Technical and Semantic Interoperability in the Cloud Broker

ABDESSELAM OUARDI
Computer Science Departement
Faculty of Science, Ibn Zohr University
Agadir- Morocco
abdesselam.ouardi@gmail.com

ABDERRAHIM SEKKAKI
Computer Science Departement
Faculty of Science , Ain Chock,
Hassan II University
Casablanca- Morocco
a_sekkaki@yahoo.fr

DRISS MAMMASS
Computer Science Departement
Faculty of Science, Ibn Zohr University
Agadir- Morocco
mammass@uiz.ac.ma

Abstract: - Cloud Computing represents an evolution of information systems. This technology is suitable for large groups but also for SMEs that offers a very high computing power at lower costs. It is used to interconnect several organizations disregarding their geographic location, and transforms current computer infrastructures and services. Cloud computing brings a new approach to computing, a different way of using computer resources. This development has given existence to several providers offering multiple services. Then, Cloud end users are faced with the choice of the appropriate provider in terms of supported technologies, security and access rules. Despite the advantages of cloud computing, there are still problems in terms of interoperability, security and confidentiality arrangements between Cloud Service Providers. In this sense, the cloud broker acts as an intermediary between various service providers and users to ensure proper operation. In this paper, we propose a new approach of Cloud Broker's functional architecture to the Cloud in order to deal with interoperability semantic and technical issue. Indeed, we provide the Cloud Broker of an authentication system based on federated identity that secure and optimize reliable access, this will increase technical interoperability. We also have set up a mechanism for dynamic management of services required by the user, which will increase the semantic aspect of interoperability.

Key-Words: - Cloud Computing; Interoperability; Cloud Broker; CompatibleOne; Semantic Interoperability ; Technical Interoperability.

1 Introduction

Today's Internet is radically changing our habits, with the massive influx of mobile technologies, the Internet of Things, the increasing use of grid computing, wireless networks and the emergence of new approaches in recent years. In particular virtualization of IT infrastructures that helped define a new model called "Cloud Computing" [1], introducing a fairly clean break with traditional models, can be seen as a preparatory step towards the future Internet. To run dynamically on multiple machines, a platform for data management must rely on a distributed system combining speed, scalability, and security.

Many efforts have been developed to standardize the definition of "Cloud Computing", in this context, we will use the definition provided by the National Institute of Standards and Technology (NIST) [2] : " 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." However, the rapid evolution of cloud technologies lets different cloud providers to cooperate exchanging data, applications and VMs. So interoperability problems arise specially the vendor lock-in problem [3].

The diversification of Cloud Service Providers has generated the diversification of their offers in terms of resource providing, security and access rules. Therefore, end-users are faced to a big challenge to choose the appropriate Cloud provider. This choice should be based on the provider' features such as security rules, cost optimization and/or compatibility with the end-users' requested technologies, etc. Cloud service brokers will play an important role, mediating between providers and consumers. In fact, Brokers help companies to choose the right providers, determine trusted users, deploy services across multiple Clouds, and even provide Cloud arbitrage services that allow end-users to shift between different platforms [4].

In this paper, we will present an approach that will help strengthen semantic and technical interoperability by providing a cloud broker:
A federated identity system which will allow an increase in the level of security, and differentiate trusted from malicious attempts. This part will increase technical interoperability.

- A dynamic service management system; it will be possible for the Cloud Broker to search and find services needed by user without a human intervention. Subsequently a notification will be sent to the user and also to the provider to keep traceability of the required service. This mechanism will increase the level of semantic interoperability.

The structure of this paper is organized as follows: In introduction, we give a definition of cloud computing, its characteristics, its service levels and its deployment model. Section 2 is about related works, we define dynamics management service, cloud broker and federated identity. Section 3 describes interoperability and its issues. Section 4 discusses the proposed approach; it explains the implantation of our system in the Cloud Broker and finally, Section 5 presents the conclusion and future work.

2 Related Work

The number of Cloud-based services has augmented rapidly and strongly in the last decade, and being so it increased the complexity of the infrastructures behind these services. User satisfaction is a focal point and the main concern for cloud providers.

2.1 Dynamic management Service

Many studies were oriented to put in place systems that can provide the user services at a lower cost and in a timely manner with optimal QoS.

In [5], authors proposed how to select appropriate service from the service pool with the optimal QoS parameters, and focus on the dynamic characteristics of problems that can change dynamically in terms of service and network properties. This work present also a complete definition of Cloud Computing Service Composition and expose associated concept and a comprehensive analysis applied to algorithms, mechanisms, framework and techniques. Its gives also 14 parameters of QoS

Also, [6] focuses on the importance of resource management techniques such as resource provisioning, resource allocation, resource mapping and resource adaptation:

- Resource provisioning: is providing a better QoS by provisioning the resource to the user or an application via load balancing and high availability mechanism.
- Resource allocation: is the allocation of proper resources to perform computation with minimal time and infrastructure cost.
- Resource mapping: is a system-building process that enables a community to identify existing resources and match those resources to a specify goal.
- Resource adaptation: is when a company pays a provider for used resources (pay-as-you-go) and does not need to overprovision its IT resources

In the other hand, Some of the recent research works [7] consider that Quality of Service (QoS) will provide an intelligent environment of self-management components based on domain knowledge in which cloud components can be optimized easing the transition to an advanced governance environment.

2.2 Cloud Broker

The NIST [8] defines Cloud Broker as an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

In general, a cloud broker can provide services in three categories (Fig.1):

- Service Intermediation: A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers.
- Service Aggregation: A cloud broker combines and integrates multiple services into one or more new services.
- Service Arbitrage: Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed.

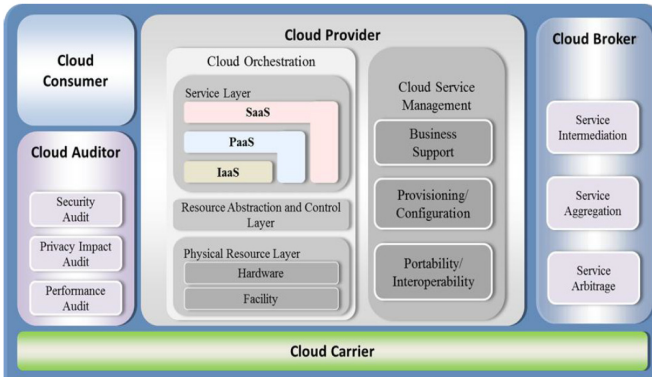

Fig. 1. The Combined Conceptual Reference Diagram of Cloud Computing [7]

The business model for cloud brokerage is still evolving.

[9] consider that the cloud broker brings intelligence into the Cloud , so [9] is an extension of the functionality offered by the cloud broker, these last feature of intelligence react to the change of business process in order to change the configuration of the cloud. In effect, it has implemented several rules to be followed by a cloud broker, in order to decide how to react facing change and determine the required actions.

However, the large number of services offered by providers of cloud generated a variety of resource providers, which influences the level of security and access rules adopted.

To resolve this ambiguity, the user is in perplexity to choose the right provider, ie, one that offers solid security rules, which optimizes the cost of use of resources and has compatibility with the technology required by the user.

[4] propose a new Open Source Cloud Broker called Compatible One which provides solutions to help Cloud users in their providers choice. It's based on interoperable middleware that describe and feder heterogeneous Clouds and resources provisioned by different Cloud providers.

Compatible One could be considered as an advanced Cloud resource management and automatic provisioning software environment because it gives a model and execution platform:

- Model: called Compatible One Resource Description System, is an object based description of Cloud applications, services and resources.
- Execution platform: called Advanced Capabilities for Compatible One Resource Description System, is a Cloud application provisioning and deployment control system.

In the same context, [10]proposes the trust evaluation of the cloud providers with the use of OPTIMIS Cloud Broker (CBR) as a mediation layer, it also presents a model cohesively works with the cloud broker in different modes using SLA and cloud characteristic parameters for evaluating the trust worthiness of the providers, and is well-placed against attacks based on malicious entities ;

2.3 Federated identity

Identity Management (IdM) is a set of functions and capabilities, such as administration, management and maintenance, discovery, information exchange, policy enforcement and authentication, used to ensure identity information, thus assuring security. An identity management system (IMS) provides tools for managing individual identities in a digital environment [11].

FIdM, or the "federation" of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration [12].

There are several technologies that go into creating a federated identity solution. Most solutions use standard technologies for authentication, authorization, and security such:

SAML: (The Security Assertion Markup Language) is an XML-based open standard to specify authentication and authorisation data. It's expressed in the form of SAML assertions that are exchanged between Identity Provider (IdP) and Service Provider (SP).

According to [13], SAML based federation has the advantage of simplifying the trust relationship is between the SP and IDP. The SPs can have one agreement with the federation instead of using multiple bilateral agreements with IdPs.

OAuth :(Open Authorization) is an open standard for secure authorisation. It allows third-party applications to get access to a web resource with the approval of the resource owner. In the most common OAuth scenario, a user can allow site A to access their information from site B without providing with his or her access credentials for site B. OAuth v2.0 is the newest version of OAuth, its two main goals are security and interoperability. Currently, it's not compatible with previous versions of OAuth [14].

3 Interoperability

There are several research initiatives focusing on definition of interoperability [15], it has been a topic of concern for at least 30 years.

In the context of networked enterprise, interoperability refers to the ability of exchanging information and service between enterprise [16]

Interoperability in a cloud environment is when localized resources on a Cloud provider communicate with resources from another provider as a user.

According to [17], interoperability in a Cloud Computing systems is the ability of cloud providers to collaborate or interact with each other and create a federation of Clouds.

We must differentiate between interoperability, portability, compatibility and data migration:

- Interoperability is the possibility to communicate between two different cloud providers [18] .
- Portability can be defined as the ability to run components or systems intended for one environment in another environment. In a cloud computing environment, this includes the software and hardware (physical and virtual) .So, users can move their data and applications across multiple cloud environments with a low cost and minimal disruption [19][20].
- Compatibility is the ability is the ability that application and data can work in the same way regardless of the cloud provider[21].
- Data migration is the ability to perform the periodic transfer of data from one hardware or software to another or from one generation of computer technology to the next generation configuration. Migration is a necessary action to maintain data integrity and to allow users to search, retrieve and use data while continuing evolution of technology [20]

3.1 Cloud interoperability issues

Interoperability between clouds is very important, both cloud provider and costumers benefit from several advantages such as avoiding vendor lock-in, scalability, availability, low access latency and energy efficiency. And this, by establishing standard interfaces, protocols, formats and architectural components that allow an easy collaboration and inter-exchange between clouds.

According to [22], there are several approaches that allow to establish cloud interoperability as:

- Hybrid cloud: it is to establish an association between the private cloud and public cloud to enable application to run in a private datacenter and to burst into a public cloud when there is a demand for computing capacity.
- Cloud federation : implies the creation of a group of aggregated provider that collaborate to share their resources in order to improve each other's service.
- Inter-cloud: all cloud are interconnected, il offer easy migration and allows a dynamic scaling of application across multiple clouds.

The author also explains the difference between cloud federation and inter-cloud, indeed, intercloud is based on the future standards and open interfaces whereas federation use a provider version of the interface. In the same context, [19] defines horizontal federation; many cloud providers join together to create a federation cloud, it offers the advantage of choosing the cloud that offers the best cost and QoS [23].

To apply interoperability in practice, there are two approaches [24] :

- Adhering to published interface standard.
- Developing a broker of service that can convert one product's interface into another product's "interface on the fly"

4 Discussion and proposed approach

The cloud environment is considered as an ultra large scale system. Ultra large scale system [25][15] is a new generation of distributed software system, it offers the ability to manage complex system whose architecture is heterogeneous. It is characterized by the fact that it's ensures decentralization (data, development and evolution), diverse requirements and heterogeneous elements and with new paradigms for acquisition and policy. But the major problem faced here is the interoperability between these components. To achieve effective interoperability, we must determine the expectations of providers and users about the features of the cloud.

In this sense, the author [18] presents the point of views of the cloud customer and the cloud provider on interoperability The first wants an interoperable cloud where it can have total control to deploy it own applications and services without sorting to additional investment costs. But, the provider considers that this incompatibility between clouds protects the interest of each provider but temporarily.

Then he listed the various items of the taxonomy of the interoperability for IAAS level, such as: Access Mechanism, Virtual Appliance, storage, network, security and SLA. Also he presented the different standardizations (OVF, CDMI, and OCCI) that help to associate between the user application and cloud provider interoperability.

In order to apply interoperability, we need to intervene on several distinct levels.

There are four types of interoperability: technical, semantic, syntactic and organizational interoperability.

- ***Technical Interoperability*** is associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centered on (communication) protocols and the infrastructure needed for those protocols to operate.
- ***Semantic Interoperability*** is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged.
- ***Syntactical Interoperability*** is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables.
- ***Organizational Interoperability,*** as the name implies, is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures.

We will take an interest in our study of the technical and semantic interoperability. For each type of interoperability, there are four levels of maturity.

A maturity model for enterprise interoperability [26] aims to:

- Define a common framework for assessing and measuring potential interoperability maturity. It provides information for how far along an enterprise is in terms of targeted maturity levels.
- Provide information about 'best practices' that allow enterprises to improve their interoperability potential.

Each maturity level is characterized by a number of criteria that need to be satisfied to reach the considered level except level 0.

Level 0 –At this level, the enterprise generally does not have an appropriate environment for developing and maintaining interoperability; systems run stand-alone and are not prepared for interoperation.

Level 1 – defined: From this level, the system is considered open to interoperability; system is capable of performing some ad-hoc interoperations with other systems. The IT infrastructure (generally ad-hoc) is in place, providing support, some basic IT devices are connectable, simple electronic data exchange becomes possible.

- Technical interoperability: Resource Management: At this level of maturity model, resource management must be implemented for establishing interoperability among heterogeneous resources by following some standards and protocols.
- Semantic interoperability: Dynamic service creation: At this level, we have to check and evaluate mechanisms for creation of new samples of services during runtime.

Level 2 – aligned: At this level, system is able to make changes in its components in order to adhere to common references. Processes, models, data and services are managed and mostly based on standards or common formats and practices.

Some guidelines exist to describe how interoperability can occur and how to adjust the business if needed.

- Technical interoperability: Data management: At this level of maturity model, data management is evaluated. Data management includes storing, accessing and transferring data that must be studied and assessed in this step.
- Semantic interoperability: Discovery: At this level, it is checked if the mechanisms for searching available services and services specifications have been defined and determined.

Level 3 – organized: At this level, the decision-making is generally decentralized to improve flexibility and reactivity.

Level 3 interoperability maturity allows an enterprise to work simultaneously with different partners in an unstable partnership environment (partners can change), without the necessity to reengineer its systems each time.

- Technical interoperability: At this level, items of security are evaluated such as:
  - *Authentication and authorization*: Authentication mechanisms are required so that the identity of individuals and services

can be established and authorization should accommodate various access control models and implementations.

- *Delegation*: Mechanisms that allow for the delegation of access rights from service requestors to service providers are required.
- *Security policy exchange*: Service requestors and providers should be able to exchange dynamically security policy information to establish a negotiated security context between them.

- Semantic interoperability: Lifetime management and notification: we define some mechanisms for repairing services and their failures and also for informing clients about changes in services condition.

Level 4 – adaptive: At this level, companies should be able to dynamically adjust and accommodate 'on the fly.' It is the highest level where interoperability itself becomes a subject of continuous improvement (evolution and adaptation).

- Technical interoperability: Runtime resource management: At this level, activities related to runtime resource management are provided in a dynamic environment. These activities include adding, changing and removing a new resource during runtime.
- Semantic interoperability: Dynamic service management: At this level, services are managed dynamically.

Interoperability Maturity Levels	Technical Interoperability	Semantic Interoperability
4 INTEROPERATING LEVEL	Remove Existing Ressource (Runtime)	Dynamic Service Composition
	Modify Existing Ressource (Runtime)	Dynamic Service Invocation
	Add new Ressource (Runtime)	Dynamic Service Discovery
3 INTEGRATING LEVEL	Security Policy Exchange	Notification
	Delegation	Lifetime Management
	Athentification and Authorization	
2 ENABLING LEVEL	Data Transfer	Discovery
	Date Access	
	Data Storage	
1 INITIATING LEVEL	Ressource Access	Dynamic Service Creation
	Ressource Discovery	
	Collaboration and Ressource Sharing	
DEFAULT LEVEL	Default Level	Default Level

Table1 .maturity and components of interoperability

Table 1. illustrates the types of interoperability with their levels. As noted in blue color, represents the current level of maturity of the interoperability, what is red, is the targeted level for each type and level of interoperability.

In our case, we will take an interest in increasing the level of semantic interoperability and technical interoperability.

To increase technical interoperability level from Level 2 to Level 3 in the cloud, there must be a system that provides more matured security. In fact level three requires a level of authentication and authorization more mature. For our approach, it is proposed that authentication will be done in a federated identity system that will verify that the user is reliable and what type of access he has and then, directed to the appropriate service.

To increase semantic interoperability level, some mechanisms must be defined for repairing service and their failures in order to inform clients about changes in services conditions.

In order to solve this problem, the cloud broker must have a system upgrade that will dynamically manage the services.

The proposed architecture is as follows.

4.1 Federated identity system

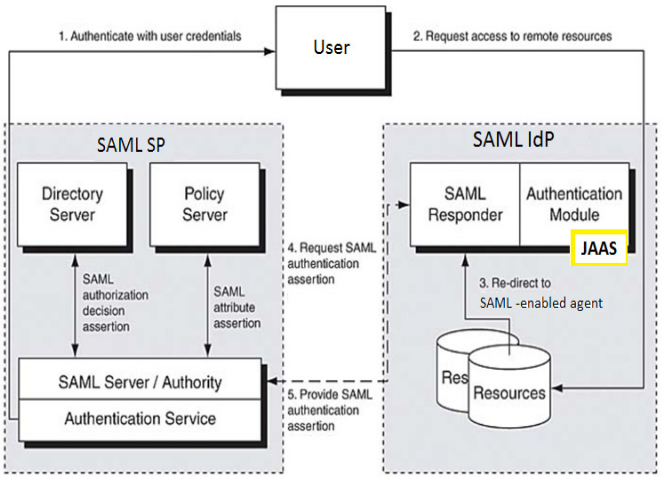

Fig. 2. Proposed Federated identity system

SAML SP has built an authentication service (Authentication Authority), directory server (Attribute Authority that stores the policy attributes), and a policy server (that determines what the client is entitled to). The SAML server (or authority) processes requests for SAML assertions and responds to the SAML-enabled agent.

The following describes the interaction between components (Fig.2):

The user has already authenticated with the authentication service offered by the SAML SP (Step 1).

The client creates an application request to the remote sources at SAML IdP (Step 2). The SAML IdP has a SAML-enabled agent that uses an authentication module to generate authentication assertions.

In our case, we works with Java Authentication and Authorization Service (JAAS) to authenticate and authorize for application, we also set up an Authorization Schema that configured to check multiple credential providers in a defined order by using (Lightweight Directory Access Protocol (LDAP) and Relational Database Management Systems (RDBMS)

The remote destination redirects the application request to the SAML-enabled agent (Step 3).

The SAML-enabled agent issues a SAML authentication assertion request to the SAML SP (Step 4).

The SAML-enabled authentication service processes the SAML authentication assertion request and provides a response to the SAML IdP (Step 5).

4.2 Automatic management of service:

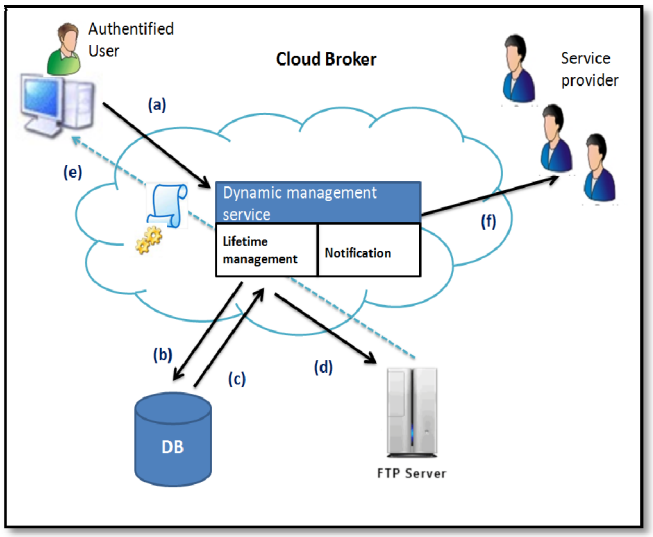

Fig. 3. Proposed Dynamic management service (DMS)

The figure (Fig.3) shows the flow of processing performed by the DMS :

The user wants to use Service A, he finds that in his machine the service “ServA.exe” is not installed. He will access to the dynamic service management (DMS) to install it.

After the choice of service, DMS will send a query to the database to check if the service exists. (In the database, we will store all services that user has the right and permission to install).

The return of the response of the BD. if the answer is yes, the DMS will memorize all the necessary service information to be able to access the FTP server.

The DMS will look for the target service in the FTP server; FTP Server will contain all services from different providers.

The "ServA.exe" service will be downloading from the server FTP and then install on the client machine by a script that will be executed automatically.

The notification module will send to the provider all the information about the service installed and the target machine.

As for the architecture, we chose to use CompatibleOne as cloud broker open source because it offers the following advantages:

- Compatible with most platforms to provide maximum freedom to users and developpers
- Compatible One aims to renders «clouds» interoperable
- Break vendor lock-in.

Is based on the architecture of CompatibleOne [4][27],openStack[28] and OpenNebula[29], the functional architecture of our approach will be as follows (Fig. 4):

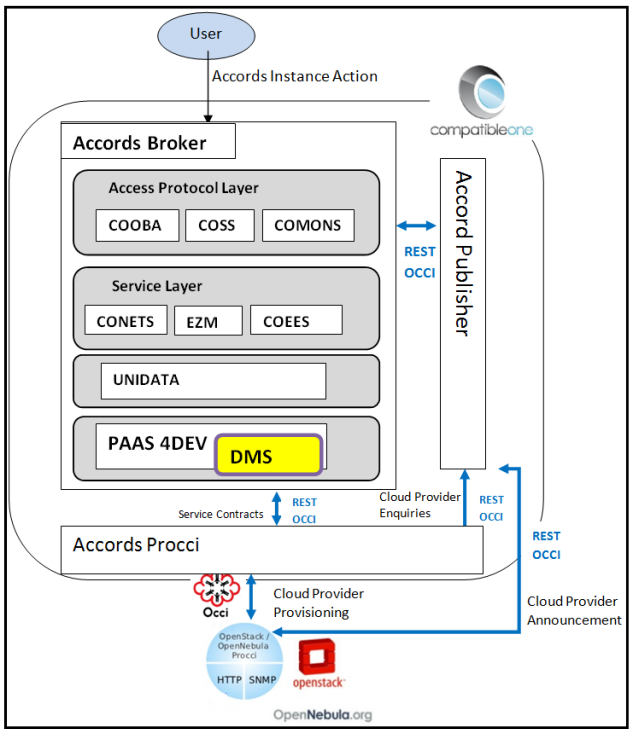

Fig. 4. The functional architecture

- The DMS will be integrated at Paas 4Dev.
- CompatibleOne will be connected using REST API (OCCI) to OpenNebula and OpenStack

- ACCORDS Advanced Capabilities for CompatibleOne Resources Distribution Services
- Broker: aggregation of diverse services from heterogenous providers and enables interoperability and portability.
- COOBAS: provide billing and accounting.
- PROCCI: (OCCI Proxy): :a gateway to any cloud provider whatever has their one procci e.g OpenStack, Amazon or Azure Procci.
- COSS (Security Service): insures security of platform services of the plateform and platform produced services .
- COMONS(Monitoring Service): collection of information as required to insure SLA compliancy.
- EZVM Virtual Machine Interoperability.
- CONETS: The CompatibleOne Network Service component.
- COEES: The CompatibleOne Energy Efficiency Service component.
- Publisher: provides the base on which the rest of the platform reposes
- PaaS4DEV Runtime OSGI
- UNIDATA Data Interoperability

5 Conclusion

In this paper, we presented initially an overview of cloud computing. We defined also the cloud broker and his role as being intermediary between users and provider. And we exposed different type of interoperability, its issues and we define the maturity levels of each type of interoperability.

In previous sections of this paper, an approach to increase level interoperability was proposed. Where we provide the Cloud Broker with an authentication system based on federated identity to secures and optimize reliable access, this will increase technical interoperability. We have set up a mechanism for dynamic management of services required by the user, which will increase the semantic aspect of interoperability.

Future work is planned to develop a system that can manage dynamically Install/Execute Services in detriment of the intervention humaine.et other hand, we will put a strong authentication system. The two systems will be integrated in the open source cloud broker to cover the semantic and technical aspects of interoperability and to benefit from the qualities offered by open source.

Despite the benefits of cloud, there is the issue of interoperability between providers. Several studies have been done to create standards to solve the problem of security and privacy

References:

[1] A. Kertesz, G. Kecskemeti, et I. Brandic, « An interoperable and self-adaptive approach for SLA-based service virtualization in heterogeneous Cloud environments », *Future Gener. Comput. Syst.*, vol. 32, p. 54□68, mars 2014.

[2] N. US Department of Commerce, « Final Version of NIST Cloud Computing Definition Published ».http://www.nist.gov/itl/csd/cloud-102511.cfm.

[3] J. P. Martin-Flatin, « Challenges in Cloud Management », *IEEE Cloud Comput.*, vol. 1, n° 1, p. 66□70, mai 2014.

[4] S. Yangui, I.-J. Marshall, J.-P. Laisne, et S. Tata, « CompatibleOne: The Open Source Cloud Broker », *J. Grid Comput.*, vol. 12, n° 1, p. 93□109, mars 2014.

[5] A. Jula, E. Sundararajan, et Z. Othman, « Cloud computing service composition: A systematic literature review », *Expert Syst. Appl.*, vol. 41, n° 8, p. 3809□3824, juin 2014.

[6] S. S. Manvi et G. Krishna Shyam, « Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey », *J. Netw. Comput. Appl.*, vol. 41, p. 424□440, mai 2014.

[7] D. Kourtesis, J. M. Alvarez-Rodríguez, et I. Paraskakis, « Semantic-based QoS management in cloud systems: Current status and future challenges », *Future Gener. Comput. Syst.*, vol. 32, p. 307□323, mars 2014.

[8] N. US Department of Commerce, « Final Version of NIST Cloud Computing Definition Published »,http://www.nist.gov/itl/csd/cloud-102511.cfm.

[9] S. G. Grivas, T. U. Kumar, et H. Wache, « Cloud Broker: Bringing Intelligence into the Cloud », in *2010 IEEE 3rd International Conference on Cloud Computing (CLOUD)*, 2010, p. 544□545.

[10] P. S. Pawar, M. Rajarajan, T. Dimitrakos, et A. Zisman, « Trust Assessment Using Cloud Broker », in *Trust Management VIII*, J. Zhou, N. Gal-Oz, J. Zhang, et E. Gudes, Éd. Springer Berlin Heidelberg, 2014, p. 237□244.

[11] M. A. P. Leandro, T. J. Nascimento, D. Santos, D. R, C. M. Westphall, et C. B.

Westphall, « Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth », presented at ICN 2012, The Eleventh International Conference on Networks, 2012, p. 88□93.

[12] « Federated identity », *Wikipedia, the free encyclopedia*.

[13] M. Hardt, A. Hayrapetyan, P. Millar, et S. Memon, « Combining the X.509 and the SAML Federated Identity Management Systems », in *Recent Trends in Computer Networks and Distributed Systems Security*, G. M. Pérez, S. M. Thampi, R. Ko, et L. Shu, Éd. Springer Berlin Heidelberg, 2014, p. 404□415.

[14] D. Rountree, « Chapter 3 - Federated Identity Technologies », in *Federated Identity Primer*, D. Rountree, Éd. Boston: Syngress, 2013, p. 37□60.

[15] R. Rezaei, T. K. Chiew, et S. P. Lee, « An interoperability model for ultra large scale systems », *Adv. Eng. Softw.*, vol. 67, p. 22□46, janv. 2014.

[16] I. Mezgár et U. Rauschecker, « The challenge of networked enterprises for cloud computing interoperability », *Comput. Ind.*, vol. 65, n° 4, p. 657□674, mai 2014.

[17] R. Cohen, « ElasticVapor: Examining Cloud Compatibility, Portability and Interoperability ». .

[18] Z. Zhang, C. Wu, et D. W. L. Cheung, « A Survey on Cloud Interoperability: Taxonomies, Standards, and Practice », *SIGMETRICS Perform Eval Rev*, vol. 40, n° 4, p. 13–22, avr. 2013.

[19] D. Petcu, « Portability and Interoperability between Clouds: Challenges and Case Study », in *Towards a Service-Based Internet*, W. Abramowicz, I. M. Llorente, M. Surridge, A. Zisman, et J. Vayssière, Éd. Springer Berlin Heidelberg, 2011, p. 62□74.

[20] R. Rezaei, T. K. Chiew, S. P. Lee, et Z. Shams Aliee, « A semantic interoperability framework for software as a service systems in cloud computing environments », *Expert Syst. Appl.*, vol. 41, n° 13, p. 5751□5770, oct. 2014.

[21] M. Sharma, K. Jindal, et S. Srinivasan, « Evaluating Various Aspects of Cloud Computing Vendors with Comparison », *strategies*, vol. 1, n° 1, p. 4□8, 2014.

[22] A. N. Toosi, R. N. Calheiros, et R. Buyya, « Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey », *ACM Comput Surv*, vol. 47, n° 1, p. 7:1–7:47, mai 2014.

[23] R. Buyya, R. Ranjan, et R. N. Calheiros, « InterCloud: Utility-oriented Federation of Cloud Computing Environments for Scaling of Application Services », Berlin, Heidelberg, 2010, p. 13–31.

[24] D. Chen et G. Doumeingts, « European initiatives to develop interoperability of enterprise applications—basic concepts, framework and roadmap », *Annu. Rev. Control*, vol. 27, n° 2, p. 153□162, 2003.

[25] R. Rezaei, T. K. Chiew, S. P. Lee, et Z. Shams Aliee, « Interoperability evaluation models: A systematic review », *Comput. Ind.*, vol. 65, n° 1, p. 1□23, janv. 2014.

[26] W. Guédria, Y. Naudet, et D. Chen, « Maturity model for enterprise interoperability », *Enterp. Inf. Syst.*, vol. 0, n° 0, p. 1□28, juin 2013.

[27] F. D. Sanchez, S. Al Zahr, M. Gagnaire, J. P. Laisne, et I. J. Marshall, « CompatibleOne: Bringing Cloud as a Commodity », in *2014 IEEE International Conference on Cloud Engineering (IC2E)*, 2014, p. 397□402.

[28] « OpenStack Docs: Current ». http://docs.openstack.org/.

[29] « OpenNebula Documentation ». http://opennebula.org/documentation/