Intercloud Architecture Framework for Heterogeneous Cloud based Infrastructure Services Provisioning On-Demand

Yuri Demchenko, Canh Ngo, Cees de Laat
University of Amsterdam, Amsterdam, The Netherlands
e-mail: {y.demchenko, t.ngo, delaat}@uva.nl

Joan Antoni Garcia-Espin, Sergi Figuerola
I2CAT, Barcelona, Spain
e-mail: { joan.antoni.garcia, sergi.figuerola}@i2cat.net

Juan Rodriguez, Luis M. Contreras
Telefónica I+D, Madrid, Spain
e-mail: {juanrm, lmcm}@tid.es

Giada Landi, Nicola Ciulli
NextWorks, Pisa, Italy
e-mail: {g.landi, n.ciulli}@nextworks.it

***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, to allow their on-demand provisioning. 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 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 paper also provides suggestions for consistent inter-cloud security infrastructure. 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, Cloud Security.

I. INTRODUCTION

Clouds are widely used by both industry and research community; clouds provide an affordable access to powerful computing facilities for open public. Cloud Computing [1, 2] technologies are evolving as a common way to provide infrastructure services, using resources virtualization as a tool for the efficient usage of the physical resources, and requiring on-demand provisioning capabilities for an adequate commercialization. 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 heterogeneous 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 initial research results presented in the authors paper [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. 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 presents a general analysis of the cloud security issues and refers to ongoing works by the authors. Section IX provides information about ongoing implementation of the ICAF components in the GEYSERS project. Related works are discussed in section X, and the paper concludes with the future developments in section XI.

II. Cloud Standardisation Overview

For the purpose of this paper, we provide a short overview of the cloud related standards by National Institute of Standards and Technology (NIST) that define the Cloud Computing Reference Architecture (CCRA) [2], and IEEE standardisation activity by IEEE P2302 Intercloud Working Group to define Intercloud Interoperability and Federation (SIIF) [9] framework. Suggestions are given how they can be used for the definition of the general Intercloud architecture for interoperability and integration.

We also refer to the Technical Reports (Part 1 to 7) published by the ITU-T Focus Group on Cloud Computing (FG-Cloud) [10] that present taxonomies, use cases, functional requirements, cloud infrastructure and reference architecture definition, cloud security, and discuss scenarios with inter-cloud peering, federation and brokering, all this from the telecommunication perspectives. These documents provide a valuable input about importance of manageable network infrastructure as a part of provisioned cloud infrastructure.

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) [11], Cloud Data Management Interface (CDMI) [12], and Open Cloud Computing Interface (OCCI) [13]. 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 Reference Architecture (CCRA)

NIST is leading an internationally recognized activity on defining standard base in Cloud Computing, which has resulted in a number of documents that create a solid base for cloud services development and offering: NIST SP 800-145 cloud definition [1], NIST SP 500-292, Cloud Computing Reference Architecture, v1.0 [2], NIST SP 800-146, Cloud Computing Synopsis and Recommendations [14].

The NIST Cloud Computing Reference Architecture (CCRA) identifies the major actors (Cloud Consumer, Cloud Service Provider, Cloud Auditor, Cloud Broker, and Cloud Carrier) and 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 explaining 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 inter-cloud services integration and interoperability, in particular, to address inter-cloud 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 [15].

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 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;

(2) large project-oriented scientific infrastructures (capable of handling big data) including dedicated transport network infrastructure that need to be provisioned on-demand [16];

(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.

All use cases should allow the whole infrastructure of computers, storage, network and other utilities to be provisioned on-demand, independently for the physical platform 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.

The main goal of the enterprise or scientific infrastructure is to support the enterprise or scientific workflow and operational procedures related to processes monitoring and data processing. Cloud technologies simplify building such infrastructure and provisioning it on-demand.

Figure 1 illustrates how an example enterprise or scientific workflow can be mapped to cloud based services and then deployed and operated as an instant inter-cloud infrastructure. It contains cloud infrastructure segments IaaS (VR3-VR5) and PaaS (VR6, VR7), separate virtualised resources or services (VR1, VR2) that can be also enterprise none-cloud legacy applications, two interacting campuses A and B with existing campus facilities, 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.

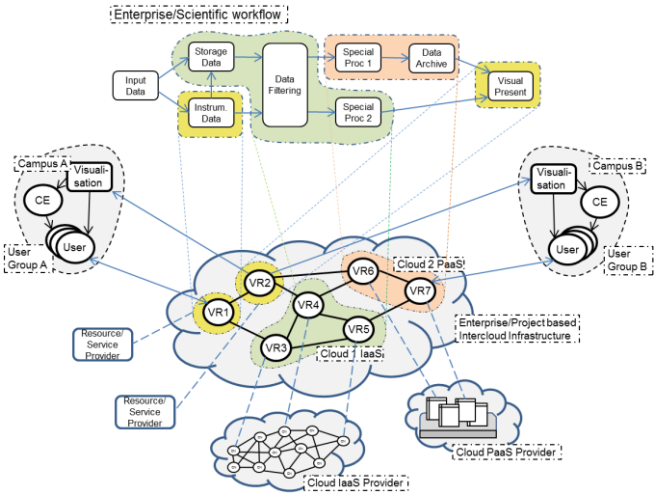

Figure 1. Enterprise or project oriented collaborative cloud based infrastructure created to support enterprise or scientific workflow.

IV. ICAF Requirements and Definition

The proposed Intercloud Architecture Framework 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:

- 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
- Allow applications control infrastructure and related supporting services at different service layers to achieve run-time optimization (Intercloud control and management functions).
- 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 federations
- 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, Service Oriented Architecture (SOA) and Grid/OGSA [17], in particular, support Virtual Organisations (VO) infrastructure federation mechanisms widely used by e-Science/Grid community.

From 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 federation of independently managed clouds and related infrastructure components belonging to different cloud providers and/or administrative domains. It 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 together with their relations in terms of resources operation, management and ownership. ICOF requires support from and interacts with both ICCMP and ICFF.

At this stage of research, we have defined in details only the multi-layer Cloud Services Model that provides a basis for the definition of all other functional components and protocols. and the CSM can be built using modern SOA technologies to support basic cloud service models. For the other components (ICCMP, ICFF and ICOF) we have defined the main functionalities and their interfaces, while the internal architecture design and their implementation in support of on-demand IaaS provisioning are still in progress.

V. Multi-Layer Cloud Services Model (CSM)

Figure 2 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 in most cases expose standard based interfaces to user services or applications, in fact, use proprietary interfaces to the provider's physical resources and platform. In this respect the proposed model can be used for the inter-layer interfaces definition.

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. 2):

(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.

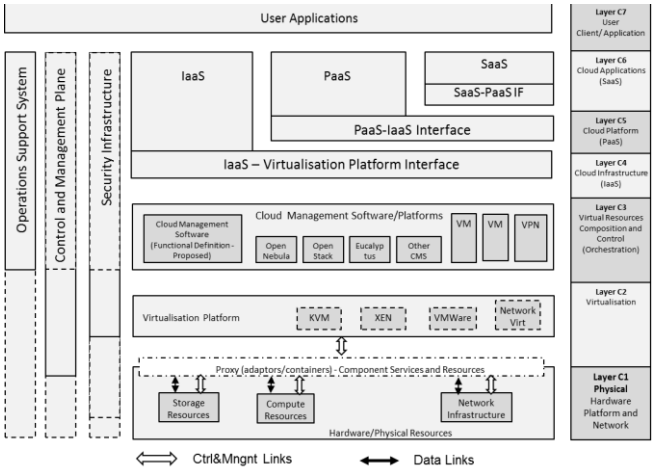

Figure 2. Reference Multilayer Cloud Services Model (CSM).

The three vertical planes or cross-layer infrastructures (on the left part of the figure) 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 3 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 resources (virtualised or physical) may be non-standard or proprietary. The role of ICCMP is to provide logical and functional interfaces 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 inter-cloud 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.

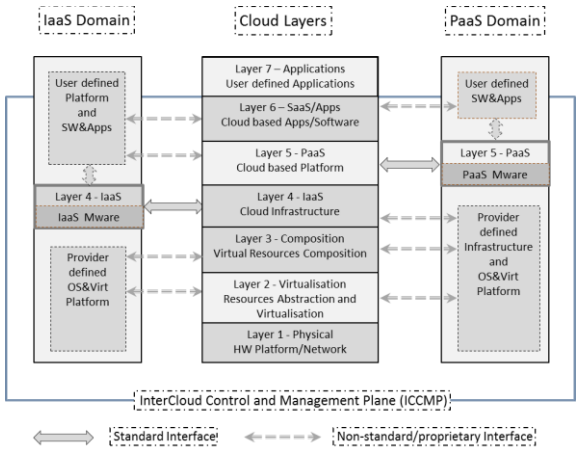

Figure 3. Example of the IaaS and PaaS cloud domains communication that uses standard interfaces and proprietary interfaces

Based on the GEYSERS project implementation (see section IX) we can suggest the GMPLS [18] as an appropriate technology that can be extended to build an ICCMP control plane able to optimise the network infrastructure servicers according to the required compute and storage resources attached to network nodes [19, 20]. However, management functionalities will require the development of new interfaces.

B. *Intercloud Federation Framework (ICFF)*

Figure 4 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 inter-cloud infrastructure requires a number of functionalities, protocols and interfaces to support its operation:

- Trust and service brokers
- Service Registry
- Service Discovery
- Identity providers (IdP) and attributes services
- Trust managers/routers
- Intercloud gateway and/or attribute/namespace translators.

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].

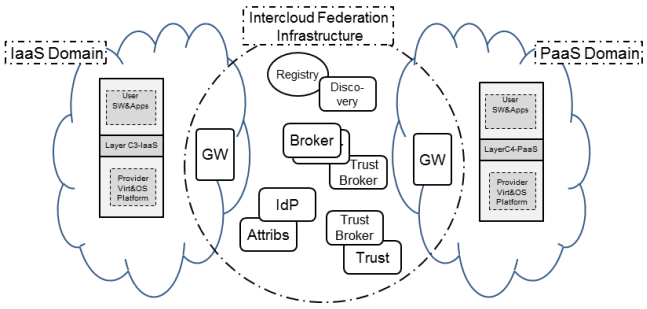

Figure 4. Intercloud Federation Framework (ICFF) components

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 [19]. 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 standards related to eTOM and Operational Support Systems [24], Service Delivery Framework (SDF) [25].

VII. Abstract Model for Cloud based Infrastructure Services Provisioning

Figure 5 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), and 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) [26] that defines the core components supporting services composition and the composite services lifecycle management.

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 a provisioning workflow all processes that are run by different supporting systems and executed by different actors.

Physical Resources (PR), including IT and network resources, 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 Resources (LR) that will undergo a number of abstract transformations possibly including 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 [16].

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.

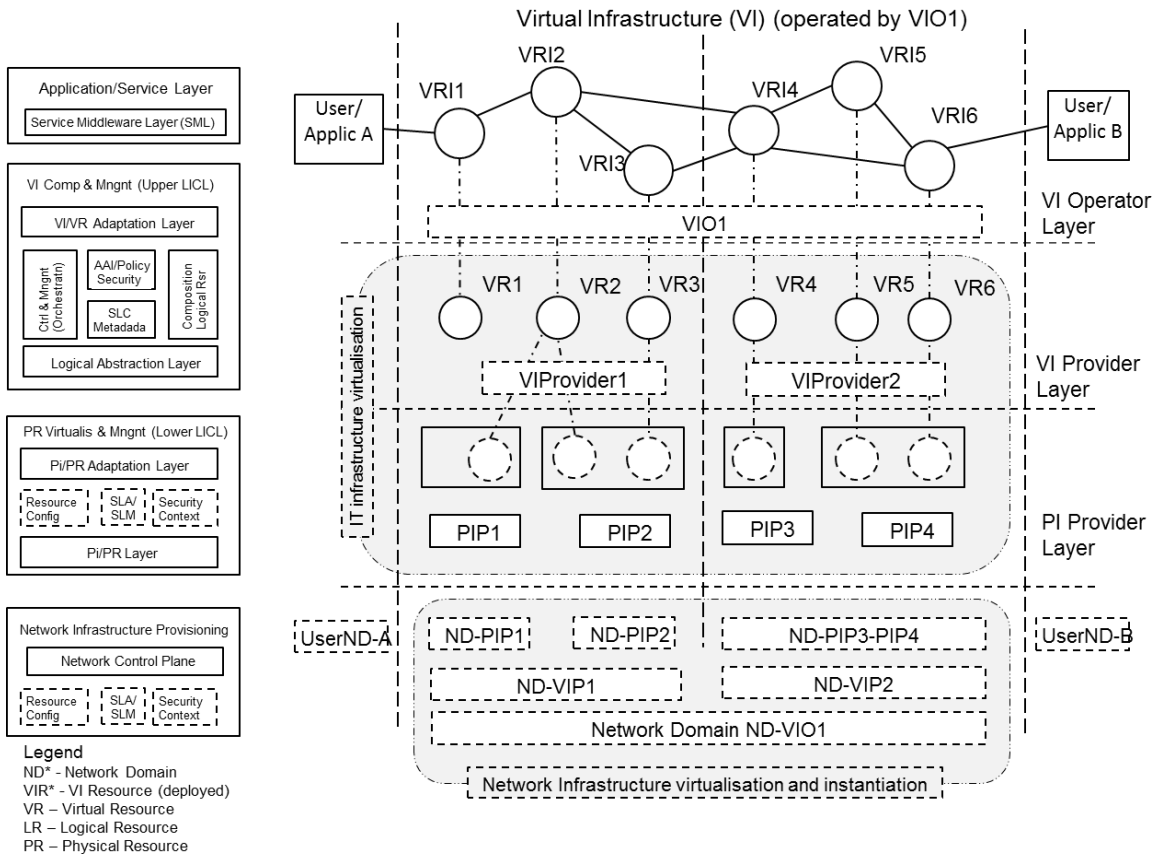

Figure 5. Main actors, functional layers and processes in on-demand infrastructure services provisioning

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). From the user/consumer point of view, VIO provides valuable services over the heterogeneous virtual infrastructure, including – including IT resources and networks, and is in charge of managing the provisioned infrastructure optimizing usage of resources.

VIII. INTERCLOUD SECURITY INFRASTRUCTURE

Security infrastructure is an important component of the provisioned on demand cloud and intercloud based infrastructures. Current cloud security model is based on the assumption that the user/customer should trust the provider. This is governed by the Service Level Agreement (SLA) that in general defines mutual provider and user expectations and obligations. However, such approach doesn't scale well with the potential need to combine Cloud based services from multiple providers when building complex infrastructures.

Currently provided security services are based on VPN security model and provide only simple access control services based on users access over SSH as a commonly used secure channel to access remote processing environment. More advanced security services and fine grained access control cannot be achieved without deeper integration with the cloud virtualisation platform and incumbent security services, what in its own turn can be achieved with open and well defined cloud IaaS platform architecture.

In the clouds data are sent to and processed in the environment that is not under the user or data owner control, and potentially can be compromised either by clouds insiders or by other users sharing the same resource. Data/information must be secured during all processing stages – upload, process, store, stream/visualize. Policies and security requirements must be bound to the data and there should be corresponding security mechanisms in place to enforce these policies.

The following problems and challenges can be identified when intending to build security infrastructure for the intercloud environment and infrastructure:

- Data protection both stored and "on-wire" that include, besides the traditional confidentiality, integrity, access control services, also data lifecycle management and synchronization.
- Access control infrastructure virtualisation and dynamic provisioning, including dynamic/automated access control policies generation or composition.
- Security services lifecycle management, in particular service related metadata and properties, and their binding to the main services.
- Security sessions and related security context management during the whole security services lifecycle,

including binding security context to the provisioning session and virtualisation platform.

- Trust and key management in provisioned on demand security infrastructure, and support of the Dynamic Security Associations (DSA) that should provide fully verifiable chain of trust from the user client/platform to the virtual resource and the virtualisation platform.
- SLA management, including initial SLA negotiation, SLA enforcement at the planning stage and SLA monitoring at the operation stage. SLA can specify security requirements and trust anchors that can be used for bootstrapping the DSA at the provisioning stages.

The security solutions and supporting infrastructure should support consistent security sessions management:

- Special session for data transfer that should also support data partitioning and run-time activation and synchronization.
- Session synchronization mechanisms that should protect the integrity of the remote run-time environment.
- Secure session fail-over that should rely on the session synchronization mechanism when restoring the session.

Wider clouds adoption by industry and their integration with advanced infrastructure services will require implementing manageable security services and mechanisms for the remote control of the cloud operational environment integrity by users.

We refer to the ongoing research by the authors on the general cloud security infrastructure and services definition to address the described above requirements and challenges [26, 27, 28]. The CloudCom2011 paper [26] describe the general security architecture for cloud IaaS service model and its implementation in the Dynamic Access Control Infrastructure (DACI) that uses DSA to provision consistent security infrastructure on-demand. The two follow-on papers are devoted to the policy and security context management in the provisioned on-demand multi-domain and multi-provider cloud infrastructure [27] and propose the Dynamic Infrastructure Trust Bootstrapping Protocol (DITBP) [28] that allows creating DSA during the infrastructure provisioning process.

IX. 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 the on-demand provisioning of optimized Network+IT infrastructures and services. The proposed architecture is structured in three different layers (Figure 6):

(a) Logical Infrastructure Composition Layer (LICL) for infrastructure services (Network+IT) virtualisation and provisioning;

(b) Enhanced Network Control Plane (NCP+) for operating the virtual infrastructure domains and providing on-demand connectivity services;

(c) Service Middleware Layer (SML) that actually represents the Application Layer in CSM.

The project also defines an operational framework for combined network and IT services provisioning (including planning and re-planning), monitoring, SLA and services lifecycle management [19, 30].

Figure 6 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.

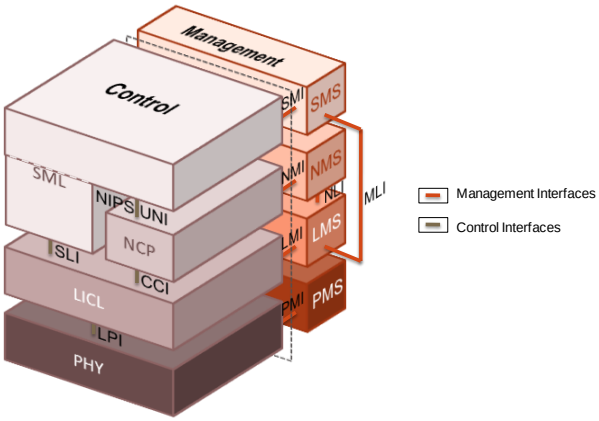

Figure 6. GEYSERS control and management architecture and interfaces.

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].

X. 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]. Regarding the inter-cloud issue, GICTF has recently released a white paper [31] describing a number of inter-cloud uses cases and has derived from them a collection of technical requirements to be taken into account for supporting such interconnection scenarios. A few works [32-35] 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 [32] 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 [33] explores an approach to describe the inter-cloud operations based on the New Generation Service Overlay Network (NGSON) but the proposed solutions are rather focused on the content delivery overlay networks. Paper [34] 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 [35] presented by Alcatel-Lucent Bell Labs provides an 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. A further example on this can be found in [36] where it is described a framework to offer Telecom as a Service as a way for hosting and operating telecom services in a cloud environment. In this case, the framework tries to consider specific particularities of telecom services such as statefulness, disruption intolerance, and long duration sessions (if compared with typical web sessions duration).

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 [37] that provides a lot of useful detail on CCRA implementation, interfaces and programming models with the IBM tools and platforms.

XI. 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 inter-cloud architectures by splitting concerns and using already existing and widely accepted solution where possible. The analysis of the security issues in provisioning complex heterogeneous multi-provider intercloud infrastructures presented in the paper will also provide a good basis for the further intercloud security infrastructure definition and development.

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) [38], and IETF on Cloud Architecture Framework definition [39]

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).

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. Proc. 10th Intern Conf. 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

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

[8] Demchenko, Y., C.Ngo, M.Makkes, R.Strijkers, C. de Laat, Defining Inter-Cloud Architecture for Interoperability and Integration. The Third Intl Conf on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2012), July 22-27, 2012, Nice, France.

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

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

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

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

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

[14] 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

[15] On-Demand Infrastructure Services Provisioning Best Practices. Open Grid Forum ISOD-RG Draft. Version 0.8. [online] https://forge.ogf.org/sf/go/doc16494?nav=1

[16] 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

[17] GFD.80: Open Grid Services Architecture (OGSA). Open Grid Forum standard. [online]

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

[19] 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

[20] G. Landi, N. Ciulli, J. Buysse, K. Georgakilas, M. Anastasopoulos, A. Tzanakaki, C. Develder, E. Escalona, D. Parniewicz, A. Binczewski, B. Belter, "A Network Control Plane architecture for on-demand co-provisioning of optical network and IT services", Future Network & Mobile Summit 2012, Berlin, Germany, July 2012

[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] TeleManagement 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] 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.

[27] Demchenko, Y., C.Ngo, C. de Laat, T.Wlodarczyk, C.Rong, W.Ziegler, Security Infrastructure for On-demand Provisioned Cloud Infrastructure Services, Proc. 3rd IEEE Conf. on Cloud Computing Technologies and Science (CloudCom2011), 29 Nov - 1 Dec 2011, Athens, Greece.

[28] Ngo, C., P. Membrey, Y.Demchenko, C. de Laat, Policy and Context Management in Dynamically Provisioned Access Control Service for Virtualised Cloud Infrastructures. The 7th Intl Conf on Availability, Reliability and Security (AReS 2012), 20-24 Aug 2012, Prague, Czech Republic.

[29] Membrey, P., K.C.C.Chan, C.Ngo, Y.Demchenko, C. de Laat, Trusted Virtual Infrastructure Bootstrapping for On Demand Services. The 7th International Conference on Availability, Reliability and Security (AReS 2012), 20-24 August 2012, Prague. ISBN 978-0-7695-4775-6

[30] Antonescu, A.-F., P. Robinson, P., L.M. Contreras, J. Aznar, S. Soudan, F. Anhalt, J.A. García-Espin, Towards Cross Stratum SLA Management with the GEYSERS Architecture, 10th IEEE International Symposium on Parallel and Distributed Processing with Applications, (ISPA) 2012

[31] Global Inter-Cloud Technology Forum (GICTF). White Paper: Technical Requirements for Supporting the Intercloud Networking. [online]. http://www.gictf.jp/doc/GICTF_NWSWG-WhitePaper_e_20120420.pdf

[32] 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

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

[34] 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.

[35] 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.

[36] Chang, Y.-J., A. Hari, P. Koppol, A. Martin, T. Stathopoulos, Scalable and Elastic Telecommunications Services in the Cloud, Bell Labs Technology Journal, No. 17, vol. 2, pp. 81-96, September 2012.

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

[38] 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

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