private cloud platform services;

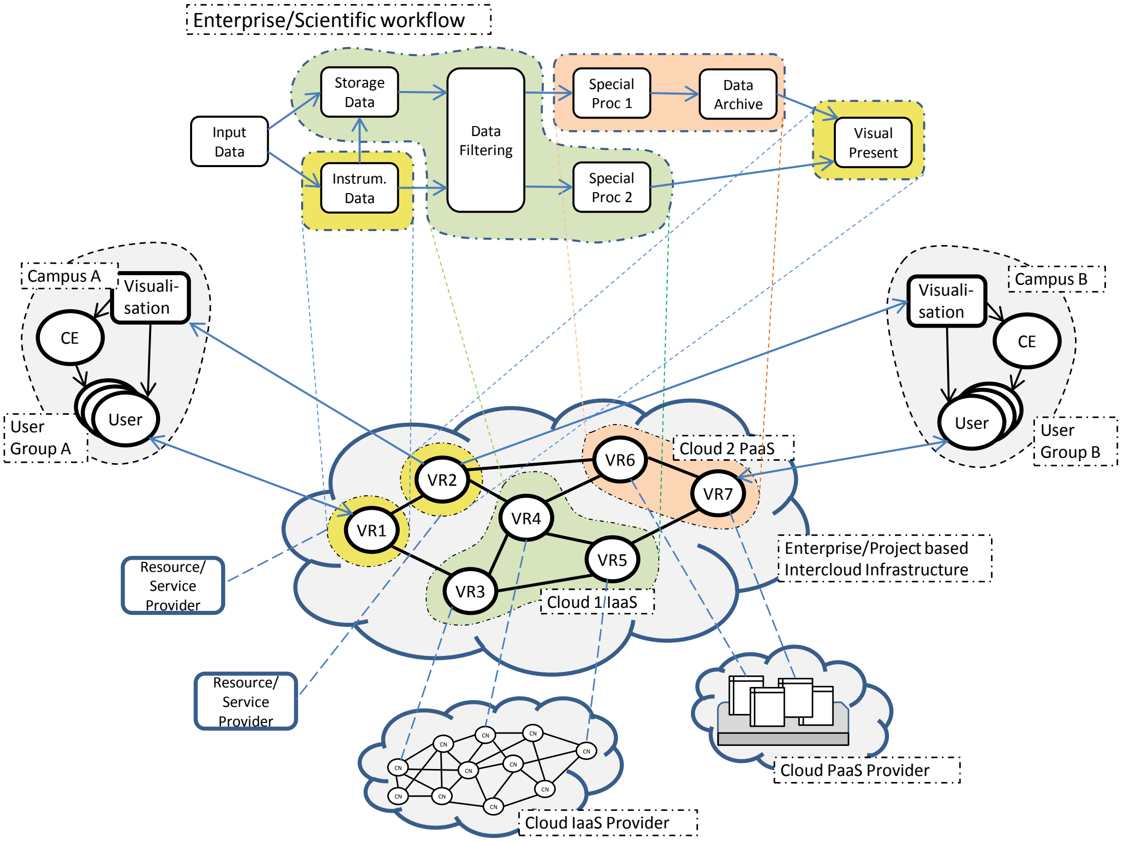

Figure 2. Enterprise or project oriented collaborative cloud based infrastructure

(2) Large project-oriented scientific infrastructures (capable of handling big data) including dedicated transport network infrastructure that need to be provisioned on-demand [TMFFwx];

(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.

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. This is actually based on the resources and services virtualization provided by the cloud technologies.

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

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 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.

4. 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 life-cycle 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.

The proposed Intercloud Architecture Framework includes the following components that separate all functions related the cloud services design, control, management and operations into orthogonal groups:

(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, including also the Access and Delivery Infrastructure layer that interconnects cloud provider datacenter or Point of Presence (POP) and customer/user location and infrastructure.

(2) **Intercloud Control and Management Plane (ICCMP)** for Intercloud 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 and 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;

(5) **Intercloud Security Framework (ICSF)** that provides a basis for secure operation of all components of the Intercloud infrastructure, including secure operation of the cloud federations. In this respect ICSF should provide a basis for integration of the security services between different CSM layers and all participating cloud service providers.

At this stage of research, we define in details multi-layer Cloud Services Model that provides a basis for all other functional components and protocols definition and Intercloud Federation Framework that are discussed in details below. We also define the main functional components and suggested interfaces for ICCMP and ICOF that are currently being developed for integrated IaaS infrastructure services provisioning on-demand and 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.

5. 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. In the proposed CSM the following layers are defined including user client or application at the top (numbering from bottom up, see Fig. 4):

(C6) User/customer side resources and services located in and provided by the customers enterprise or campus network to support their integration with the cloud based infrastructure; these may include identity management, infrastructure administration, data services and visualization.

(C5) Access/Delivery infrastructure hosting components and functions to provide access to cloud services/resources and interconnect multiple cloud domains; cloud federation services are located at this layer.

(C4) Cloud services layer that may include different type of cloud services IaaS, PaaS, SaaS that are exposed to upper customer faced layer via standard interfaces while potentially using non-standard internal and lower facing interfaces.

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

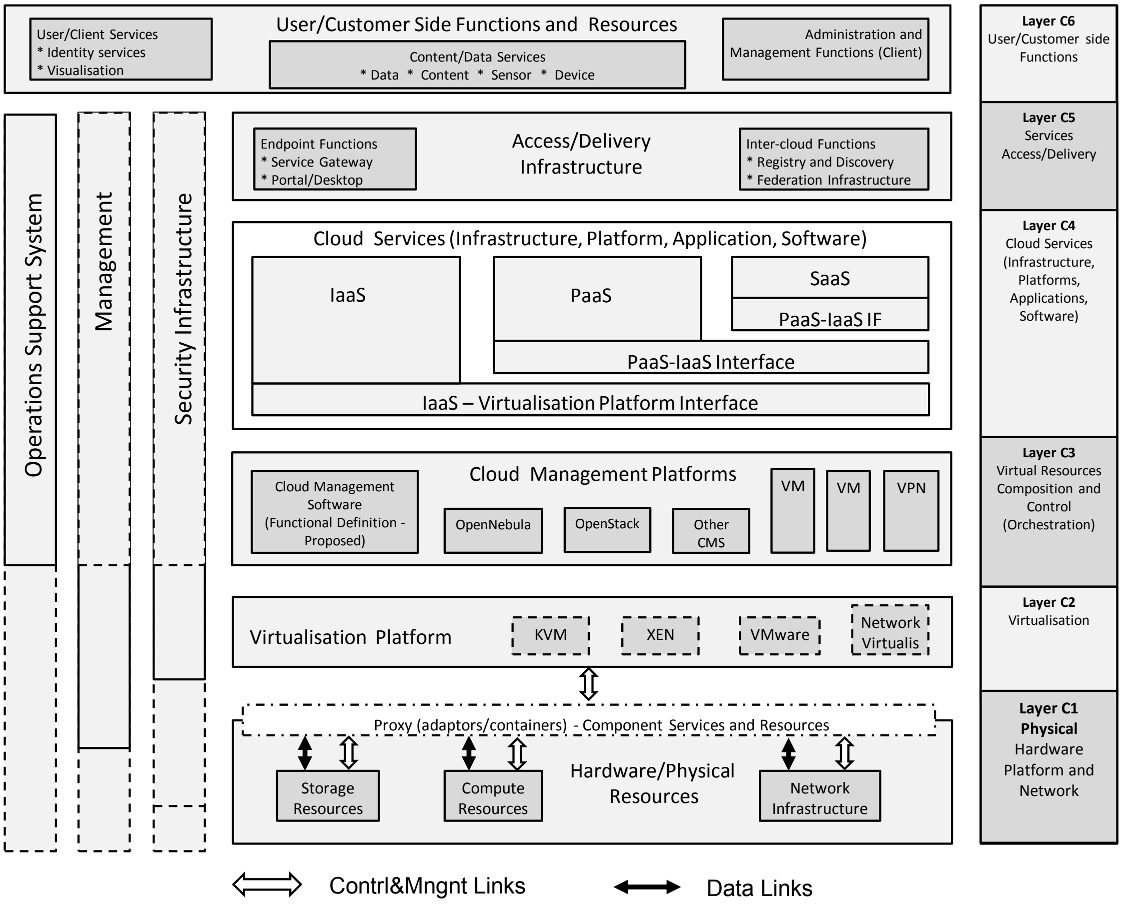
User/Customer Side Functions and Resources
User/Client Services
* Identity services
* Visualisation
Content/Data Services
* Data * Content * Sensor * Device
Administration and Management Functions (Client)
Layer C6
User/Customer side Functions
Operations Support System
Management
Security Infrastructure
Access/Delivery Infrastructure
Endpoint Functions
* Service Gateway
* Portal/Desktop
Inter-cloud Functions
* Registry and Discovery
* Federation Infrastructure
Layer C5
Services Access/Delivery
Cloud Services (Infrastructure, Platform, Application, Software)
IaaS
PaaS
SaaS
PaaS-IaaS IF
PaaS-IaaS Interface
IaaS – Virtualisation Platform Interface
Layer C4
Cloud Services (Infrastructure, Platforms, Applications, Software)
Cloud Management Platforms
Cloud Management Software (Functional Definition - Proposed)
OpenNebula
OpenStack
Other CMS
VM
VM
VPN
Layer C3
Virtual Resources Composition and Control (Orchestration)
Virtualisation Platform
KVM
XEN
VMware
Network Virtualis
Layer C2
Virtualisation
Proxy (adaptors/containers) - Component Services and Resources
Storage Resources
Compute Resources
Hardware/Physical Resources
Network Infrastructure
Layer C1
Physical
Hardware Platform and Network
Contrl&Mngnt Links
Data Links

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

ers) and may include additional services for combined inter-cloud infrastructure composition and orchestration.

(C2) Cloud virtualisation layer (e.g. represented by VMware, Xen or KVM as virtualisation platforms; or using custom virtualisation platform for non-computer resources).

(C1) Physical platform (PC hardware, storage, network, and network infrastructure); to interface with the virtualisation layer the physical resources layer may provide special adaptors functionality.

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 which functionality is defined by Intercloud Control and Management Plane.
- Operations Support System represented by Intercloud Operations Framework.
- Security Infrastructure that is defined in as Intercloud Security Framework.

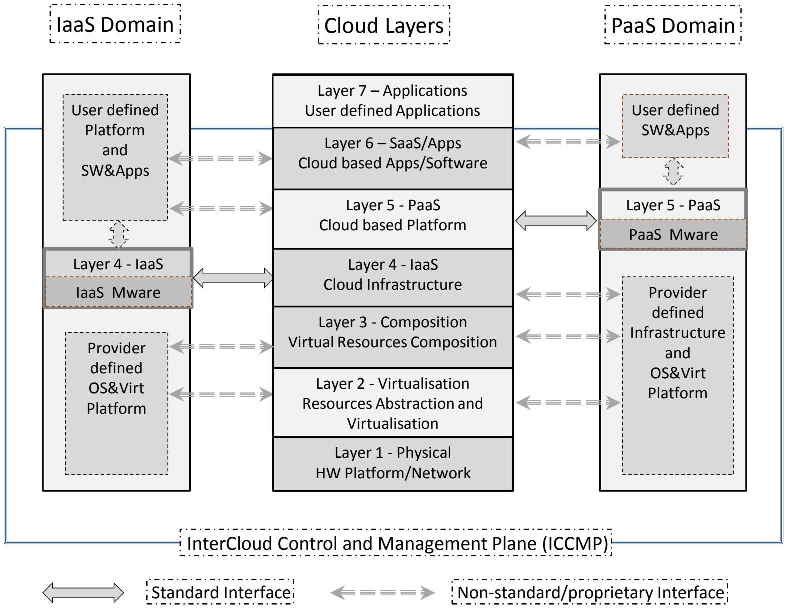
IaaS Domain
Cloud Layers
PaaS Domain
User defined Platform and SW&Apps
Layer 4 - IaaS
IaaS Mware
Provider defined OS&Virt Platform
Layer 7 – Applications User defined Applications
Layer 6 – SaaS/Apps Cloud based Apps/Software
Layer 5 - PaaS Cloud based Platform
Layer 4 - IaaS Cloud Infrastructure
Layer 3 - Composition Virtual Resources Composition
Layer 2 - Virtualisation Resources Abstraction and Virtualisation
Layer 1 - Physical HW Platform/Network
User defined SW&Apps
Layer 5 - PaaS
PaaS Mware
Provider defined Infrastructure and OS&Virt Platform
InterCloud Control and Management Plane (ICCMP)
Standard Interface
Non-standard/proprietary Interface

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

6. ICAF COMPONENTS

6.1 Intercloud Control and Management Plane(ICCMP)

Figure 4 illustrates a scenario where two different cloud segments/domains 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).

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 X) we can suggest the GMPLS [RFC3945] 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 [GEYSERS D2.2]. However, management functionalities will require development of new interfaces.

6.2 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 [GEYSERS D2.2]. 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 [TMFFwx], Service Delivery Framework (SDF) [TR139]. ICOF will also evaluate an approach for market-oriented allocation of resources in clouds [Buyya et al. 2008].

7. ICFF INFRASTRUCTURE COMPONENTS

7.1 ICFF functionalities and Requirements

The proposed ICFF allows clouds from different administrative domains to create a federation[Makkes et al. 2013]. The federation allows for end-users to access cloud services from multiple domains without need to obtain a separate identity, while services remain under control of their original operator or home provider.

The Intercloud Federation Framework is responsible for coordinating allocation of resources in a unified way. 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. At the same time the federated Intercloud infrastructure requires a number of functionalities, protocols and interfaces to support its operation:

- Service and Trust Brokers
- Service Registry
- Service Discovery
- Identity provider (IDP), including attributes management
- Service and/or inter-domain gateway.

Correspondingly, the ICFF interfaces should support the following functionalities:

- Names and attributes resolution, translation and management (if/as needed)
- Publishing and subscription
- Discovery
- Trust/key management
- Service, infrastructure and federation itself lifecycle management.

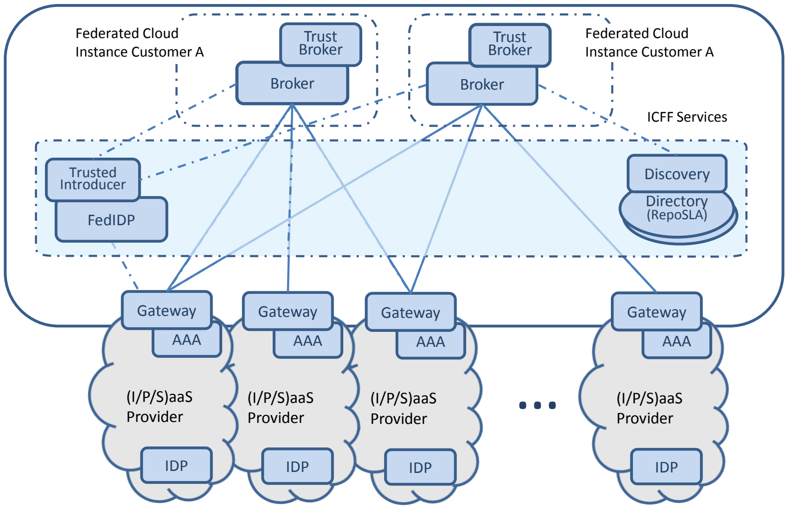

Figure 5. Intercloud federation infrastructure

The following federation related issues must be addressed in the further ICFF definition:

- Federation, delegation and trust management
- Single Sign On (SSO) and session credentials management
- Attributes management in federations, attributes validation , mapping and translation
- Federation governance, including federation lifecycle 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 [Subramanian 2011; GN3 FedNet ; OASIS]

7.2 Cloud Service Broker

To overcome these shortcomings of decentralized non-coordinated allocation of resources with in multi-provider multi-domain heterogeneous cloud services, we introduce a service broker to solve allocation of resources. We identify the broker as the key component for federation, which does not have to be exclusive.

The role and responsibility of the service broker is to solve the resource brokering problem defined as: "allocation of resources across the multiple cloud resources such as computational clusters, parallel supercomputers, storage clusters that belong to different administrative domains.

The service broker has interaction with both customers and providers to allocate and deallocation resources across multiple cloud providers on behave of the customers. Having a broker allocate resources on behave will simplify administration for cloud providers, as cloud provider only have to do accounting for service brokers, instead for every customer. Service broker brings benefits of having a unified interface to all cloud providers in the federation what facilitates also interoperability between different participating clouds.

7.3 Service registry

The service registry is a directory where cloud providers can publish information about available services IaaS, SaaS and PaaS, that includes details about services, their interfaces and availability as well as Service Level Agreements and associated policies. The broker can query service registry information and negotiate SLA and policy with the clients, including allocation in a specific cloud provider.

7.4 Identity Provider

ICFF operates across security domains, which are involving different cloud entities, from cloud providers to cloud consumers [NIST SP 500-292]. In this context, ICFF needs to support and integrate with the identity and trust management for these entities for both provider and customer sides. The dynamic resource provisioning in the collaboration scenarios of cloud providers require the trust management to carry out trust establishments between them. The trust management in the ICFF needs to support following requirements:

- Dynamic trust establishment between indirect cloud entities: Current relationships between cloud entities often rely on SLAs, which are mostly suitable for direct relationships. ICFF scenarios require a cloud provider or cloud consumer could connect to other unknown entities, through a chain of direct SLA relationships, which is known as dynamic trust relationship [Ngo et al. 2012].
- Interoperate and extend standardized mechanisms on multi-domain identity management and trust management, which are SAML [Cantor et al. 2005], OAuth2 [Kaila 2008], to support on-demand provisioned clouds.
- A fine-grained trust management policy language. ICFF should take into account federated identity management in its operation management:
- Compatible with existing public identity management systems.
- Interoperate between identity management with the on-demand access control services to manage cloud resources.

8. INTERCLOUD FEDERATION OPERATIONAL PATTERNS

8.1 Roles and Actios

We define the following main actors and roles adopting the Resource-Ownership-Role-Action (RORA) model proposed in [Garcia-Espin et al. 2012]:

- Cloud Service Provider (CSP) as entity providing cloud based services to customers, on their request and based on the business agreement that is expressed as Service Level Agreement (SLA). We need to admit specifics of business relation in clouds due to the fact that majority of cloud services are self-services and they are governed under general or individualized SLA.
- Cloud Broker is an entity that may play a role of the third party in offering cloud service adding value of negotiating with many CSPs or customer groups and in some cases managing complex multi-provider services.
- Cloud Service Operator and/or Integrator is a new emerging role of the company that provides a value added service of integrating services from multiple cloud providers and delivering them to the customer.
- Customer (like enterprise or university)
- User is an end-user consuming cloud based services; in cloud services provisioning.

Other roles such as Cloud Carrier and Cloud Auditor are defined in the NIST standards [NIST SP 800-145].

Typically, federation membership is managed by IDP hosted by customer or user home organization. In case of the dynamic federation that can be initiated by the user, a new IDP will be created as a part of the provisioned cloud based infrastructure. The following are assumption about what basic services and mechanism the new dynamically created IDP will possess or inherit:

- Instantiated from the CSP IDP and by creation is federated with the other user IDPs where user is a member;
- The created dynamic trust federation will use the dynamic IDP as a trust proxy or a broker in case if user processes run across multiple CSP resources or services.

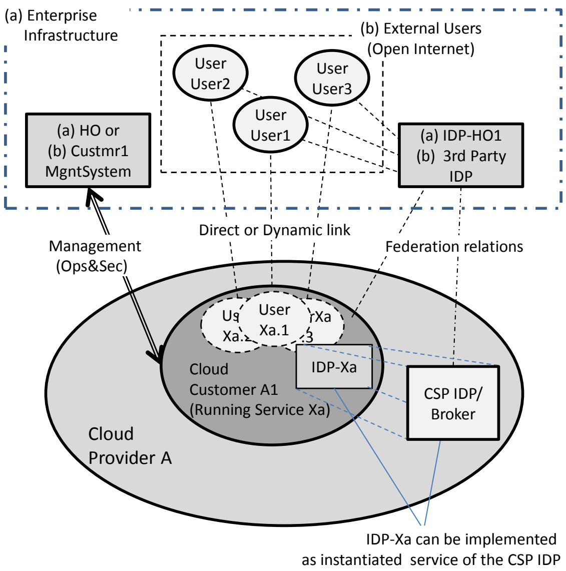
(a) Enterprise Infrastructure
(b) External Users (Open Internet)
User User2
User User3
User User1
(a) HO or (b) Custmr1 MgntSystem
(a) IDP-HO1 (b) 3rd Party IDP
Management (Ops&Sec)
Direct or Dynamic link
Federation relations
User Xa.1
IDP-Xa
Cloud Customer A1 (Running Service Xa)
CSP IDP/ Broker
Cloud Provider A
IDP-Xa can be implemented as instantiated service of the CSP IDP

Figure 6. Customer/user side federation for delivery of the federated cloud services to enterprise customers

8.2 Customer side and Provider side Federations

We define the two general use cases for federating cloud resources on the provider side or creating federated multi-provider infrastructures and services to deliver federated cloud services to the customer.

Figure 6 illustrates two cases when (a) cloud based services and/or infrastructure needs to be integrated/federated with the existing user accounts and enterprise infrastructure, or (b) or cloud based public services can use external IdP and in this way already existing user accounts with the single or multiple 3rd party IDP (such as Google+/GooglePlay, Facebook, Microsoft, or other open IDP).

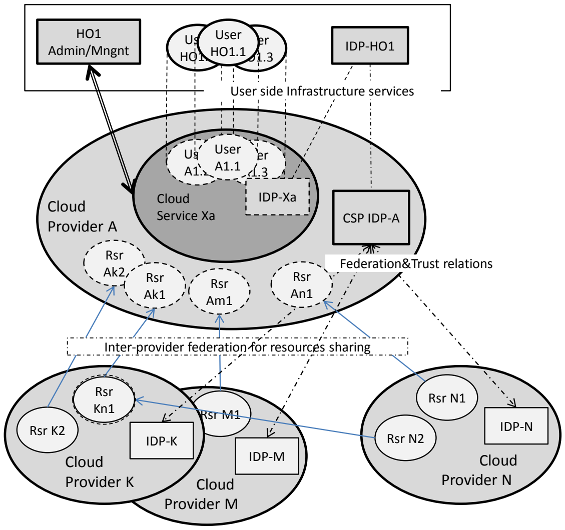

Figure 7. Provider side federation for resources sharing and outsourcing

Figure 7 illustrates the major actors and their relation in the provider side federation to share and outsource cloud resources when providing a final service to the customer.

9. ABSTRACT MODEL FOR CLOUD BASED INFRASTRUCTURE SERVICES PROVISIONING

Figure 8 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) [Demchenko et al. 2012].

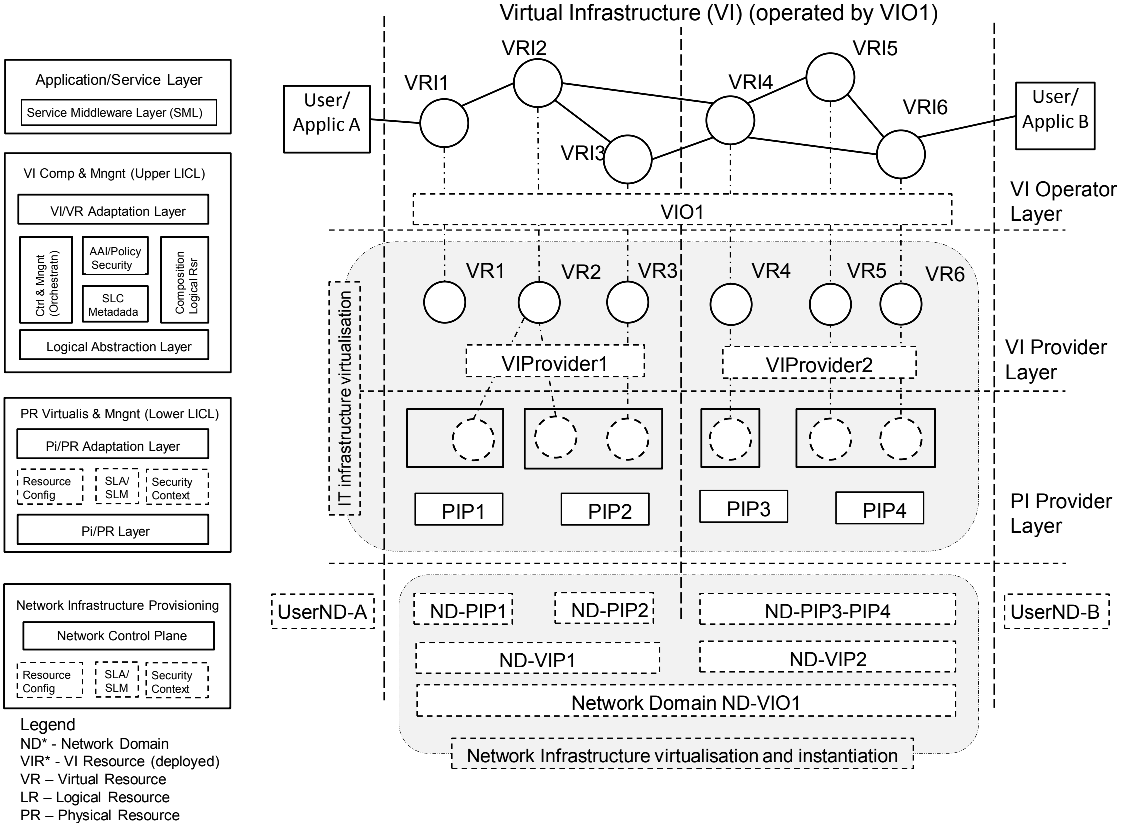

Figure 8. Main actors, functional layers and processes in on-demand infrastructure services provisioning

The infrastructure provisioning process, also referred to as Service Delivery Framework (SDF), is adopted from the TeleManagement Forum SDF [TR139] 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.

The infrastructure services virtualisation and composition is defined by the Infrastructure Services Modeling Framework (ISMF) described in the previous authors' work [20].

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.

10. 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 9): 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 [GEYSERS D2.2].

Figure 9 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 [Ngo et al. 2011].

LICL is the key element in the GEYSERS architecture in order to provision infrastructure services 20]. The LICL is divided into two main sub-systems: the upper-LICL which is responsible mainly for the virtual infrastructure management and satisfies the needs and requirements of the virtual infrastructure provider; and the lower-LICL, which is responsible for physical resource virtualisation and management and which satisfies the requirements of the physical infrastructure provider.

The upper-LICL functionalities covered include the virtual infrastructure creation, management and re-planning, and the SLA enforcement. The virtual infrastructure creation is done as a composition of different virtual resources available from one or multiple PIPs. Such a virtual

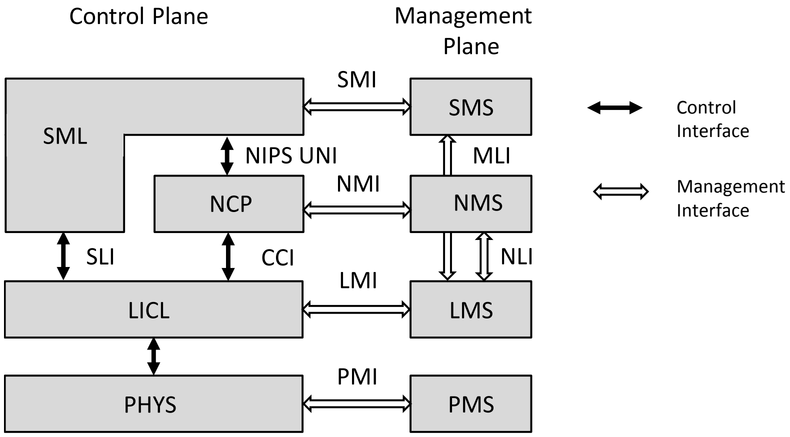

Figure 9. GEYSERS control and management architecture and interfaces.

infrastructure is provisioned towards the virtual infrastructure operator as a unit. The upper-LICL offers dynamic re-planning functionalities as a response to the changing requirements of the VIO. Such dynamic re-planning may involve the inclusion of new resources to the virtual infrastructure, the release of un-used resources, or resizing of some of them (e.g., increase or decrease the total bandwidth capability of a virtual link). As a part of the system oriented to provide dynamic infrastructure services, the upper-LICL provides capabilities to ensure SLA levels are met during the whole service lifecycle.

The lower-LICL covers the functionalities regarding physical resource abstraction and resource virtualisation. The tools offered by the lower-LICL are used by the PIP in order to manage its own infrastructure. The lower-LICL is responsible for the physical resource abstraction that basically comprehends all the necessary steps to create a logical resource representing the physical resource. It also is in charge of the virtual resource creation and management, as well as the resource monitoring and configuration.

11. RELATED WORK

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 [NIST SP 500-292]. A few works [Zhang and Zhou 2009; Shan et al. 2012; Takefusa et al. 2011; Bosch et al. 2011; IBM CCRA] 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 [Zhang and Zhou 2009] proposes the Cloud Computing Open Architecture (CCOA) based on SOA and virtualisation and derives ten interconnected architectural models, but it doesnt go further with suggesting implementation. The position paper [Shan et al. 2012] 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 [Takefusa et al. 2011] 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 [Bosch et al. 2011] 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 [IBM CCRA] that provides a lot of useful detail on CCRA implementation, interfaces and programming models with the IBM tools and platforms.

12. CONCLUSION 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) [OGF], IETF on Cloud Architecture Framework definition [IETF-Cloud 2013].

REFERENCES

Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., and Morrow, M. 2009. Blueprint for the intercloud - protocols and formats for cloud computing interoperability. In *ICIW*. 328–336.

Bosch, P., Duminuco, A., Pianese, F., and Wood, T. L. 2011. Telco clouds and virtual telco: Consolidation, convergence, and beyond. In *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*. IEEE, 982–988.

Buyya, R., Ranjan, R., and Calheiros, R. 2010. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. *Algorithms and architectures for parallel processing*, 13–31.

Buyya, R., Yeo, C. S., and Venugopal, S. 2008. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*. Ieee, 5–13.

Cantor, S., Kemp, J., Philpott, R., and Maler, E. 2005. Assertions and protocols for the oasis security assertion markup language. *OASIS Standard (March 2005)*.

Demchenko, Y., Ngo, C., Makkes, M., Strijkers, R., and de Laat, C. 2012. Defining inter-cloud architecture for interoperability and integration. In *CLOUD COMPUTING 2012, The Third International Conference on Cloud Computing, GRIDs, and Virtualization*. 174–180.

Demchenko, Y., Ngo, C., Martínez-Julia, P., Torroglosa, E., Grammatikou, M., Jofre, J., Gheorghiu, S., Garcia-Espin, J. A., Perez-Morales, A. D., and de Laat, C. 2012. GEMBus based services composition platform for cloud paas. In *Service-Oriented and Cloud Computing*. Springer, 32–47.

DMTF OVF. Open Virtualization Format (OVF), DMTF. `http://www.dmtf.org/standards/ovf`.

Garcia-Espin, J., Riera, J., Figuerola, S., and Lopez, E. 2012. A multi-tenancy model based on resource capabilities and ownership for infrastructure management. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*. 682–686.

GEANT. GEANT Project. `http://www.geant.net/pages/home.aspx`.

GEYSERS. GEYSERS Project. Generalised Architecture for Dynamic Infrastructure Services. `http://www.geysers.eu/`.

GEYSERS D2.2. GEYSERS Project Deliverable 2.2 (update): GEYSERS overall architecture & interfaces specification and service provisioning workflow. http://wiki.geysers.eu/images/5/55/Geysers-deliverable_2.2_update_final.pdf.

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

GN3 FedNet. GEANT3 Project. Federated Network Architectures. http://www.geant.net/Research/Future_Network_Research/Pages/FederatedNetworkArchitectures.aspx.

IBM CCRA. Cloud Computing Reference Architecture 2.0.

IEEE P2302. Standard for intercloud interoperability and federation (SIIF). http://standards.ieee.org/develop/project/2302.html.

IETF-Cloud. 2013. Cloud Reference Framework. Internet-Draft, version 0.5, July 2, 2013. [online]. http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-05.txt

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

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

Kaila, P. 2008. OAuth and OpenID 2.0, From End-to-End to Trust-to-Trust. https://www.zotero.org/jod999/items/itemKey/S449GVRK.

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

Makkes, M. X., Ngo, C., Demchenko, Y., Stijkers, R., Meijer, R., and de Laat, C. 2013. Defining intercloud federation framework for multi-provider cloud services integration. In *CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization*. 185–190.

Ngo, C., Demchenko, Y., and de Laat, C. 2012. Toward a dynamic trust establishment approach for multi-provider intercloud environment. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*. IEEE, 532–538.

Ngo, C., Membrey, P., Demchenko, Y., and de Laat, C. 2011. Security framework for virtualised infrastructure services provisioned on-demand. In *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*. IEEE, 698–704.

NIST SP 500-292. Cloud Computing Reference Architecture, v1.0. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

NIST SP 800-145. The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

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

OASIS. IDCloud TC: OASIS Identity in the Cloud TC. http://wiki.oasis-open.org/id-cloud/.

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

RFC3945. RFC 3945. Generalized Multi-Protocol Label Switching (GMPLS) Architecture. http://www.ietf.org/rfc/rfc3945.txt.

Shan, C., Heng, C., and Xianjun, Z. 2012. Inter-cloud operations via NGSON. *Communications Magazine, IEEE 50,* 1, 82–89.

SNE-IaaS. 2011. Generic Architecture for Cloud Infrastructure as a Service (IaaS) Provisioning Model. http://staff.science.uva.nl/~demch/worksinprogress/Jsne2011-techreport-2011-03-clouds-iaas-architecture-release1.pdf.

SNIA CDMI. Cloud Data Management Interface, SNIA. http://www.snia.org/cdmi.

Subramanian, K. October 6, 2011. Defining federated cloud ecosystems. http://www.cloudave.com/15323/defining-federated-cloud-ecosystems/.

Takefusa, A., Nakada, H., Takano, R., Kudoh, T., and Tanaka, Y. 2011. Gridars: a grid advanced resource management system framework for intercloud. In *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*. IEEE, 705–710.

TMF Fwx. TM Forum Frameworx. http://www.tmforum.org/frameworx/1911/home.html.

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

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

Zhang, L. and Zhou, Q. 2009. CCOA: Cloud computing open architecture. In *Web Services, 2009. ICWS 2009. IEEE International Conference on*. Ieee, 607–616.

Dr. Yuri Demchenko is a Senior Researcher at the System and Network Engineering of the University of Amsterdam. He is graduated from the National Technical University of Ukraine ”Kiev Polytechnic Institute” where he also received his PhD (Cand. of Science) degree. His main research areas include Cloud and Intercloud Architecture, Big Data Science Infrastructure, general security architectures and distributed access control infrastructure for cloud based services and data centric applications. He is currently involved in the European projects GN3plus and EUBrazil where he conducts research and developments on the cloud federation infrastructure and cloud based scientific infrastructures. His past projects included the major European projects EGEE, Phosphorus, GEYSERS, GEANT3. He is actively contributing to the standardisation activity at OGF, IETF, NIST, TMF on defining general Cloud and Intercloud architectures for infrastructure services provisioning on-demand. Yuri is a IEEE and Computer Society member and is conducting an active community activity contributing to IEEE Cloud Computing Initiatives projects and numerous conferences and workshops organization as a co-chair and a Program Committee member, e.g. conferences CloudCom2011-2013, CTS2007-2013, workshops COLSEC009, SECOTS2010, NetCloud2011-2013 to name few of them.

Marc X. Makkes received a Bsc degree in computer science from the University of Amsterdam and MSc in Information Security Technology from Eindhoven University of Technology. He currently pursues a PhD degree at the University of Amsterdam and works as a researcher at TNO. He has several papers published which include journal, conference and workshop papers in the field of cryptography and distributed computing. His research interest include distributed computing, control and information theory.

Rudolf J. Strijkers received a BSc and MSc degree in computer science from the University of Amsterdam. He currently pursues a PhD degree at the same university and works as a researcher at TNO. He has published several papers in conferences and workshops. His research interests include distributed computing, and the design and implementation of new networking concepts.

Canh Ngo received the BEng degree in Information Technology in 2006 from Hanoi University of Technology, Vietnam and MSc degree in Computer Engineering in 2008 from the Kyung Hee University, South Korea. Currently he is a PhD student in the Informatics Institute at the University of Amsterdam. His research interests include security, access control, identity management systems, cloud computing and distributed systems.

Prof. Cees de Laat chairs the System and Network Engineering (SNE) research group. Research covers optical and switched networking and workflows for processing of big data in PetaScale e-Science applications, Semantic Web to describe e-infrastructure resources, information complexity, Authorization architectures and Systems Security & privacy of information in distributed environments. Prof. de Laat serves as gfsg member of Open Grid Forum, is chair of GridForum.nl and serves on the Lawrence Berkeley Laboratory Policy Board on matters regarding ESnet, is co-founder and organizer of several past meetings of the Global Lambda Integrated Facility (GLIF) and founding member of CineGrid.org. http://delaat.net/