System and Network Engineering Group, UvA

Universiteit van Amsterdam

SNE

System and Network Engineering

Intercloud Architecture for Interoperability and Integration

Release 1, Draft Version 0.5

Yuri Demchenko, Marc X. Makkes, Rudolf Strijkers, Canh Ngo
(open list to all contributors)

6 September 2012

http://staff.science.uva.nl/~demch/worksinprogress/sne2012-techreport-12-05-intercloud-architecture-draft05.pdf

Abstract

This report presents on-going research to develop the Intercloud Architecture (ICA) Framework that should address problems in multi-provider multi-domain heterogeneous Cloud based infrastructure services and applications integration and interoperability, including integration and interoperability with legacy infrastructure services. Cloud technologies are evolving as a common way of infrastructure services and resources virtualisation and provisioning on-demand. In this way, they bring applications and infrastructure services mobility and physical/hardware platform independency to the existing distributed computing and networking technologies. The report refers to existing standards in Cloud Computing, in particular, recently published NIST Cloud Computing Reference Architecture (CCRA). The proposed Intercloud Architecture Framework defines four complimentary components addressing Intercloud interoperability and integration: 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; Intercloud Control and Management Plane (ICCMP) that supports cloud based applications interaction; Intercloud Federation Framework (ICFF), Intercloud Operation Framework (ICOF).

The report briefly presents the architectural framework for cloud based infrastructure services provisioned on-demand being developed by authors that can be used as a basis for building multilayer cloud services integration framework that can allow optimised provisioning of both computing, storage and networking resources. The proposed architecture is intended to provide a conceptual model for developing Intercloud middleware and in this way will facilitate clouds interoperability and integration.

SNE technical report SNE-UVA-2012-05

Table of Contents

1 Introduction

Cloud Computing technologies [1, 2] are emerging as infrastructure services for provisioning computing and storage resources on-demand in a simple and uniform way and may involve multi-provider and multi-domain resources, including integration with the legacy services and infrastructures. 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 (similar to utilities) and mobility. Current development of the cloud technologies demonstrate movement to developing Intercloud models, architectures and integration tools that could allow integrating cloud based infrastructure services into existing enterprise and campus infrastructures, on one hand, and provide common/interoperable environment for moving existing infrastructures and infrastructure services to virtualised cloud environment. 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 virtualisation allows for easy upgrade and/or migration of enterprise application, including also the whole IT infrastructure segments. This brings significant cost saving comparing to traditional infrastructure development and management that requires lot of manual work.

Cloud based applications operate as regular applications in particular using modern SOA Web Services platforms for services and applications integration, however their composition and integration into distributed cloud based infrastructure will require a number of functionalities and services that can be jointly defined as Intercloud Architecture.

This report presents on-going research at the University of Amsterdam to develop the Intercloud Architecture (ICA) that should address problems with multi-domain heterogeneous cloud based applications integration and interoperability, including integration and interoperability with legacy infrastructure services, and to facilitate interoperable and measurable intra-provider infrastructures and clouds federation. The papers refers to the architectural framework for provisioning Cloud Infrastructure Services On-Demand [3] being developed by authors as a result of cooperative efforts in a number of currently running projects such as GEANT3 [4] and GEYSERS [5], that provides a basis for defining the proposed Intercloud architecture. This report summarises numerous discussions, developments and experimentations in a number of other projects the SNE group of the University of Amsterdam is involved.

The report is organised as follows. Section 2 provides overview and detailed analysis of the on-going standardisation activities at NIST and IEEE that have direct relation with and provide a basis for the proposed ICA. Section 3 describes basic use cases for defining ICA. Section 4 summarises the requirements and defines the main components of the proposed Intercloud architecture. Section 5 describes the proposed multi-layer cloud services model. Sections 6-8 consequently introduce basic functionality of the Intercloud Control and Management Plane, Intercloud Federation Framework, and Intercloud Operation Framework. Section 9 describes the abstract model for cloud based infrastructure services provisioning that also include the Virtual Infrastructure Composition and Management layer and Infrastructure Services Modelling Framework. Section 10 provides information about current implementation status and suggestions for future developments.

2 Cloud Standardisation Overview

For the purpose of this paper, in this section we provide detailed analysis of the related standards by National Institute of Standards and Technology (NIST) that define the Cloud Computing technology and Cloud Computing Reference Architecture, and IEEE standardisation activity to define Intercloud Interoperability and Federation framework. Suggestions are provided for the required extensions in the context of the proposed Intercloud Architecture.

At this stage of our research, we don't provide overview of the standards that define internal cloud management, components design and communications. This category of standards is well presented by DMTF, SNIA and OGF standards that correspondingly define standards for Open Virtual Machine Format (OVF) [7], Cloud Data Management Interface (CDMI) [8], and Open Cloud Computing Interface (OCCI)

[9]. These standards are commonly accepted by industry and provide a basis for intra-provider infrastructure operation and services delivery to customers.

2.1 IEEE Intercloud Working Group (IEEE P2302)

IEEE P2302 Working Group recently published a draft Standard on Intercloud Interoperability and Federation (SIIF) [10] 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.

However, the proposed approach has a limited scope by attempting to address a hypothetical scenario when all resources and applications are located and run in multiple clouds and they need to be federated similar to Contend Distribution Network (CDN) [11]. The proposed architecture tries to replicate the CDN approach but doesn't address the generic problems with interoperability and integration of the heterogeneous multi-domain and multi-provider cloud base infrastructure.

The proposed in [12] solutions use extended XMPP protocol as a base for the Intercloud protocol, what requires creating an Intercloud root that will interact with exchange hosts in each cloud domain to support communications, trust management and identity federation.

The proposed architecture originated from the position paper published by Cisco in 2009 [13] that tried to leverage the basic routing and messaging Internet protocols such as BGP, OSPF, XMPP to address Intercloud integration and interoperability.

The limitation of the proposed architecture and approach is that it tries to closely imitate Internet approach in building hierarchical interconnected infrastructure for Internet protocol based services to support Intercloud communication. But actually there is no need for such additional Intercloud layer or infrastructure because cloud applications and infrastructure can use all Internet technologies directly to support intra-provider communications and user-customer-provider or inter-provider communications, given the appropriate network virtualisation and address translation technologies are used. Cloud technologies provide a virtualisation platform for IT and network services and allow for the entire infrastructure instantiation together with related protocols and core infrastructure services related to control and management functions.

2.2 ITU-T Focus Group on Cloud Computing

The ITU-T Focus Group on Cloud Computing (FG-Cloud) [14] was established to identify the telecommunication aspects, i.e. the transport via telecommunications networks, security aspects of telecommunications, service requirements, etc., in order to support cloud services/applications and suggest the further studies and ITU-T standardization activities.

As a result of its chartered operation in 2010-2011, the FG-Cloud published the Technical Report (Part 1 to 7) [15] that presents taxonomies, use cases, functional, cloud infrastructure and reference architecture definition, cloud security. The reports also analyse the cloud technology benefits from telecommunication perspectives and discuss scenarios with inter-cloud peering, federation and brokering.

2.3 NIST Cloud Computing related standards

NIST is active in fostering cloud computing practices that support interoperability, portability, and security requirements that are appropriate and achievable for important usage scenarios. Since first publication of the currently commonly accepted NIST Cloud definition in 2008, NIST is leading wide internationally recognised activity on defining conceptual and standard base in Cloud Computing, which has been resulted in publishing the following documents that create a solid base for cloud services development and offering:

- NIST SP 800-145, A NIST definition of cloud computing[1]
- NIST SP 500-292, Cloud Computing Reference Architecture, v1.0 [2]

- DRAFT NIST SP 800-146, Cloud Computing Synopsis and Recommendations [16]
- NIST SP500-291 NIST Cloud Computing Standards Roadmap [17]

NIST SP 800-145 document defines Cloud Computing in the following way:
"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling. rapid elasticity, measured Service), 3 service/provisioning models. (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)), 4 deployment models (public, private, community, hybrid clouds)."

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

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

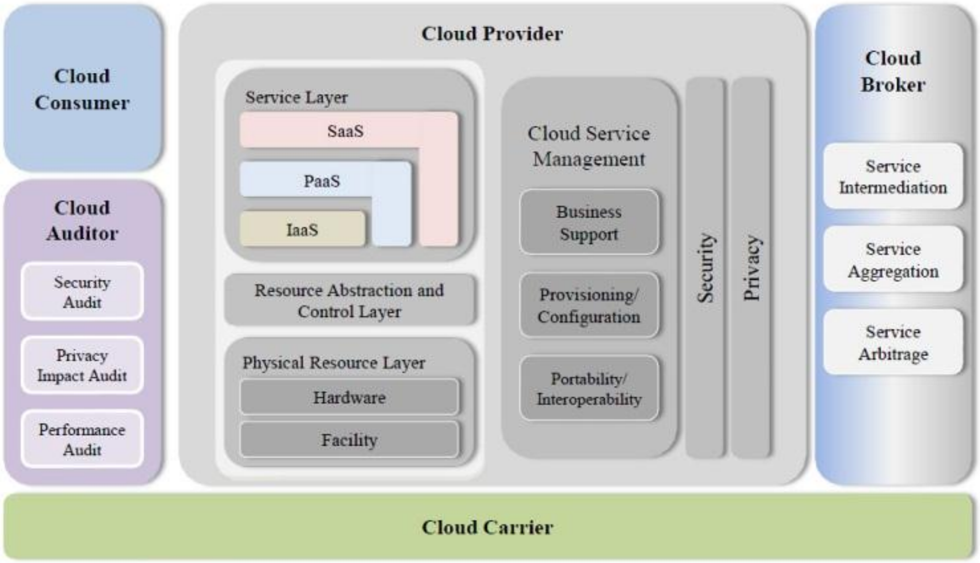


Figure 1. NIST Cloud Computing Reference Architecture (CCRA) [2]

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

2.4 Extending Cloud definition and CCRA for ICA

NIST CCRA and Cloud Computing definition are well suited for describing service and business or operational relations, however it has limited applicability for design purposes and defining basic functional components and related interfaces between component services and functional layers.

Despite that the recently published CCRA includes Cloud Carrier as representing 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 IaaS cloud service model doesn't include explicitly provisioning of the controlled network services and infrastructure. The reason for this is that cloud computing has been developed primarily for provisioning storage and computing resources and in assumption that network connectivity is provided as ubiquitous Internet connectivity. However, this situation presents serious limitations for large scale use of cloud in enterprise applications that require guaranteed network connectivity QoS and low network latency, in particular.

Another limitation of the current CCRA is that it is not suitable for defining required security infrastructure and its integration with main Cloud services or infrastructure that can be potentially multilayer and multi-domain.

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

- Define layered cloud services model that is suitable for defining main inter-layer and inter-service (functional) interfaces
- Define resources and services virtualisation as one of cloud features (where virtualisation includes resources abstraction, pooling, composition, instantiation, orchestration, and lifecycle management)
- Include improved network services definition capable of provisioning required QoS and allowing control from user run applications.
- Define infrastructure services as a new type of services that include the following attributes/features:
    - Topology describing computing, storage resources and interconnecting them network infrastructure
    - Infrastructure/topology description format that allows topology transformation operations for infrastructure control and optimization (e.g., homomorphic, isomorphic, QoS, energy aware etc.)

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

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

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

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

3 General use cases for ICA

The three basic use cases for Intercloud Architecture can be considered: (1) Enterprise IT infrastructure migration to cloud and evolution that will require both integration of the legacy infrastructure and cloud based components, and move from general cloud infrastructure services to specialised private cloud platform services; (2) large project-oriented scientific infrastructures including dedicated transport network infrastructure that need to be provisioned on-demand [18]; (3) IT infrastructure disaster recovery that requires not only data backup but also the whole supporting infrastructure restoration/setup on possibly new computer/cloud software or hardware platform. The networking research area itself introduces another use case for wide spread “cloud + network” infrastructure to support small and medium scientific experiments for testing new protocols and network dynamics that are too small for super computers but too big for desktop systems. All use cases should allow the whole infrastructure of computers, storage, network and other utilities to be provisioned on-demand, physical platform independent and allow integration with local persistent utilities and legacy services and applications.

Figures 2 illustrates the typical example of building e-Science or enterprise collaborative infrastructure based on the defined scientific or enterprise workflow that includes campus/enterprise proprietary infrastructure and cloud based computing and storage resources, instruments, visualization system, interconnecting network infrastructure, and users represented by user clients.

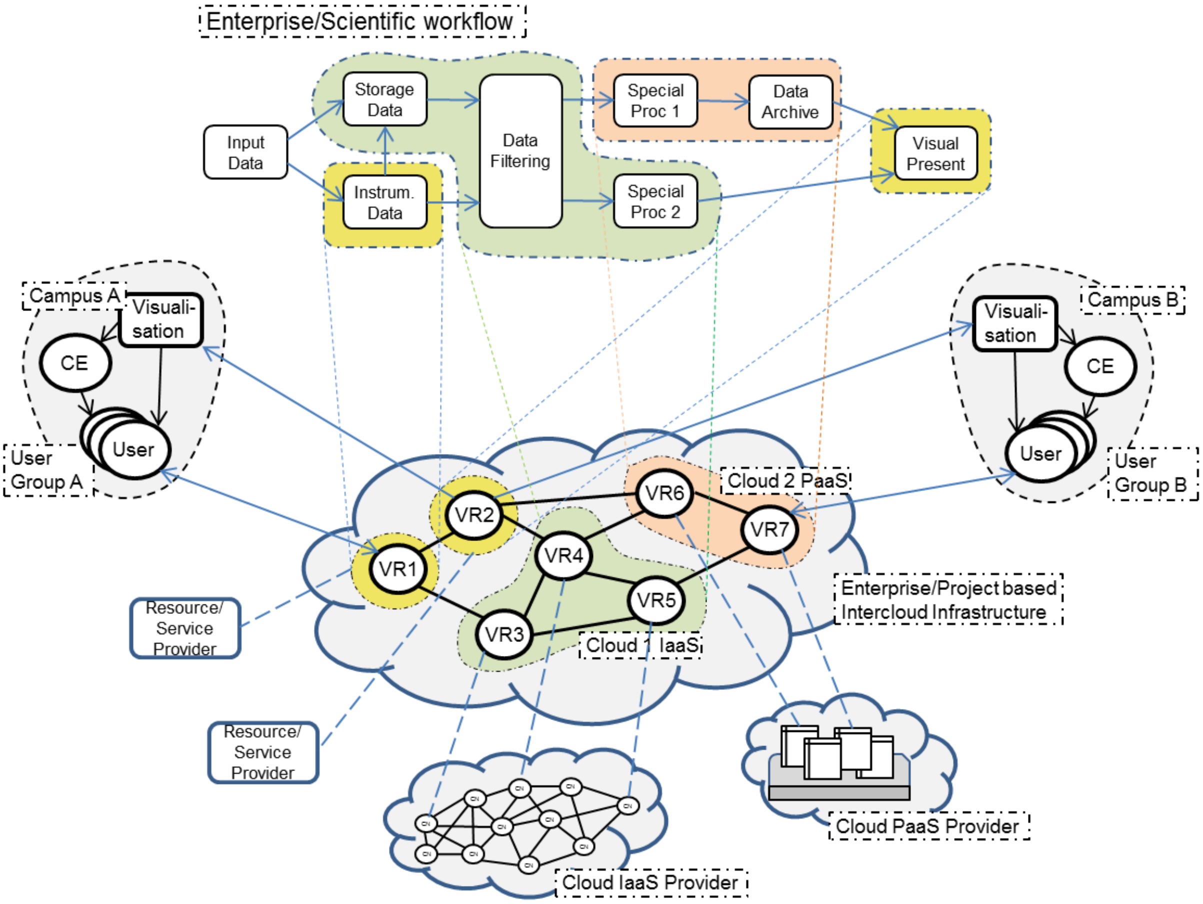


Figure 2. Enterprise or project oriented collaborative cloud based infrastructure including IaaS (VR3-VR5) and PaaS (VR6, VR7) cloud infrastructure segments, separate virtualised resources or services (VR1, VR2) and two interacting campuses A and B.

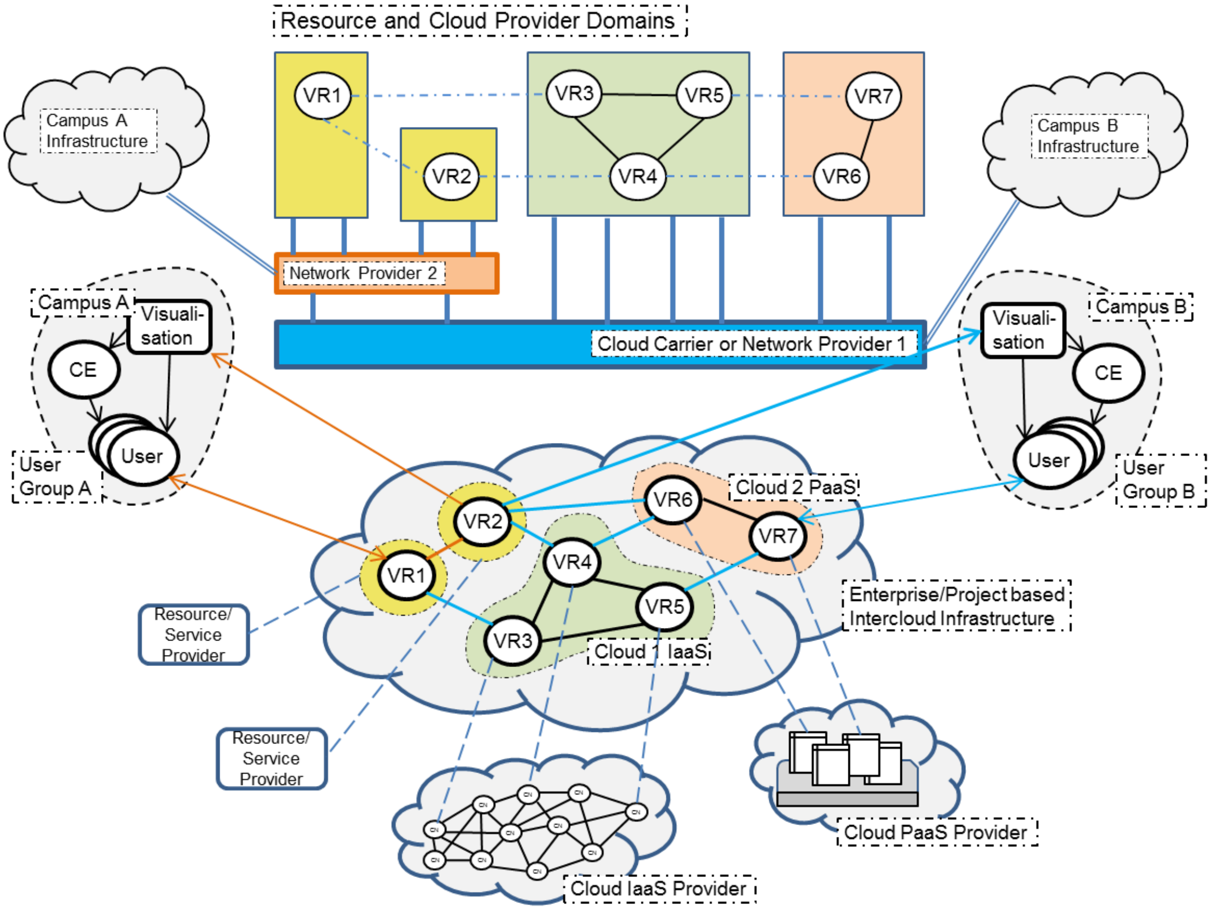


Figure 3. Required network interconnecting infrastructure that can be provided either single Cloud Carrier or together with the regular network provider.

The figures also illustrates a typical case when two different types of cloud services such as IaaS and PaaS based need to interoperate to allow consistent hybrid cloud infrastructure control and management.

4 ICA Definition and Requirements

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 ICA should address the following goals, challenges and requirements:

- ICA should support communication between cloud applications and services belonging to different service layers (vertical integration), between cloud domains and heterogeneous platforms (horizontal integration).
  - Be compatible and provide multi-layer integration of existing Cloud service models – IaaS, PaaS, SaaS and Apps clouds
- ICA should provide a possibility that applications could 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 signalling for better cloud services and network integration

- ICA should support cloud services/infrastructures provisioning on-demand and their lifecycle management, including composition, deployment, operation, and monitoring, involving resources and services from multiple providers.
- Provide a framework for heterogeneous inter-cloud federation
- Facilitate interoperable and measurable intra-provider infrastructures
- Explicit/Guaranteed intra- and inter-Cloud network infrastructure provisioning (as NaaS service model)
- Support existing Cloud Provider operational and business models and provide a basis for new forms of infrastructure services provisioning and operation

The proposed ICAF should use the reach experience of the Grid and Internet community and possibly following the same architecture patterns as Internet and Grid/OGSA, including provide functionalities for creating VO based infrastructures

Following the above requirements, we define the following complimentary 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 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, accounting. ICOF defines the basic roles, actors and their relations in sense of resources operation, management and ownership. ICOF requires support from and interacts with both ICCMP and ICFF.

At this stage of research, we define only multi-layer Cloud Services Model that can be built using modern SOA technologies re-factored to support basic cloud service models as discussed below and in the following section. Future research on ICCMP will try to leverage the technologies of User Programmable Private Networks (UPVN) [19], and general Internet technologies such as provided by CDN [11] and Generalized Multi-Protocol Label Switching (GMPLS) [20].

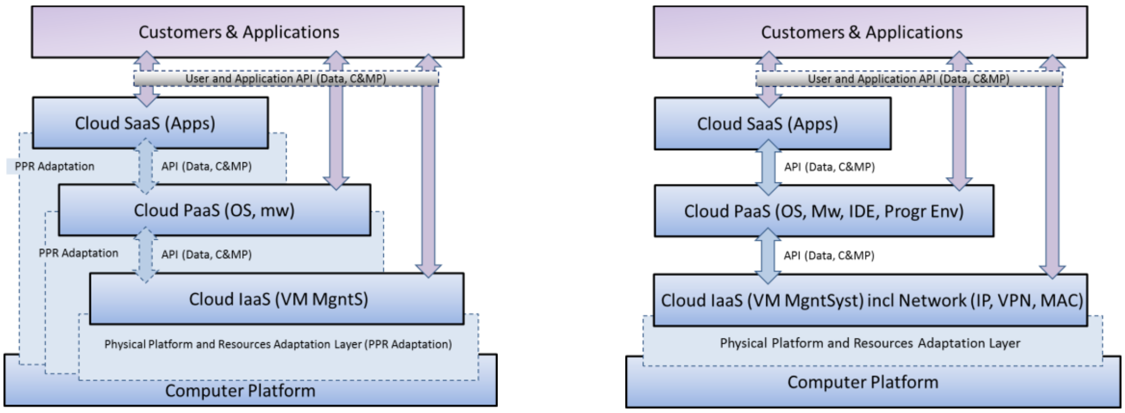
The ICFF will extend current cloud federation concept [21] and leverage existing platforms for federated network access and federated identity management widely used for multi-domain and multi-provider infrastructure integration [22, 23].

The ICOF definition will include analysis of the TeleManagement Forum (TMF) documents related to eTOM and Operational Support Systems [24], Service Delivery Framework (SDF) [25]. ICOF will also evaluate an approach for market-oriented allocation of resources in clouds [26]. A market concept and environment allows participants to locate providers or consumers with the right offers, while the banking system ensures the financial transactions pertaining to agreements and are carried out between participants. The role of the broker performs the same function in such a market as in any other market, and can provide substantial benefits for customers if the market and broker can operate in an automated fashion.

5 Multi-Layer Cloud Services Model

5.1 Moving from current proprietary cloud services model to layered model

Figure 5, a illustrates current relation between basic cloud service models IaaS, PaaS, SaaS that expose in most cases standard based interface to user services or applications but actually use proprietary interface to the physical provider platform. However in case of multiple heterogeneous cloud services integration in one integrated infrastructure or application (as illustrated by Figure 2), cloud services from different service models and layers need to interact. This motivates definition of the layered cloud services model with interlayer interfaces that is depicted on Figure 5, b.


Customers & Applications
User and Application API (Data, C&MP)
Cloud SaaS (Apps)
PPR Adaptation
API (Data, C&MP)
Cloud PaaS (OS, mw)
PPR Adaptation
API (Data, C&MP)
Cloud IaaS (VM MgntS)
Physical Platform and Resources Adaptation Layer (PPR Adaptation)
Computer Platform
Customers & Applications
User and Application API (Data, C&MP)
Cloud SaaS (Apps)
API (Data, C&MP)
Cloud PaaS (OS, Mw, IDE, Progr Env)
API (Data, C&MP)
Cloud IaaS (VM MgntSyst) incl Network (IP, VPN, MAC)
Physical Platform and Resources Adaptation Layer
Computer Platform

(a) Current relation between cloud service models (b) Proposed layered cloud service models

Figure 5. Migration from proprietary internal cloud platform interfaces to inter-layer interfaces.

Figure 6 illustrates the CSM layer 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 interface to user services or applications but actually use a proprietary interface to the physical provider 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. 6):

(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.

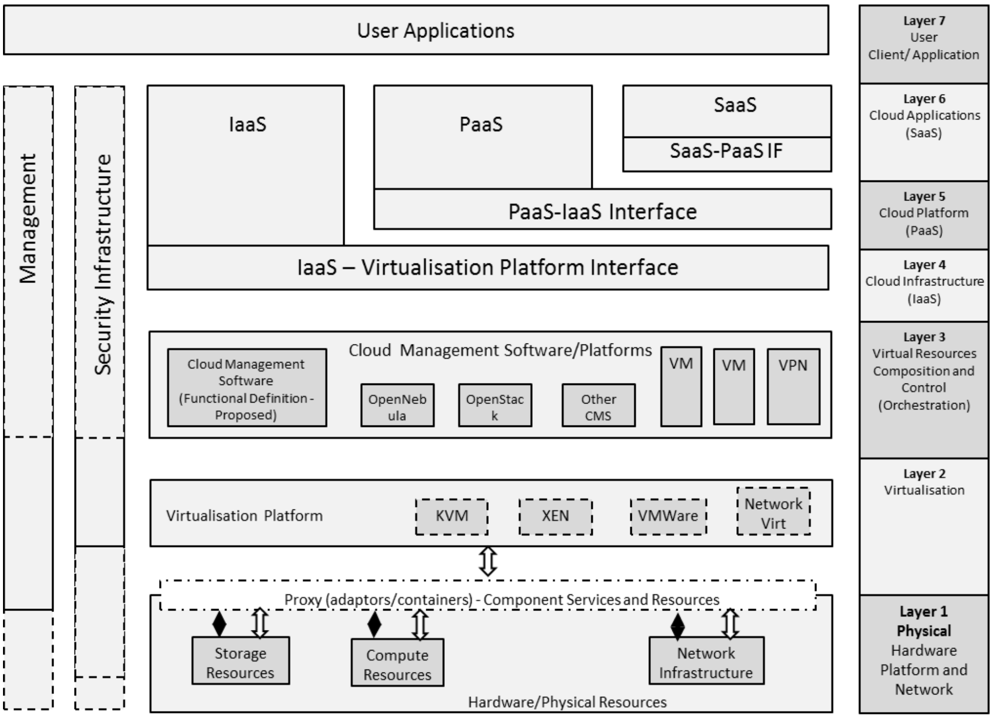

User Applications
Management
Security Infrastructure
IaaS
PaaS
SaaS
SaaS-PaaS IF
PaaS-IaaS Interface
IaaS – Virtualisation Platform Interface
Cloud Management Software (Functional Definition - Proposed)
Cloud Management Software/Platforms
OpenNebula
OpenStack
Other CMS
VM
VM
VPN
Virtualisation Platform
KVM
XEN
VMWare
Network Virt
Proxy (adaptors/containers) - Component Services and Resources
Storage Resources
Compute Resources
Network Infrastructure
Hardware/Physical Resources
Layer 7 User Client/ Application
Layer 6 Cloud Applications (SaaS)
Layer 5 Cloud Platform (PaaS)
Layer 4 Cloud Infrastructure (IaaS)
Layer 3 Virtual Resources Composition and Control (Orchestration)
Layer 2 Virtualisation
Layer 1 Physical Hardware Platform and Network

Figure 6. Reference Multilayer Cloud Services Model (CSM).

5.2 Definition of inter-layer interfaces

This section will provides suggestions about functional definition of inter-layer interfaces.
The section will investigated a possibility to re-use experiences from the GEYSERS architecture definition.

Figure 6 below illustrates a set of interfaces both that are currently defined for cloud services and their possible grouping to allow cross-layer communication in multilayer cloud services stack.

To be added.

6 Intercloud Control and Management Plane

This section will formulate requirements to Intercloud control and management protocols, functional components and interfaces. The main scenario should allow upper layer applications and processes to control underlying layers of the cloud infrastructure or platform. Figure 7 illustrate a scenario of IaaS and PaaS cloud domains communication that should use standard interfaces and proprietary interfaces.

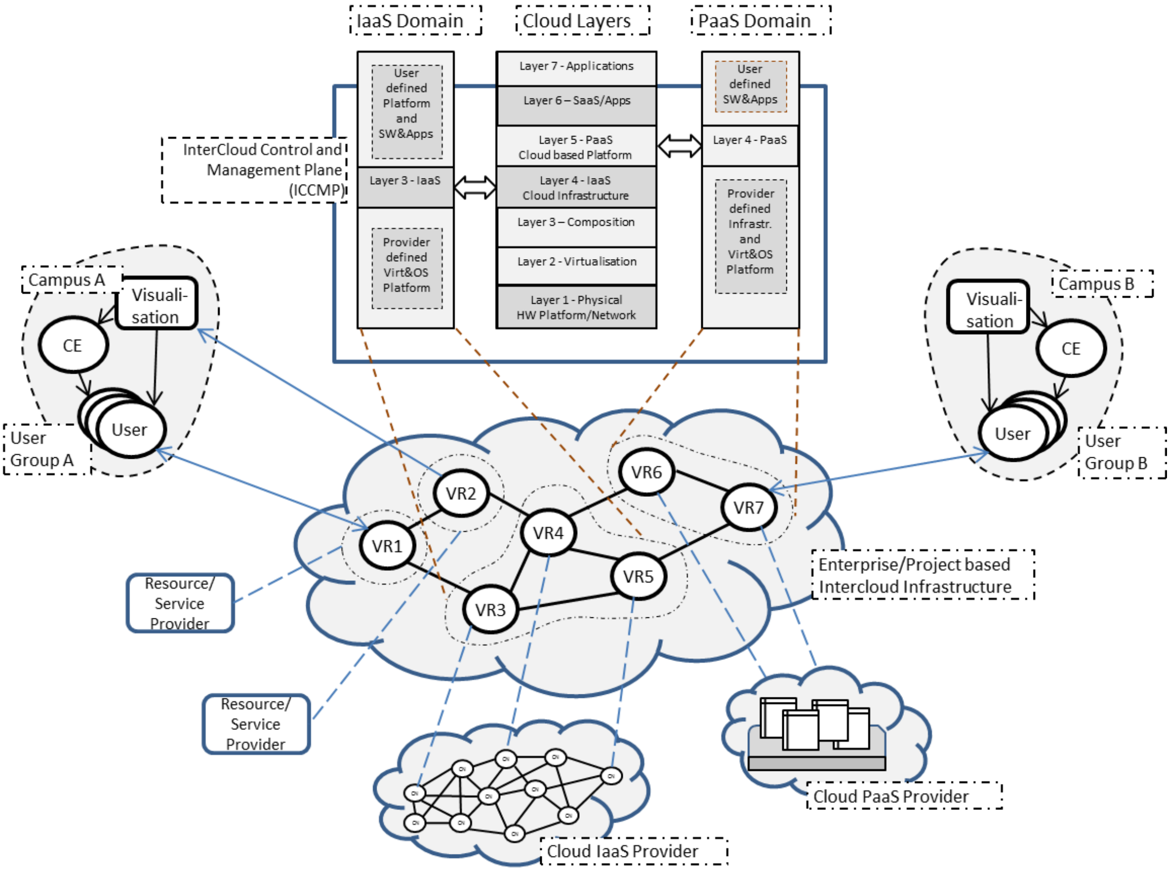

IaaS Domain
Cloud Layers
PaaS Domain
User defined Platform and SW&Apps
Layer 3 - IaaS
Provider defined Virt&OS Platform
Layer 7 - Applications
Layer 6 – SaaS/Apps
Layer 5 - PaaS Cloud based Platform
Layer 4 - IaaS Cloud Infrastructure
Layer 3 – Composition
Layer 2 - Virtualisation
Layer 1 - Physical HW Platform/Network
User defined SW&Apps
Layer 4 - PaaS
Provider defined Infrastr. and Virt&OS Platform
InterCloud Control and Management Plane (ICCMP)
Campus A
Visuali-sation
CE
User
User Group A
Campus B
Visuali-sation
CE
User
User Group B
VR1
VR2
VR3
VR4
VR5
VR6
VR7
Resource/ Service Provider
Resource/ Service Provider
Enterprise/Project based Intercloud Infrastructure
Cloud PaaS Provider
Cloud IaaS Provider

Figure 7. Intercloud Control and Management Plane providing single control and management domain to heterogeneous intercloud infrastructure.

Figure 8 illustrates a case when two different cloud/segments domain IaaS and PaaS need to interact allowing applications from one domain to control underlying virtualised resourceы 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.

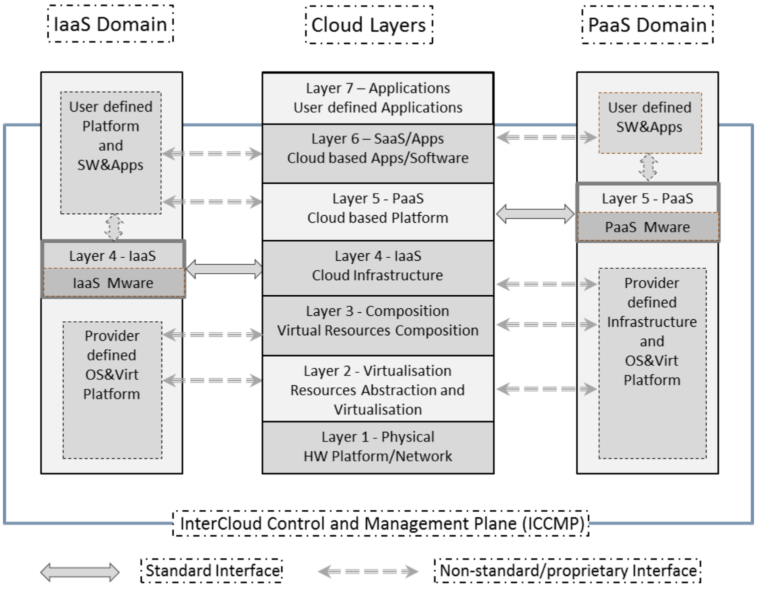

IaaS Domain
Cloud Layers
PaaS Domain
User defined Platform and SW&Apps
Layer 4 - IaaS
IaaS Mware
Provider defined OS&Virt Platform
Layer 7 – Applications User defined Applications
Layer 6 – SaaS/Apps Cloud based Apps/Software
Layer 5 - PaaS Cloud based Platform
Layer 4 - IaaS Cloud Infrastructure
Layer 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 8. Example of the IaaS and PaaS cloud domains communication that uses standard interfaces and proprietary interfaces

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
- Topology aware infrastructure management
- Configuration and protocols management.

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

7 Intercloud Federation Framework

Figure 9 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 provider (IdP)
- Trust manager/router
- Attribute/namespace resolver
- Intercloud gateway and/or attribute/namespace translator.

Correspondingly, the ICFF Interfaces should support the following functionalities:

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

The ICFF can be built using existing platforms for federated network access and federated identity management widely used for multi-domain and multi-provider infrastructure integration [21, 22, 23].

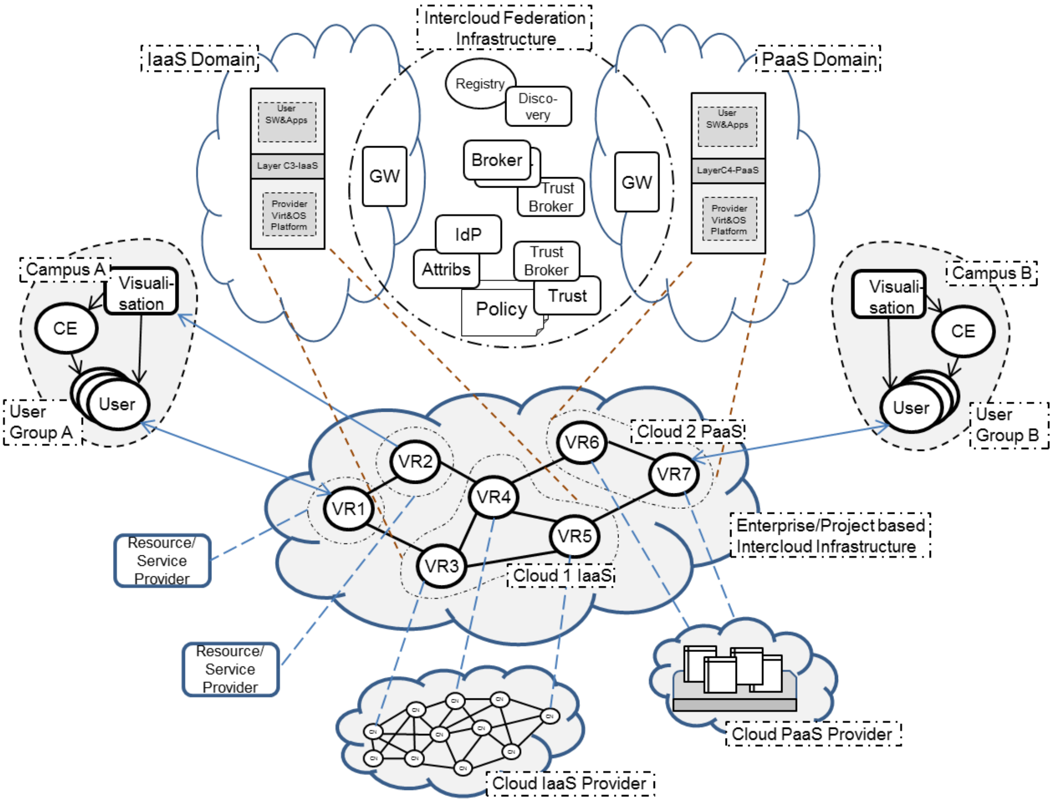


Figure 9. Main components of the Intercloud Federation Framework.

8 Intercloud Operation Framework

This section will discuss possible Intercloud infrastructures operation scenarios and provide formal models for describing relations between main actors in such scenarios.

8.1 Intercloud Operations Framework Model

Figure 10 illustrates relation between the main components involved into services delivery and management. 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

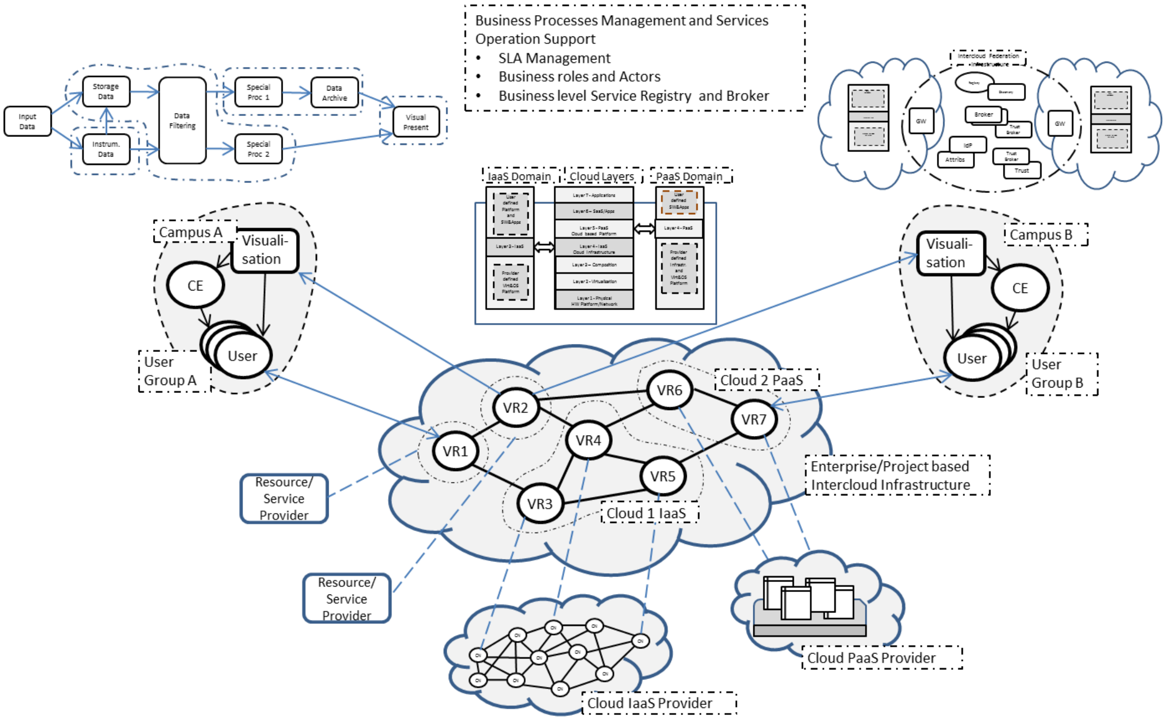


Figure 10. Intercloud Operation Framework providing a cloud services lifecycle and operation management

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

8.2 RORA Model

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

To be added by external contributors.

9 Abstract Model for Cloud based Infrastructure Services Provisioning

9.1 General model

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 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 includes functional components and services used to support normal operation of all mentioned actors. The Virtual Infrastructure Composition and Management (VICM) layer includes the Logical Abstraction Layer and the VI/VR Adaptation Layer facing correspondingly lower PIP and upper Application layer. VICM related functionality is described below and actually implements the proposed by authors Composable Services Architecture (CSA) [3, 18].

The proposed architecture is a SOA (Service Oriented Architecture) based and uses the same basic operation principle as known and widely used SOA frameworks, what also provides a direct mapping to the possible VICM implementation platforms such as Enterprise Services Bus (ESB) [27] or OSGi framework [28].

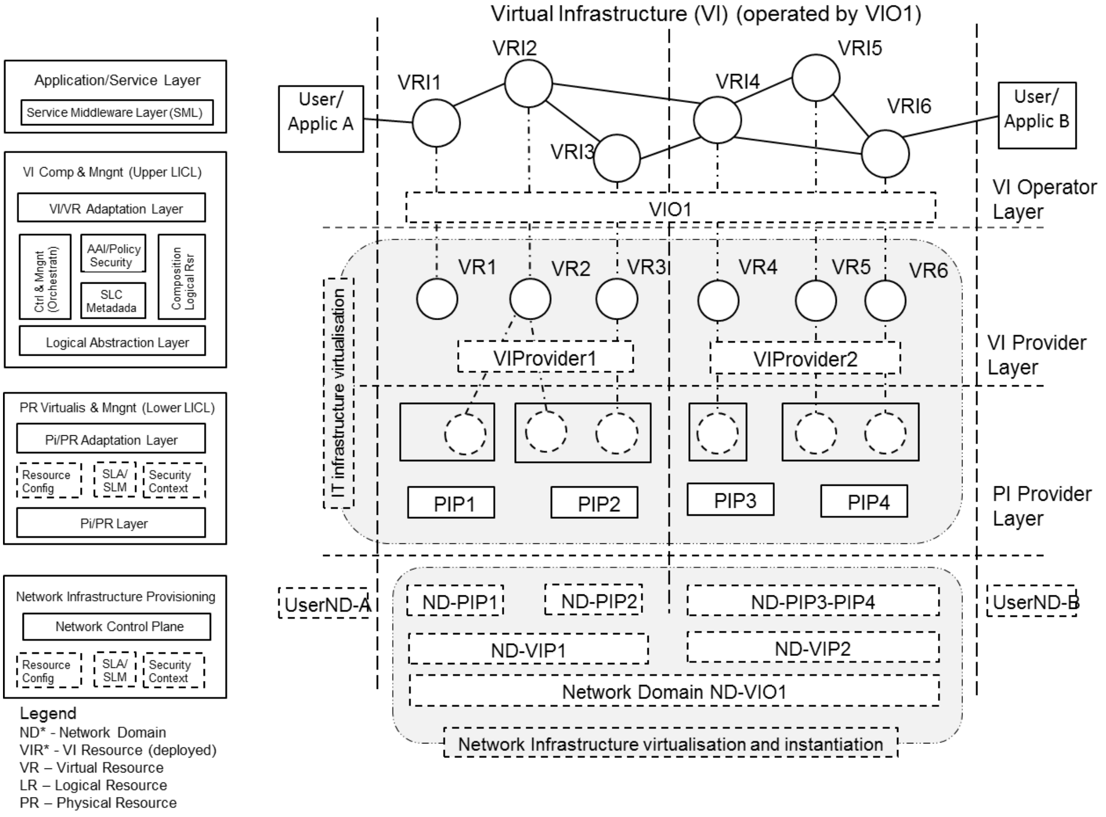


Figure 5. Main actors, functional layers and processes in on-demand infrastructure services provisioning

The infrastructure provisioning process, also referred to as Service Delivery Framework (SDF), is adopted from the TeleManagement Forum SDF [25] with necessary extensions to allow dynamic services provisioning. It includes the following main stages: (1) infrastructure creation request sent to VIO or VIP that may include both required resources and network infrastructure to support distributed target user groups and/or consuming applications; (2) infrastructure planning and advance reservation; (3) infrastructure deployment including services synchronization and initiation; (4) operation stage, and (5) infrastructure decommissioning. The SDF combines in one provisioning workflow all processes that are run by different supporting systems and executed by different actors.

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

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

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

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

9.2 Virtual Infrastructure Composition and Management Layer

The IaaS infrastructure services provisioning is the dynamic creation of an infrastructure consisting of different types of resources together with necessary (infrastructure wide) control and management planes, all provisioned on-demand. The proposed VICM is defined according to CSA and provides a framework for the design and operation of the composite/complex services provisioned on-demand. It is based on the component services virtualisation, which in its own turn is based on the logical abstraction of the (physical) component services and their dynamic composition.

Figure 6 shows the major functional components of the proposed VICM and their interactions. The central part of the architecture is the VICM middleware, which should ensure smooth service operation during all stages of the composable services lifecycle.

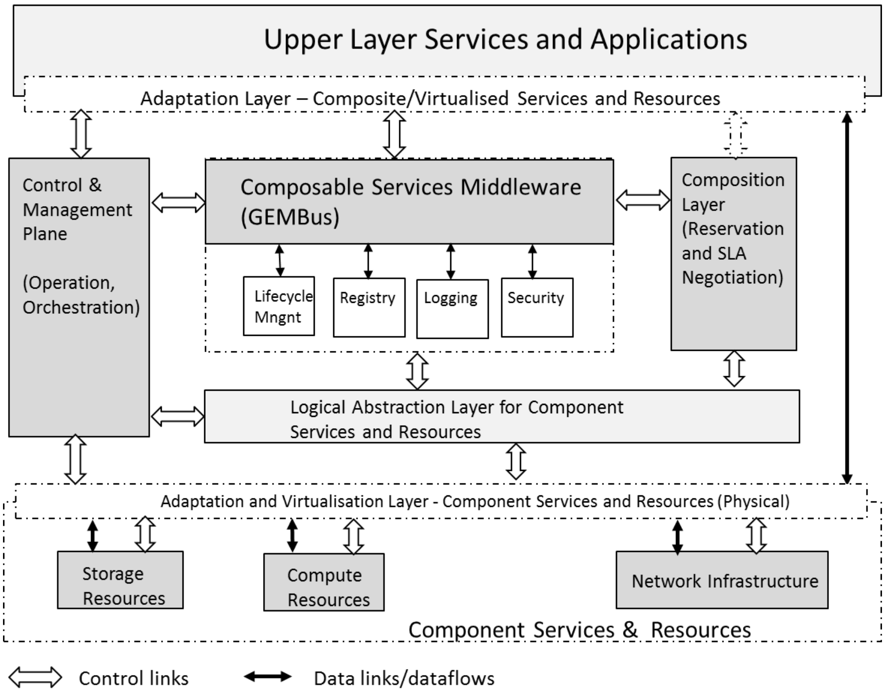

Upper Layer Services and Applications
Adaptation Layer – Composite/Virtualised Services and Resources
Control & Management Plane
(Operation, Orchestration)
Composable Services Middleware (GEMBus)
Lifecycle Mngnt
Registry
Logging
Security
Composition Layer (Reservation and SLA Negotiation)
Logical Abstraction Layer for Component Services and Resources
Adaptation and Virtualisation Layer - Component Services and Resources (Physical)
Storage Resources
Compute Resources
Network Infrastructure
Component Services & Resources
Control links
Data links/dataflows

Figure 6. Virtual Infrastructure Composition and Management (Orchestration) layer.

The VICM (VICM-MW) provides a common interaction environment for both (physical) component services and complex/composite services built with them. Besides exchanging messages, VICM-MW also contains/provides a set of basic/general infrastructure services required to support reliable and secure (composite) services delivery and operation:

- Service Lifecycle Management that stores the services metadata, including the lifecycle stage, the service state, and the provisioning session context.
- Registry service that contains information about all component services and dynamically created composite services. The Registry should support automatic services registration.
- Logging service that can be also combined with the monitoring service.
- Middleware Security services that ensure secure operation of the VICM/middleware.

Note, both logging and security services can also be provided as component services that are composed of other services in a regular way.

The VICM (and CSA) defines also Logical Abstraction Layer for component services and resources that is necessary part of creating services pool and virtualisation. Another functional layer is the Services Composition layer that allows presentation of the composed/composite services as regular services to the consumer.

The Control and Management plane provides necessary functionality for managing composed services during their normal operation. It may include Orchestration service to coordinate component service operation. In a simple case it may be standard workflow management system.

The VICM defines a special adaptation layer to support dynamically provisioned Control and Management plane interactions with the component services. These must implement adaptation layer interfaces that are capable of supporting the major VICM provisioning stages, in particular, service identification, services configuration and metadata including security context, and provisioning session management.

Security services are applied at multiple layers to ensure consistent security. Management functions are also present at all layers and can be seen as the management plane.

9.3 Infrastructure Services Modeling Framework

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

9.3.1 Resource Modeling

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

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

The ISMF is based on semantic web technology. This means that the description format will be based on the Web Ontology Language (OWL) [22]. This approach ensures the ISMF is extensible and allows for easy abstraction of resources by adding or omitting resource description elements. Furthermore, this approach has enabled us to re-use the Network Description Language [23] to describe infrastructure topologies.

9.3.2 Virtual Resource Lifecycle

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

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

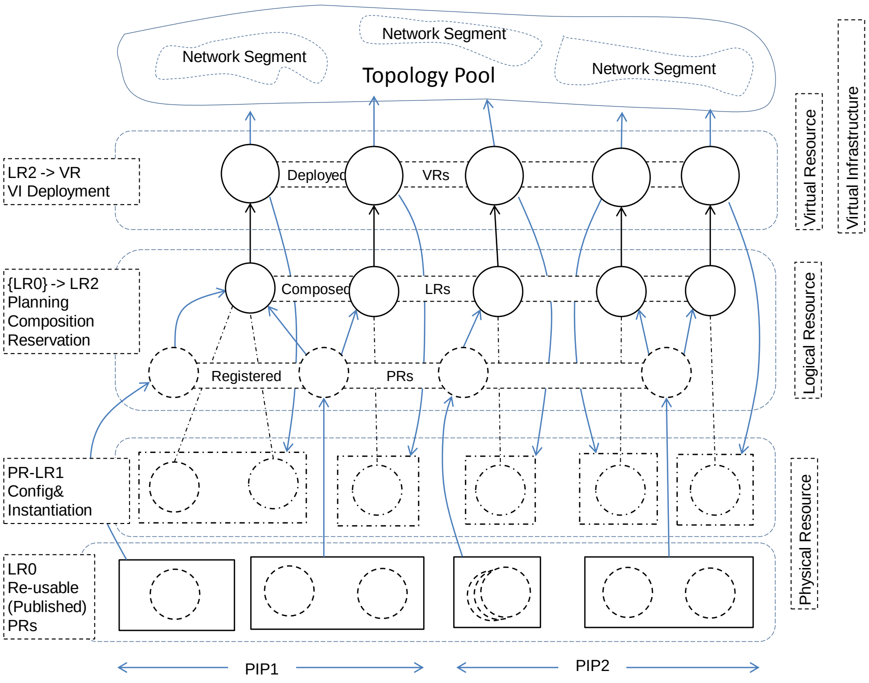


Figure 5. Relation between different resource presentations in relation to different provisioning stages.

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

10 Security Infrastructure for Federated Intercloud Infrastructure Services

This section will discuss numerous aspects related to building consistent security infrastructure for on-demand provisioned Intercloud infrastructure services and Intercloud applications

Operational security, certification/attestation and assurance issues will be also discussed.

However it is intended that the detailed security architecture and design will be published in another document.

11 Implementation Status and Suggestions

The presented Intercloud Architecture actually answers a number of identified issues in currently ongoing research and development projects such as GEYSERS [5] and GEANT3 Composable Services [4] that correspondingly develop Logical Infrastructure Composition Layer (LICL) and GEMBus (GEANT Multidomain Bus) as an implementation of the Composable Services Architecture [3].

GEYSERS architecture and LICL is currently being extended to provide a basis for cloud IaaS infrastructure services provisioning platform with the manageable network infrastructure services. A number of interfaces defined in GEYSERS [29] can be re-factored to more general CSM and ICCMP inter- and cross-layer interfaces. As a part of its security architecture the project also defined the Common Security Services Interface (CSSI) and security infrastructure for dynamically provisioned virtualised security services [30].

12 Summary and Future Development

This document presents the ongoing research on developing architecture and framework for dynamically provisioned and reconfigurable infrastructure services to support modern e-Science and high-technology industry applications that require both high-performance computing resources (provisioned as Grids or Clouds) and high-speed dedicated transport network.

The paper presents on-going research at the University of Amsterdam to develop the Intercloud Architecture (ICA) that should address problems with multi-domain heterogeneous cloud based applications integration and inter-provider and inter-platform interoperability.

Further research will be focused on definition of Intercloud Control and Management Plane (ICCMP) and Intercloud Federation Framework (ICFF) what will require analysis and evaluation both existing protocols and interfaces and those that are developed in GEYSERS and other cooperating projects such as CONTRAIL (http://contrail-project.eu/), SAIL (http://www.sail-project.eu/), and Mantychore (http://www.mantychore.eu/).

The presented research is planned to be contributed to a number of standardisation bodies where the authors are involved and play active role, in particular, the Open Grid Forum Research Group on Infrastructure Services On-Demand provisioning (ISOD-RG) [31], IETF on Cloud Architecture Framework definition [32], TeleManagement Forum on Cloud and Intercloud management aspects [33].

The proposed CSA is currently being implemented in the framework of the GEANT3 Project as an architectural component of the GEANT Multidomain service bus (GEMBus). The GEMBus extends the industry adopted Enterprise Service Bus (ESB) technology with the additional functionality to support multidomain services provisioning. The GEMBus infrastructure intended to allow dynamic composition of the infrastructure services to support collaboration of the distributed groups of researchers.

The future developments will include further development of all defined components and further definition of the security architecture and related security services and mechanisms to support creation of the dynamic security and trust associations.

Special attentions will be also given to the definition of the Infrastructure Services Modelling Framework, in particular, integrating related developments on defining common network and IT resources description framework.

13 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[15] ITU-T Focus Group on Cloud Computing. http://www.itu.int/en/ITU-T/focusgroups/cloud/Pages/default.aspx

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

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

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

[19] Demchenko, Y., J. van der Ham, M. Ghijsen, M. Cristea, V. Yakovenko, C. de Laat, "On-Demand Provisioning of Cloud and Grid based Infrastructure Services for Collaborative Projects and Groups",

The 2011 International Conference on Collaboration Technologies and Systems (CTS 2011), May 23-27, 2011, Philadelphia, Pennsylvania, USA

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

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

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

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

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

[25] TM Forum Frameworx. http://www.tmforum.org/frameworx/1911/home.html

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

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

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

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

[30] 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

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

[32] 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

[33] Cloud Reference Framework. Internet-Draft, version 0.2, December 27, 2011. [online] http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-02.txt

[34] TeleManagement Forum Cloud Management http://www.tmforum.org/community/groups/cloud_computing_services/wiki/cloud-management.aspx

Additional References

[35] ITU-T Recommendation Y.2011 (2004) - General principles and general reference model for Next Generation Networks.

[36] ITU-T Recommendation Y.2234 (09/2008) - Open service environment capabilities for NGN

[37] Securing the Cloud: Designing Security for a New Age, Dec. 10, 2009. [Online] Available at http://i.zdnet.com/whitepapers/ eflorida_ Securing_Cloud_Designing_Security_New_ Age.pdf

[38] Cloud Computing: Benefits, risks and recommendations for information security, Editors Daniele Catteddu, Giles Hogben, November 2009. [Online] Available at http://www.enisa.europa.eu/ act/rm/files/deliverables/cloud-computing-risk-assessment

[39] Amazon Web Services: Overview of Security Processes. November 2009. http://aws.amazon.com/security

[40] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, December 2009. [Online] Available at http://www.cloudsecurityalliance.org/csaguide.pdf

Appendix A ITU-T FG Cloud Technical Report Overview

This section will provide overview analysis of the FG Cloud Technical Report consisting of 7 parts:

Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high level requirements
Part 2: Functional Requirements and Reference Architecture
Part 3: Requirements and framework architecture of Cloud Infrastructure
Part 4: Cloud Resource Management Gap Analysis
Part 5: Cloud security
Part 6: Overview of SDOs involved in Cloud Computing
Part 7: Benefits from telecommunication perspectives