Chapter 1:
Characterizing Cloud Federation Approaches

Attila Kertesz

MTA SZTAKI, Budapest, Hungary, and

Software Engineering Department
University of Szeged, Szeged, Hungary

Abstract: Cloud Computing offers on-demand access to computational, infrastructure and data resources operated from a remote source. This novel technology has opened new ways of flexible resource provisions for businesses to manage IT applications and data responding to new demands from customers. In this chapter we give a general insight to the formation and interoperability issues of Cloud Federations that envisage a distributed, heterogeneous environment consisting of various cloud infrastructures by aggregating different IaaS provider capabilities coming from both the commercial and academic area. These multi-cloud infrastructures are also used to avoid provider lock-in issues for users that frequently utilize different clouds. We characterize and classify recent solutions that arose from both research projects and individual research groups, and show how they attempt to hide the diversity of multiple clouds and form a unified federation on top of them. Since they still need to cope with several open issues concerning interoperability, we provide guidelines to address related topics such as service monitoring, data protection and privacy, data management and energy efficiency.

Keywords: Cloud computing, Cloud Federation, Inter-Cloud, Interoperability, Data protection, Energy efficiency, IaaS.

1.1 Introduction

Cloud Computing is a diverse research area that encompasses many aspects of sharing software and hardware solutions, including computing and storage resources, application runtimes or complex application functionalities. The concept of Cloud Computing has been pioneered by commercial companies with the promise to allow elastic construction of virtual infrastructures, which attracted users early on. Its technical motivation has been introduced in [1][12]. Cloud solutions enable businesses with the option to outsource the operation and management of IT infrastructure and services, allowing the business and its employees to concen-

trate on their core competencies. As new products and technologies are offered in the near future, Gartner estimates till 2015 that $112 billion will be spent by businesses and individuals on Cloud Computing offerings from service providers such as Amazon, IBM and Microsoft [10].

In this chapter first we gather relevant architectural views of Clouds to give an insight where interoperation could be enabled to form federations, then we focus on and characterize existing solutions of Cloud Federations that envisage a distributed, heterogeneous environment consisting of various cloud infrastructures by aggregating different IaaS provider capabilities coming from both the commercial and academic area. Nowadays, cloud providers operate geographically diverse data centers as user demands like disaster recovery and multisite backups became widespread. These techniques are also used to avoid provider lock-in issues for users that frequently utilize multiple clouds. By this work we aim at revealing the important properties and capabilities of recent cloud reports and solutions dealing with federations. These approaches try to hide the diversity of multiple clouds and form a unified federation on top of them. Today's large systems need new, interoperable approaches to allow their efficient operation in terms of cost, energy consumption and balanced resource utilization, which have also been emphasized by the European Commission [5]. Therefore we also highlight the open issues concerning the interoperability of the participants of these federative approaches, such as service monitoring, data protection and privacy, data management and energy efficiency. Finally, we provide hints where future research should be driven in order to achieve the final goal of interoperable Cloud Federations.

The remainder of this chapter is as follows: Section 1.2 introduces and analyzes the architectural views of standardization bodies and relevant projects, while Section 1.3 summarizes and classifies state-of-the-art approaches aiming at Cloud federations. Section 1.4 introduces four relevant interoperability research issues of federations with possible solutions towards practical realizations. Finally Section 1.5 summarizes and concludes the chapter.

1.2 Architectural and deployment models of Clouds

In this section we gather the relevant views on the architectural and deployment models of Clouds defined and published by standardization bodies from all around the world and by corresponding European research projects.

1.2.1 Definitions of standardization bodies

The view of the European Commission

An expert group set up by the European Commission published their view on Cloud Computing in [5][13]. These reports categorize Cloud architectures into five groups, as shown in Figure 1.1. Private Clouds (i) consist of resources managed by an infrastructure provider (IP) that are typically owned or leased by an enterprise from a service provider (SP). Usually, services with "Cloud-enhanced" features are offered, therefore this group includes Software as a Service (SaaS) solutions like eBay [14]. Public Clouds (ii) offer their services to users outside of the company and may use Cloud functionality from other providers. In this solution enterprises can outsource their services to such Cloud providers mainly for cost reduction. Examples of these providers are Amazon [15] or Google Apps [16]. Hybrid Clouds (iii) consist of both private and public Cloud infrastructures to achieve a higher level of cost reduction through outsourcing by maintaining the desired degree of control (e.g., sensitive data may be handled in private Clouds). The report states that hybrid Clouds are rarely used at the moment. In Community Clouds (iv) different entities contribute with their (usually small) infrastructure to build up an aggregated private or public Cloud. Smaller enterprises may benefit from such infrastructures, and a solution is provided by Zimory [17]. Finally Special Purpose Clouds (v) provide more specialized functionalities with additional, domain specific methods, such as the distributed document management by Google's App Engine. This group is an extension or a specialization of the previous Cloud categories.

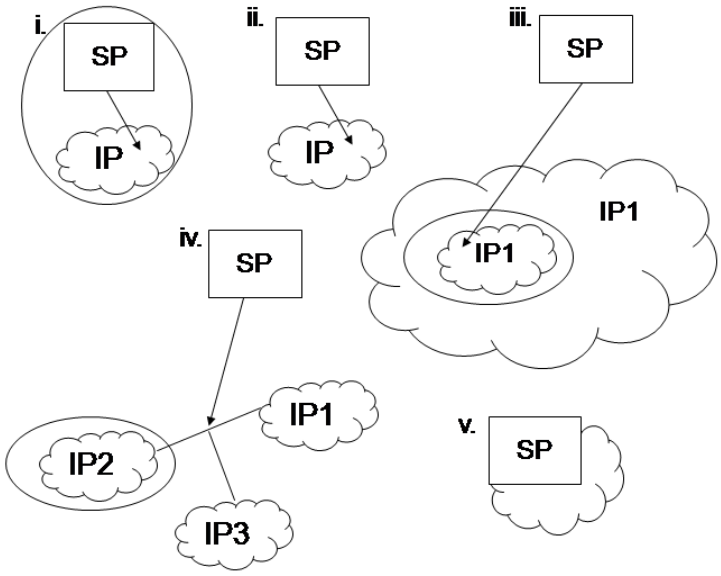

Figure 1.1: Cloud Architectures derived from the Cloud Computing Expert Working Group report

The view of ENISA

The European Network and Information Security Agency (ENISA) differentiates between four architectures [32], which are shown in Figure 1.2. A Public Cloud (i) is a publicly-available infrastructure to which any organization may subscribe and use (also called as service consumers (SC)). Private Clouds (ii) offer services built on Cloud Computing principles, but accessible only within a private network. Partner Clouds (iii) are operated by a provider to a limited and well-defined number of parties. Finally, a Cloud Federation (iv) may be built up by aggregating two or more Clouds.

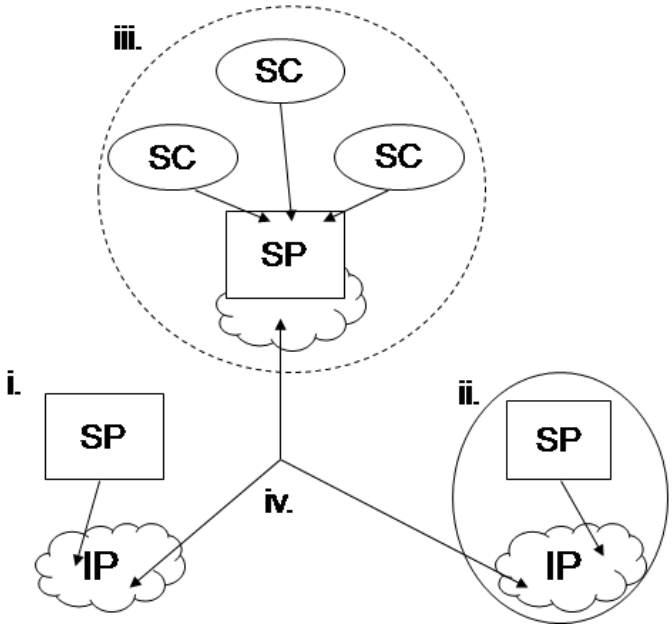

Figure 1.2: Cloud Architectures derived from ENISA reports

Cloud Architectures defined by NIST

The National Institute of Standards and Technology (NIST) defines four deployment models [7][8] depicted in Figure 1.3. According to their definitions, a Private Cloud (i) is an infrastructure operated solely for an organization that may be managed by either the organization or a third-party and located locally or remotely. A Community Cloud (ii) is shared by several organizations, and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by organizations or third parties, and may exist on premises or off premises. A Public Cloud

infrastructure (iii) is made available to the general public or a large industry group, and is owned by an organization selling Cloud services. Finally, a Hybrid Cloud (iv) is a composition of two or more Clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load balancing between Clouds).

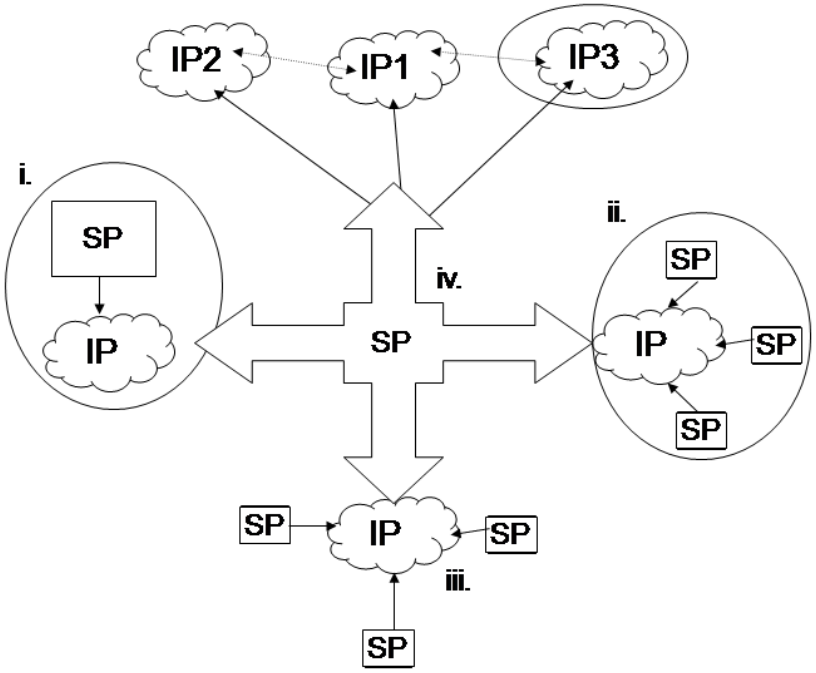

Figure 1.3: Cloud deployment models of NIST

The Cloud Computing Use Case Discussion Group [2] adopts the NIST models. They extend the view on Hybrid Clouds by stating that "multiple Clouds work together, coordinated by a Cloud broker that federates data, applications, user identity, security and other details". Though a brokering mechanism is needed for federating Clouds, no specific guidelines are given how to achieve this.

The view of DMTF

The Distributed Management Task Force (DMTF) Open Cloud Standards Incubator view [3] has also adopted the NIST models and defined different scenarios showing how Clouds may interoperate (depicted in Figure 1.4). These scenarios explain how data centers interact with Cloud providers and differentiate three cases:

- If a datacenter, run by Service Provider 1 (SP1) and hosted by Infrastructure Provider 1 (IP1), exceeds the available capacity limits then IP2 provides extra computing capacity for IP1 and SP1 is unaware of this provisioning.
- In a multiple Cloud scenario, SP1 may operate services in both IP1 and IP3 Clouds, therefore a datacenter may request services from both providers since they may support different services or Service-level Agreement (SLA) parameters.
- A provider may act as a Cloud broker to federate resources from other providers (e.g., IP1 and IP2) to make them available to its consumers transparently without using any of its own resources.

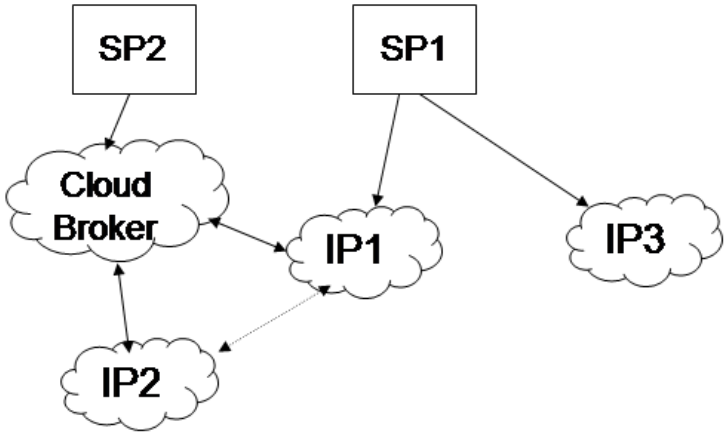

Figure 1.4: Cloud architectures by DMTF

1.2.2 Cloud models in European research projects

The view of OPTIMIS

The OPTIMIS project [9] identified that commercial solutions in the field of Cloud Computing have mainly focused on providing functionalities at levels close to the infrastructure, and higher-level solutions, like Platform as a Service (PaaS) environments are limited to a single infrastructure provider. Their goal is to build an improved cloud service ecosystem that supports higher-level concerns and non-functional aspects to achieve a wider adoption of Cloud Computing. The project follows a holistic approach for multiple coexisting cloud architectures and they target cloud service life-cycle optimization including cost, trust, risk and economic goals. They also plan to enable market-oriented multi-cloud architectures with clarified legislative background. The architectural views of the OPTIMIS project [4] are shown in Figure 1.5. The project has three basic architectural scenarios. In a

Federated Cloud Architecture (i), a Service Provider (SP) assesses an Infrastructure Provider (IP). IPs can share resources among each other. In a Multi-Cloud Architecture (ii), different infrastructure providers are used separately by a service provider. Finally in a Hybrid Cloud Architecture (iii), a Private Cloud (PC) is used by the SP, which can utilize resources of different IPs.

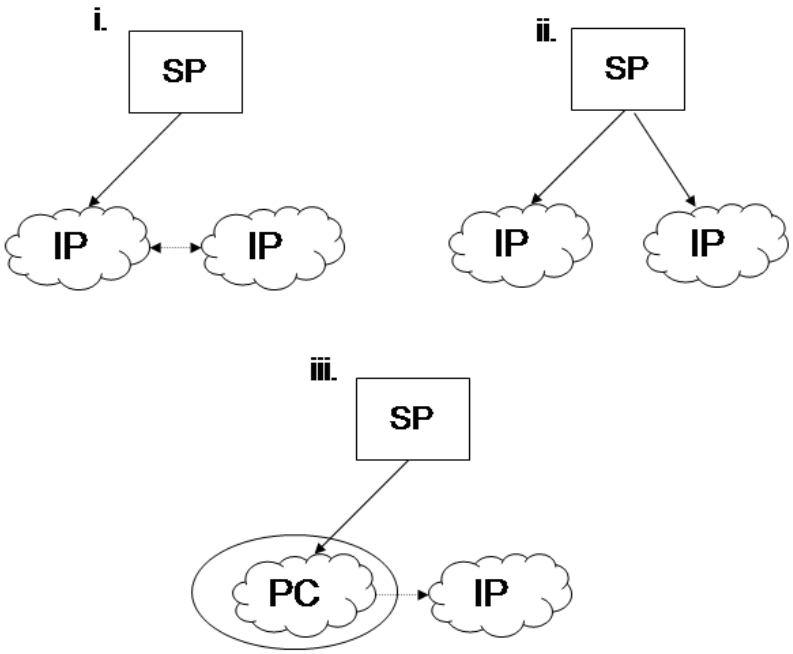

Figure 1.5: The OPTIMIS cloud architectures

The view of Reservoir

The Reservoir project [11] claims that small and medium Cloud providers cannot enter the Cloud-provisioning market due to the lack of interoperability between Clouds. Their approach is exemplified by the electric grid approach: "for one facility to dynamically acquire electricity from a neighboring facility to meet a spike in demand". Disparate datacenters should be federated in order to provide a "seemingly infinite service computing utility". Regarding the architectural view, a Reservoir Cloud consists of different Reservoir Sites (RS) operated by different IPs. Each RS has resources that are partitioned into isolated Virtual Execution Environments (VEE). Service applications may use VEE hosts from different RSs simultaneously. Each application is deployed with a service manifest that formally defines its SLA contract. Virtual Execution Environment Managers (VEEM) interact with VEEs, Service Managers and other VEEMs to enable federations to be

formed. A VEEM gathers interacting VEEs into a VEE group that serves a service application. This implies that a Reservoir service stack has to be present on the resources/sites of IPs. Their specialized Cloud architecture is depicted in Figure 1.6.

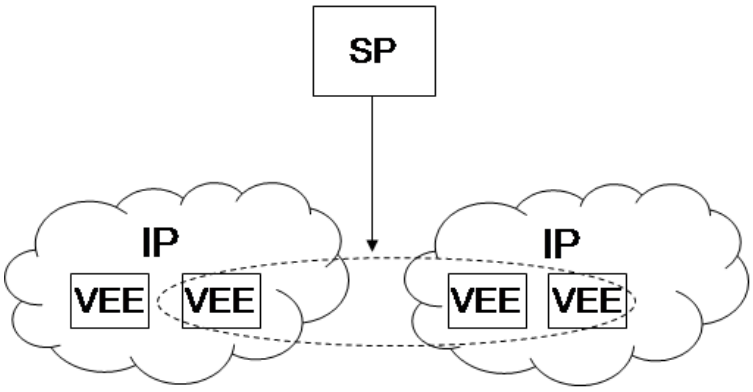

Figure 1.6: The Reservoir cloud architecture

The view of Contrail

The Contrail project [21] proposes an SLA-centered federated approach for Clouds. Its goal is to minimize the burden on the user with eliminating provider lock-in by exploiting resources belonging to different cloud providers regardless the kind of technology they use, and to increase the efficiency of using Cloud platforms by performing both a vertical and a horizontal integration. It follows an open-source approach toward technology and standards, and supports user authentication and applications deployment by providing extended SLA management functionalities. Its federation architecture, shown in Figure 1.7, acts as a bridge among the users and the cloud providers, and has three layers. The top, Interface layer provides ways to interact with the federation. It gathers requests from users and other Contrail components that rely on the federation functionalities. The middle, Core layer contains modules that fulfill the functional and non-functional requirements of the federation. The federation runtime manager operates in this layer, which uses a set of heuristics that consider different aspects to govern the federation, such as to minimize economical cost and to maximize performance levels.

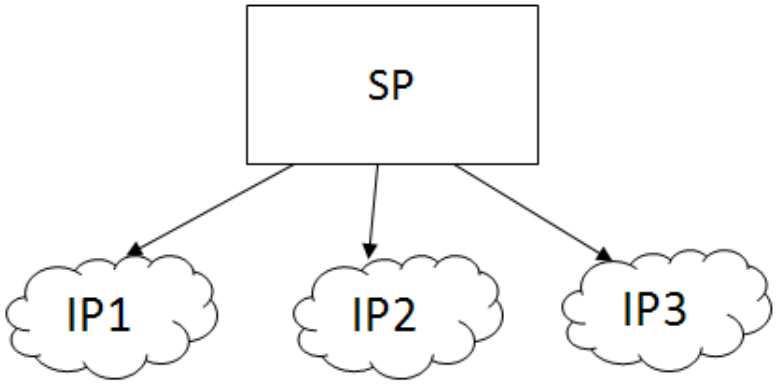

Figure 1.7: Contrail architecture

The view of BonFIRE

The BonFIRE project [19] aims at exploring the interactions between novel service and network infrastructures. The project was focused on the extension of current cloud offerings towards a federated facility with heterogeneous virtualized resources and best-effort Internet interconnectivity. They have developed a set of procedures to interconnect a multi-cloud environment with advanced facilities for controlled networking. These procedures enable the provisioning of customized network functions and services in support of experiments running in a multi-cloud test-bed. Their aim is to federate three advanced networking facilities within the BonFIRE multi-cloud environment: the interconnections with FEDERICA and GÉANT are already active, and OFELIA planned to be connected soon. The Bon-FIRE facility (shown in Figure 1.8) is composed of six geographically distributed cloud test-beds, located at EPCC, INRIA, HLRS, iMinds, HP and PSNC.

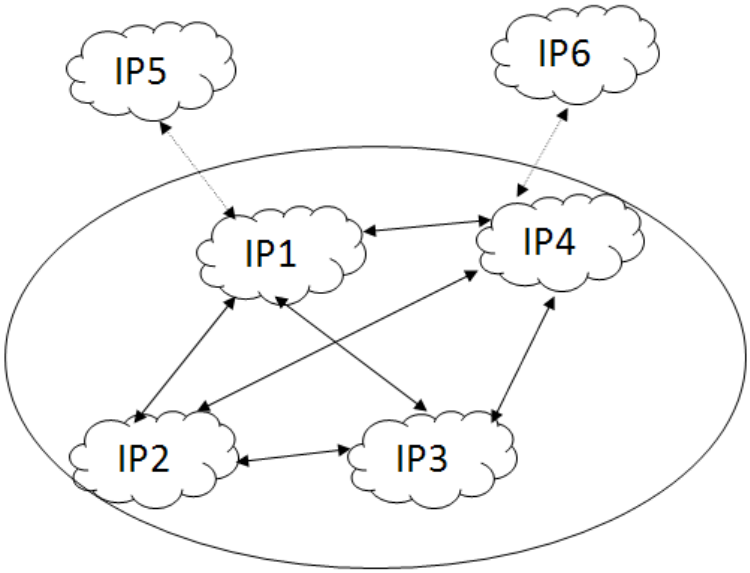

Figure 1.8: The BonFIRE facility

The view of mOSAIC

The mOSAIC project [20] offers the specification of service requirements in terms of a cloud ontology via an innovative API. The implementation of this approach will offer a higher degree of portability and vendor independence. It also provides application programming interfaces for building applications using services from multiple cloud providers and plans to realize a self-adaptive distributed scheduling platform composed of multiple agents implemented as intelligent feedback control loops to support policy-based scheduling and expose self-healing capabilities. They plan to foster competition between cloud providers by enabling the selection of best-fitting cloud services to actual user needs and efficiently outsource computations. In its hybrid cloud scenario they envision multiple clouds working together coordinated by a cloud broker that federates data, applications, user identity and security – shown in Figure 1.9.

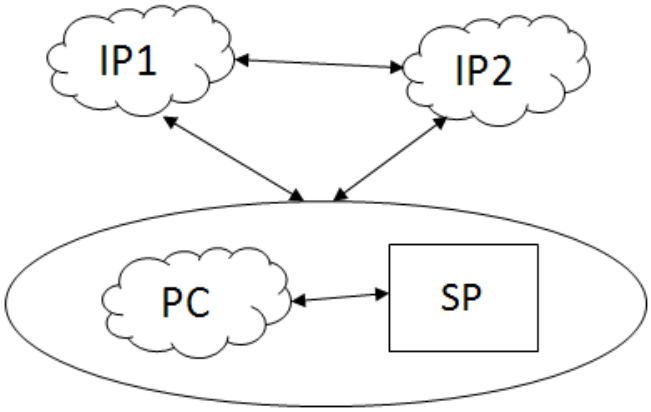

Figure 1.9: mOSAIC hybrid cloud architecture through APIs

The view of EGI Federated Cloud

The European Grid Infrastructure (EGI) is a federation of national and domain specific resource infrastructure providers, who wish to use virtualised management environments to improve the local delivery of services. Many of EGI's current and new user communities would also like to access the flexibility provided by virtualisation across the infrastructure resulting in a cloud-like environment. Federating these individual virtualised resources has been a major priority for EGI, therefore it has set up the Federated Clouds Task Force [22]. Its main objectives were to provide a guideline for its resource providers to securely federate and share their virtualised environments as part of the EGI production infrastructure, and to create a testbed to evaluate the integration of virtualised resources within the existing EGI production infrastructure for monitoring, accounting and information services. Their guidelines does not define what hypervisor the participating resource providers should use, and the federation adopts a set of well-defined functionalities and interfaces that every provider is free to implement independently. Currently there are 16 providers participating in the EGI Federated Cloud (FedCloud) testbed using OpenNebula, OpenStack and StratusLab. Their federated architecture is depicted in Figure 1.10. Currently the clouds of the participating infrastructure providers can be reached in a centralized way, and utilized separately.

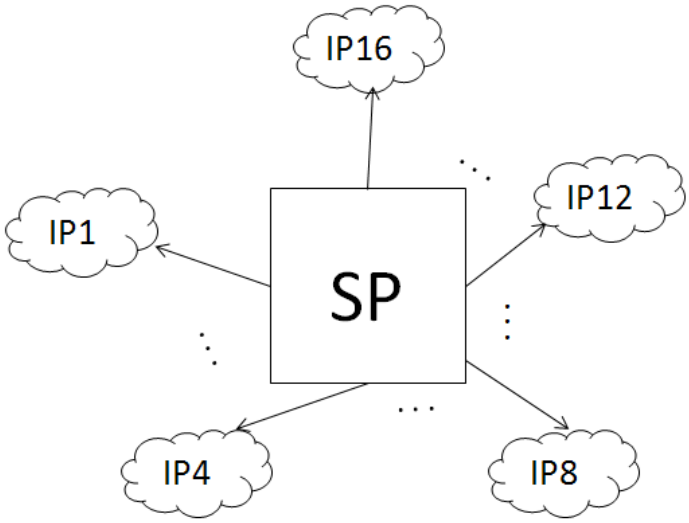

Figure 1.10: EGI Federated Cloud

Classification of research projects

In order to compare the previously introduced approaches, we have created a *classification of these views* concerning their abilities to form federations. We introduced *four categories* in this classification:

- Hierarchical type of federations: In this vision there is a usually centralized, higher level management service that is responsible for federation forming and the coordination. This type is also called as a "Multi-Cloud" approach in the literature [25].
- Horizontal type of federations: In this vision bi- or multi-lateral resource renting is the main goal of the participating providers, mainly for optimizing resource utilization and reducing operation costs. This type is generally named as "Federation" in the literature [25].
- Heterogeneity of participating providers: With this category we represent the variety of IaaS software stacks available in the federation (where "No" means that the same software stack need to be used in order to participate in a federation).
- Specialty of federation forming: Here we named one of the unique capabilities of the appropriate solution.

The actual categorization is shown in Table 1.1. The introduced categories reveal the most important properties of the surveyed solutions.

Table 1.1: Classification of federative approaches of research projects

	Hierarchical	Horizontal	Heterogeneity	Specialty
OPTIMIS [9]	X	-	Yes	Legislation awareness
Reservoir [11]	-	X	No	Reservoir service stack
Contrail [21]	X	-	Yes	SLA contracts
BonFIRE [19]	-	X	Yes	Controlled networking
mOSAIC [20]	-	X	Yes	Cloud ontology, API
EGI FedCloud [22]	-	X	Yes	Virtualised EGI environments

1.3 Inter-Cloud and Cloud federation approaches

Cloud federation refers to a mesh of cloud providers that are interconnected based on open standards to provide a universal decentralized computing environment where everything is driven by constraints and agreements in a ubiquitous, multi-provider infrastructure. Until now, the cloud ecosystem has been characterized by the steady rising of hundreds of independent and heterogeneous cloud providers, managed by private subjects, which offer various services to their clients. In this subsection next to the already overviewed research projects, we gather relevant federative approaches found in the literature. Cloud providers offering PaaS solutions may form "sub-federations" simultaneously to these approaches. Specific service applications may be more suitable for these provisions, and projects like Reservoir [11] and 4CaaSt [18] are working towards such a solution. Our considered federative works targets IaaS-type providers, e.g., RackSpace, the infrastructure services of Amazon EC2, and providers using Cloud middleware such as OpenNebula or Eucaliptus.

InterCloud vision

Buyya et al. [1] envision that one day Cloud Computing will be the 5th utility by satisfying the computing needs of everyday life. Their pioneer paper discusses the current trends in Cloud computing and presents candidates for future enhancements. They emphasize the market-oriented side of Clouds, and introduce a market-oriented cloud architecture, then discuss how global cloud exchanges could take place in the future. They further extended this vision by [24] suggesting a federation oriented, just in time, opportunistic and scalable application services provisioning environment called InterCloud. They envision utility oriented federated IaaS systems that are able to predict application service behavior for intelli-

gent down and up-scaling infrastructures. They list the research issues of flexible service to resource mapping, user and resource centric QoS optimization, integration with in-house systems of enterprises, scalable monitoring of system components. They present a market-oriented approach to offer InterClouds including cloud exchanges and brokers that bring together producers and consumers. Producers are offering domain specific enterprise Clouds that are connected and managed within the federation with their Cloud Coordinator component.

Cross-Cloud federation approach

Celesti et al. [31] proposed an approach for the federation establishment considering generic cloud architectures according to a three-phase model, representing an architectural solution for federation by means of a Cross-Cloud Federation Manager (CCFM), a software component in charge of executing the three main functionalities required for a federation. In particular, the component explicitly manages: (i) the discovery phase in which information about other clouds are received and sent, (ii) the match-making phase performing the best choice of the provider according to some utility measure and (iii) the authentication phase creating a secure channel between the federated clouds. These concepts can be extended taking into account green policies applied in federated scenarios.

Multi-Cloud approach

Bernstein et al. [23] define two use case scenarios that exemplify the problems of multi-cloud systems like (i) VM mobility where they identify the networking, the specific cloud VM management interfaces and the lack of mobility interfaces as the three major obstacles and (ii) storage interoperability and federation scenario in which storage provider replication policies are subject to change when a cloud provider initiates subcontracting. They offer interoperability solutions only for low-level functionality of the clouds that are not focused on recent user demands but on solutions for IaaS system operators.

FCM approach

In the Federated Cloud Management solution [6] interoperability is achieved by high-level brokering instead of bilateral resource renting – shown in Figure 1.11. Albeit this does not mean that different IaaS providers may not share or rent resources, but if they do so, it is transparent to their higher level management. Such a federation can be enabled without applying additional software stack for providing low-level management interfaces. The logic of federated management is moved to higher levels, and there is no need for adapting interoperability standards by the participating infrastructure providers, which is usually a restriction that some industrial providers are reluctant to undertake.

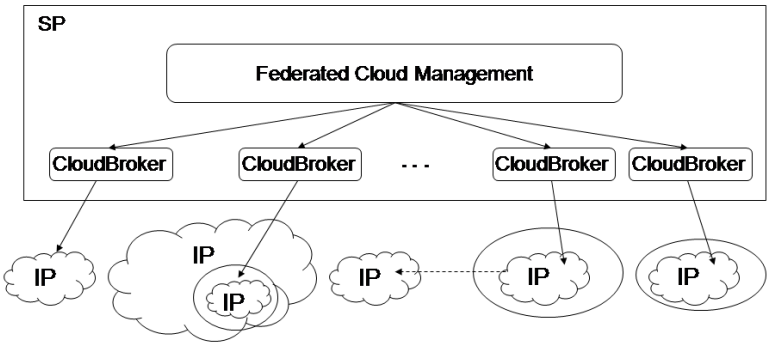

Figure 1.11: Federated Cloud Management Architecture

Classification of research approaches

In order to classify the relevant research directions addressing federations found in the literature, we use the same categorization as in Table 1.1. In this case we can also observe that both *hierarchical and horizontal federation types* are represented, and heterogeneity within the participating providers is only present in hierarchical solutions. While most of the projects considered in Section 1.2.2 applied the horizontal approach, smaller research groups are in favor of the hierarchical way. The motivation behind this observation is that research projects lasting for 3-4 years had the manpower to develop own interfaces to enable interoperation among the participating Cloud providers, and also had the ambitious aim to come up with a solution that could be standardized and used in industry later on. On the other hand, smaller research groups focused on approaches that utilize already existing standards to avoid provider lock-in, and to enable easier collaboration with industrial solutions.

Table 1.2: Classification of federative approaches of research papers

	Hierarchical	Horizontal	Heterogeneity	Specialty
InterCloud [1]	X	-	Yes	Market-oriented
Cross-Cloud [31]	-	X	Yes/No	Authentication
Multi-Cloud [23]	X	-	Yes	VM Mobility
FCM [6]	X	-	Yes	Meta-brokering

1.4 Interoperability issues of Cloud Federations

Not only the interchangeability of user applications in different clouds participating in a federation represents and open issue as a whole, but it also has several related interoperability problems concerning the management of such a large distributed ecosystem.

As we mentioned before, the European Commission has assigned an expert group to publish reports on future research challenges of Clouds [5][13]. In these reports they also performed a gap analysis of already existing commercial and academic solutions and highlighted the following topics that *need further research*:

- Manageability: Even though most Cloud solutions handle elasticity, intelligent methodologies are needed to reach optimal resource utilization.
- Data management: Most data flowing to or created in the Cloud need to be supported by meta-data information and new standards are needed to guarantee long-term storing and interoperable sharing among multiple providers.
- Privacy and security: Legislative issues of data distribution should be better addressed, and security holes during resource sharing among multiple tenants should be eliminated.
- Federation and interoperability: Proprietary data structures should be replaced by de facto standards, and new approaches are needed to ensure convergence towards real interoperability eliminating vendor lock-in.
- Virtualization and adaptability: Optimized resource scheduling solutions are needed considering cross-platform executions and migrations taking into account rapidly changing workloads.
- Programming models: Better control on data distribution should be achieved, and new means are needed to enable better application development and deployment.
- Economy: New scheduling policies are needed to enable green resource utilization, more efficient resource utilization with reduced power consumption.

By addressing many of these concerns, *we summarize four important research fields* that are necessary to be taken into account in building and operating Cloud Federations. These topics represent different facets of interoperability: (i) enhanced monitoring solutions are needed to enable optimized management of participating providers; (ii) legislative regulations need to be considered during multi-tenant data processing; (iii) sustainable and user-friendly data management solutions are needed through standard interfaces; and (iv) energy efficient resource management have to be enabled for future ecosystems.

1.4.1 Monitoring in Cloud Federations

Infrastructure as a Service cloud systems provide access to a remote computing infrastructure by allowing their users to instantiate virtual appliances on their virtualized resources as virtual machines. Nowadays, several IaaS systems co-exist, and they are independently offered by several public service providers or by smaller scale privately managed infrastructures. As we have seen before, to enable interoperability of multiple clouds, federations need to handle the differences of various cloud providers and have to negotiate user requirements with multiple parties. Federated clouds aim at supporting these users by providing a single interface on which they can transparently handle different cloud providers, as they would do with a single cloud system. Therefore it is essential to construct federated cloud systems in a way that they not only offer a single interface for their users, but also automatically manage virtual machines (VM) independently from the availably cloud systems.

An efficient cloud selection in a federated environment requires a cloud monitoring subsystem that determines the actual status of available IaaS systems. Since there is only limited monitoring information available for the users or higher-level managers in these clouds, there is a need for a sophisticated service monitoring approach to evaluate basic cloud reliability status, and to perform seamless service provisioning over multiple cloud providers in an interoperable way. We *exemplify such an extension to a federation* with our Federated Cloud Management solution, where we applied a web service monitoring approach to gather additional and more detailed service quality information from the participating cloud [26]. The FCM approach uses the Generic Meta-Broker Service as the entry point for the users of the cloud federation. This service selects the most suitable cloud provider to perform the service requests of the user by investigating the current state of the participating clouds according to the information stored in a generic service registry and the reliability metrics collected by the integrated SALMon service monitoring framework [33]. The participating clouds are managed by Cloud-Brokers that are capable of handling service requests and managing virtual machines within single IaaS cloud systems.

To enable the meta-brokering service to differentiate between cloud providers, we proposed to use a basic service that is used to cost effectively determine the important characteristics of the available VMs in the federation. As a result, the system is capable to evaluate and choose between both public and private clouds based on the same kind of metrics. We refer to this basic service as the Minimal Metric Monitoring Service (M3S), which is capable of measuring infrastructure reliability together with the integrated SALMon framework in public and private clouds. The M3S service is prepared to run in a virtual machine and it offers 3 methods to evaluate the basic capabilities of its hosting VM. SALMon uses the response times of these methods to express the reliability of the particular cloud that runs the M3S VM: it has (i) a generalized ping test to check the availability of the service; a (ii) CPU analyzer method that performs several mathematical calcula-

tions in a large loop over a predefined set of variables, consisting on integer and floating point numbers in order to determine the computational capability of a given VM; and finally (iii) bandwidth analyzer methods, which are used to compute the download and upload transfer speed of the system to determine its inbound and outbound data transfer capabilities.

Our investigations showed that both service reliability and responsiveness do vary over time and load conditions, and these measures can be used by our federated cloud management solution to select better execution environments for achieving a higher level of user satisfaction.

1.4.2 Data protection in Cloud Federations

Cloud Computing allows the outsourcing of computational power, data storage and other capabilities to a remote third-party. In the supply of any goods and services, the law gives certain rights that protect the consumer and provider, which also applies for Cloud Computing: it is subject to legal requirements and constraints to ensure Cloud services are accurately described and provided to customers with guarantees on quality and fitness-for-purpose.

To exemplify issues arising from data management in Cloud Federations, we have also evaluated the formerly introduced cloud architectures against legal requirements in [27], where we have chosen to perform an evaluation using requirements from data protection law. Data protection legislation is fundamental to Cloud Computing as the consumer looses a degree of control over personal artifacts, when they are submitted to the provider for storage and possible processing. To protect the consumer against the provider misusing their data, data processing legislation has been developed to ensure that the fundamental right to privacy is maintained. However, the distributed nature of Cloud Computing (where cloud services are available from anywhere in the world) makes is difficult to analyze every country's data protection laws for common Cloud architecture evaluation criteria. Therefore we have chosen a common directive that applies as widely as possible and used the European Data Protection Directive (DPD) [30] as a basis for our investigations. Although it is a European Union (EU) directive, countries that want to collaborate in data transactions with EU Member States are required to provide an adequate level of protection.

The requirements of the DPD are expressed as two technology-neutral actors that have certain responsibilities that must be carried out in order to fulfill the directive. These roles are the data controller and data processor, where a data controller is the natural or legal person which determines the means of the processing of personal data, whilst a data processor is a natural or legal person which processes data on behalf of the controller. However, following these definitions, a special case arises: if the processing entity plays a role in determining the purposes or the means of processing, it is a controller rather than a processor.

We have also explored Cloud Federations through a series of use cases to demonstrate where legal issues can arise. In these use cases the relevant actors and their roles were identified and the necessary actions have been stated that should be taken in order to prevent violations of the directive. We identified that there are complications when personal data is transferred to multiple jurisdictions. For example, considering a service provider (SP) located in the European Union offers services provisioned in a Cloud Federation, which utilizes different infrastructure providers (IPs, usually operating private clouds), and one of which (IP_2) is located in a non-Member State, we arrived to the following conclusion: since SP is the data controller and the participating IPs are processors, the law of the SP's Member State has to be applied, and IP_2 has to provide at least the same level of protection as the national law of SP. Otherwise, if IP_2 cannot ensure an adequate level of protection, the decision making process should rule out IP_2 from provider selection during data management.

As a result of our investigation we can state that service providers are mainly responsible for complying with the data protection regulation, and when personal data is transferred to multiple jurisdictions, it is crucial to properly identify the controller since this role may change dynamically in specific actions.

1.4.3 Cloud storage services in Cloud Federations

One of the most important open issues of Cloud Federations is the interoperable management of data among the participating systems. Retrieving and sharing user data and virtual images among different IaaS clouds is an unsolved issue. Besides concerning data privacy issues, it is also not an easy task to move a user application from one cloud infrastructure to another. Virtualization techniques and virtual image formats different providers support to run on their virtual machines are usually incompatible. Retrieving a user's Virtual Appliance (VA, which is a specialized image hosting the user application) from an IaaS cloud is impossible in most cases, not only in case of commercial providers, but also in academic solutions. Therefore finding an interoperable way for managing user data among multiple tenants is an important issue.

A popular family of cloud services is called cloud storage services. With the help of such solutions, user data can be stored in a remote location, independent from the infrastructure of cloud providers participating in a federation. Therefore *to exemplify the interoperable utilization of storage and infrastructure clouds*, we proposed an approach to retrieve and share user application data among different providers with the help of these online storage services. In this way VAs running at different cloud infrastructures can manage the same data at the same time, and the users can access these data from their own local devices without the need for accessing any IaaS clouds. Mobile devices can also benefit from Cloud services: the enormous data users produce with these devices are continuously posted to online services, which may require the modification of these data. Nowadays more

mobile devices are sold compared to traditional PCs, and Android devices are more and more popular. We have also investigated how user data could be managed in an interoperable way among different IaaS systems participating in a federation. Our aim was to develop a solution that uses cloud storage services together with infrastructure services of cloud federations, which we further used to enhance the capabilities of mobile devices [28]. Though the computing capacity of mobile devices has rapidly increased recently, there are still numerous applications that cannot be solved with them in reasonable time. Our approach is to utilize cloud infrastructure services to execute such applications on mobile data stored in cloud storages.

The basic concept of our solution is the following: services for data management are running in one or more IaaS systems that keep tracking the cloud storage of a user, and execute data manipulation processes when new files appear in the storage. The service running in the cloud can download the user data files from the cloud storage, execute the necessary application on these files, and upload the modified data to the storage service. Such files can be for example a photo or video made by the user with his/her mobile phone to be processed by an application unsuitable for mobile devices. We have developed an image generator application that interconnects mobile devices, IaaS services and cloud storage services, and evaluated the prototype application using mobile devices and a private IaaS cloud. The evaluation of this application showed that it is worth both in terms of computation time and energy efficiency to move computation-intensive tasks to clouds from mobile devices.

1.4.4 Energy efficient management of Cloud Federations

The Cloud Computing technology has created the illusion of infinite resources towards consumers, however this vision raises severe issues with energy consumption: the higher levels of quality and availability require irrational energy expenditures. The consumed energy of resources spent for idling represent a considerable amount, therefore the current trends are claimed to be clearly unsustainable with respect to resource utilization, CO_2 footprint and overall energy efficiency. It is anticipated that further growth is objected by energy consumption furthermore, competitiveness of companies will be strongly tied to these issues.

Energy awareness is a highlighted research topic, and there are efforts and solutions for processor level, component level and datacenter level energy efficiency. For instance, new energy efficient approaches were proposed to automate the operation of datacenters behind clouds, so that they help with rearranging the virtualized load from various users. Thus, smaller sized physical infrastructure is sufficient for the actual demand and momentarily unused capacities can be switched off. Nevertheless, these approaches are applicable to single data centers only. On one hand, today's large systems are composed of multiple service providers per se

that need new approaches to ensure their overall energy-aware operation. On the other hand, there is an unexplored potential for energy-aware operation in federated and interoperable clouds. Our research in [29] was targeted at examining what new aspects of energy awareness can be exploited in federative schemes.

As small cloud providers and cloud startups are becoming more popular, they soon face user demands that cannot be satisfied with their current infrastructures. Therefore these providers need to increase the size of their infrastructure by introducing multiple data centers on various locations or join a federation capable of offering unprecedented amount of resources.

Energy consumption is a major component of operating costs. Despite its significance, current IaaS clouds barely provide energy-aware solutions. Providers are restricted to reduce their consumption at the hardware level, independently from the IaaS. These reductions range from the use of more energy efficient computer components to the upgrade of their heating, ventilation and air conditioning systems to increase their power usage efficiency. Although these improvements are crucial, the energy consumption could also be significantly reduced by software means in over-provisioned IaaS systems where more physical resources are available at the provider side than actually requested by users. Over-provisioning is a key behavior at smaller sized providers that offer services for users with occasional peaks in resource demands. To reduce their energy costs, these providers should minimize their over-provisioning while they maintain a fluid experience towards their customers without violating the previously agreed service level. Energy consumption could be reduced with software techniques focusing on intra- and inter-datacenter issues.

In order to *exemplify how energy consumption and CO_2 emissions could be addressed in Cloud Federations*, we introduce enhancements in our proposed Federated Cloud Management solution [6]. At the meta-brokering layer, relying on an enhanced monitoring system within the federation, service executions can be directed to data centers of providers consuming less energy, having higher CO_2 emission quotas, or have produced less amount of CO_2 that expected within some timeframe. At the cloud brokering layer, if the energy consumption parameters of a cloud suddenly change, there should be strategies to limit or move around calls and even (if necessary) VMs federation-wise. The changes here may mean the introduction of new hardware, or just switching on/off some parts of the datacenters, or changing the number of VMs. Realigning calls may not have immediate effects, however migration of VMs across the federation is also an energy consuming operation, that needs to be measured and considered when decisions are made, thus this operation should not happen only in case of really drastic changes. An interoperable federation management system should prefer datacenters, where the difference between the highest load and the average load is small because a VM has the smallest impact on those resources.

1.5 Conclusion

In this chapter we gave a general insight to the formation and interoperability issues of Cloud Federations that envisage a distributed, heterogeneous environment consisting of various cloud infrastructures by aggregating different IaaS provider capabilities coming from both the commercial and academic area. These multi-cloud infrastructures are used to avoid provider lock-in issues for users that frequently utilize different clouds. We have surveyed and characterized recent solutions that attempt to hide the diversity of multiple clouds and form a unified federation on top of them, but they still need to cope with several open issues.

We have shown that these federative approaches arose from both research projects and individual research groups, *can be categorized into hierarchical and horizontal architecture types*. The hierarchical ones are more favorable by smaller research groups, and have the advantage of supporting more heterogeneous infrastructure providers to avoid vendor lock-in. We have also highlighted *open interoperability issues of federation forming and management* such as service monitoring, data protection and privacy, data management and energy efficiency.

We believe that these research directions can serve as guidelines for researchers in this field, and contribute to fostering further research works on Cloud Federations. By following the guidelines defined by the European Commission, and putting together the pieces of already existing, promising solutions of federation approaches of various research works, we will arrive to such federations that will be able to operate efficient ecosystems attracting thousands of users.

Acknowledgments

The research leading to these results has received funding from the CloudSME FP7 project under grant agreement 608886, and it was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TAMOP 4.2.4. A/2-11-1-2012-0001 'National Excellence Program'.

References

1. Buyya B, Yeo C S, Venugopal S, Broberg J, and Brandic I, (2009), *Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility*, Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, June 2009.
2. Ahronovitz M et. al, (2010), *Cloud Computing Use Cases*, A white paper produced by the Cloud Computing Use Case Discussion Group, version 4.0, http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf

3. DMTF, (2009), *Interoperable Clouds*, A White Paper from the Open Cloud Standards Incubator 1.0, DMTF white paper no. DSP-IS0101. http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf

4. Ferrer A J et. al, (2012), *OPTIMIS: a Holistic Approach to Cloud Service Provisioning*, Future Generation Computer Systems, vol. 28, pp. 66-77, 2012.

5. Schubert L, Jeffery K, and Neidecker-Lutz B, (2010), *The Future of Cloud Computing – Report from the first Cloud Computing Expert Working Group Meeting*. Cordis (Online), BE: European Commission. http://cordis.europa.eu/fp7/ict/ssai/docs/Cloud-report-final.pdf

6. Marosi A Cs, Kecskemeti G, Kertesz A and Kacsuk P, (2011), *FCM: an Architecture for Integrating IaaS Cloud Systems*. In Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization (Cloud Computing 2011), IARIA, pp. 7-12, Rome, Italy, 2011.

7. Mell P and Grance T, (2011), *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145. Online: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, September 2011.

8. Liu F, Tong J, Mao J, Bohn R B, Messina J V, Badger M L, Leaf D M, (2011), *NIST Cloud Computing Reference Architecture*, NIST Special Publication 500-292. Online: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505, September 2011.

9. OPTIMIS, (2010), *Cloud Legal Guidelines*, OPTIMIS FP7 project deliverable no. D7.2.1.1. http://www.optimis-project.eu/sites/default/files/D7.2.1.1~OPTIMIS~Cloud~Legal~Guidelines.pdf

10. Pring B et. al., (2010), *Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014*. Gartner report. http://www.gartner.com/DisplayDocument?ref=clientFriendly-Url&id=1378513, June 2010.

11. Rochwerger B et. al, (2009), *The Reservoir model and architecture for open federated cloud computing*, IBM Journal of Research and Development, April 2009.

12. Vaquero L M, Rodero-Merino L, Caceres J, and Lindner M, (2008), *A break in the clouds: towards a cloud definition*, SIGCOMM Comput. Commun. Rev. 39, 1, pp. 50-55, 2008.

13. Schubert L, and Jeffery K, (2012), *Advances in Clouds – Research in Future Cloud Computing*, Report from the Cloud Computing Expert Working Group Meeting. Cordis (Online), BE: European Commission, 2012. http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-finalreport-experts.pdf

14. eBay Inc, (2013), *Online Shopping Solution*, http://www.ebay.com/, Accessed 6 Sep 2013

15. Amazon, (2013), *Amazon Web Services*, http://aws.amazon.com/, Accessed 5 Nov 2013

16. Google, (2013), *Google Apps for Business*, http://www.google.com/apps/, Accessed 12 Jan 2013

17. Zimory GmbH, (2013), *Cloud Infrastructure Management*, http://www.zimory.com/, Accessed 10 Sep 2013

18. 4CaaSt EU FP7 project, (2013), *PaaS Cloud Platform*, http://4caast.morfeo-project.org, Accessed 2 Oct 2013

19. Jofre J et al., (2013), *Federation of the BonFIRE multi-cloud infrastructure with networking facilities*, Comput. Netw., http://dx.doi.org/10.1016/j.bjp.2013.11.012

20. Petcu D et al., (2013), *Experiences in building amOSAIC of clouds*. Journal of Cloud Computing: Advances, Systems and Applications 2013 2:12.

21. Carlini E, Coppola M, Dazzi P, Ricci L, and Righetti G, (2012), *Cloud Federations in Contrail*, Euro-Par 2011 Workshops, LNCS 7155, pp. 159–168, 2012.

22. EGI, (2013), *Federated Clouds Task Force*, https://wiki.egi.eu/wiki/Fedcloud-tf:FederatedCloudsTaskForce, Accessed 20 Oct 2013

23. Bernstein D, Ludvigson E, Sankar K, Diamond S and Morrow M, (2009), *Blueprint for the Intercloud -- Protocols and Formats for Cloud Computing Interoperability*. In Proceedings of The Fourth International Conference on Internet and Web Applications and Services, pp. 328-336, 2009.

24. Buyya B, Ranjan R and Calheiros R N, (2010), *InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services*, Lecture Notes in Computer Science: Algorithms and Architectures for Parallel Processing, Volume 6081, 20 pages, 2010.

25. Grozev N, and Buyya R, (2012), *Inter-Cloud architectures and application brokering: taxonomy and survey*. Softw: Pract. Exper., 2012. doi: 10.1002/spe.2168

26. Kertesz A, Kecskemeti G, Oriol M, Kotcauer P, Acs S, Rodriguez M, Merce O, Marosi A Cs, Marco J, Franch X, (2013), *Enhancing Federated Cloud Management with an Integrated Service Monitoring Approach*, Journal of Grid Computing, Volume 11 Number 4, pp. 699–720, 2013.

27. Varadi Sz, Kertesz A, Parkin M, (2012), *The Necessity of Legally Compliant Data Management in European Cloud Architectures*, Computer law and security review (CLSR), vol. 28, issue 5, pp. 577-586, Elsevier, 2012.

28. Planzner T, Kertesz A, (2013), *Towards Data Interoperability of Cloud Infrastructures using Cloud Storage Services*, 1st Workshop on Dependability and Interoperability in Heterogeneous Clouds in conjunction with EuroPar'13, Aachen, Germany, August 2013.

29. Kecskemeti G, Kertesz A, Marosi A Cs and Nemeth Zs, (2013), *Strategies for Increased Energy Awareness in Cloud Federations*, In book: High-Performance Computing on Complex Environments, Wiley Series on Parallel and Distributed Computing, Accepted in 2013.

30. European Commission, (1995), *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, pp. 31-50, Nov. 1995.

31. Celesti A, Tusa F, Villari M, Puliafito A, (2010), *How to Enhance Cloud Architectures to Enable Cross-Federation*. Proceedings of the 3rd International Conference on Cloud Computing (CLOUD 2010), IEEE: Miami, Florida, US, 2010; 337–345.

32. Catteddu D, and Hogben G, (2009), *Cloud computing Risk Assessment: Benefits, risks and recommendations for information security*, ENISA report. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

33. Oriol M, Franch X, Marco J, Ameller D, (2008), *Monitoring adaptable soa-systems using salmon*. In Workshop on Service Monitoring, Adaptation and Beyond (Mona+). pp. 19-28, 2008.

Index