ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Challenges in Achieving Interoperability in Cloud Computing

[1]Dileep, V.K. and [2]Dr. R.V. Sivabalan

[1]Assistant Professor, Dept. of CSE, LBSITW, Poojappura, Thiruvananthapuram
[2]Associate Professor, Dept. of Computer Applications, Noorul Islam University

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
Interoperability, Cloud Computing
Cloud Standards

ABSTRACT

Cloud computing is a relatively new paradigm that promises to alter the way IT services are provided. There are multiple benefits that companies can gain from cloud computing. However, there still remain a number of issues to be solved before this new computing paradigm is widely adopted. This paper discusses one of the issues-interoperability of applications. Now there is no such assessment framework to determine which system has achieved what level of interoperability. Here discusses various approaches and standards used in achieving some degree of interoperability, as well as issues in cloud interoperability. This paper conducts a detailed literature review on interoperability in cloud systems and then presents technical challenges together with many managerial issues remain an obstacle to achieving complete interoperability.

To Cite This Article: Dileep, V.K. and Dr. R.V. Sivabalan., Challenges in Achieving Interoperability in Cloud Computing. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 36-43, 2015*

INTRODUCTION

Cloud computing has emerged as a computation paradigm to deliver on-demand resources to customers similar to other utilities such as water, electricity etc. Three main services are provided by the Cloud computing architecture according to the needs of IT customers (Buyya *et al*., 2009). Typically, cloud computing consists of the three cloud layers infrastructure (IaaS), platform (PaaS) and software (SaaS) as service (Armburst *et al*., 2009) (Buyya *et al*., 2011).

A cloud delivers on-demand services ranging from software to platform or infrastructure services (SaaS, PaaS, and IaaS) over the internet. Cloud computing is defined by the National Institute of Standards and Technology(NIST) as a model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (P. Mell and T. Grance, 2011). Cloud Computing aims to deliver a network of virtual services so that users can access them from anywhere in the world on subscription at competitive costs depending on their Quality of Service requirements (Buyya *et al*., 2009). Currently, the cloud environments include hundreds of individual, heterogeneous, private/hybrid clouds with finite physical resources, but for the future expansion of the application scope of cloud services require cooperation between the clouds. This interoperability mechanism between clouds is called "Intercloud". Interoperability between clouds can provide:

- Better Quality of Service
- Avoidance of vendor lock-in.
- Enabling inter-cloud Resource Sharing

Currently, there are no implicit interoperability standards for heterogeneous cloud computing architectures to promote Intercloud interoperability.

Need For Interoperability:

There are several business decisions which may lead to a change in providers. Some reasons for this change include:

- Increase in cost at contract renewal time
- A provider suddenly closes services being used, without acceptable migration plans.
- Failure to meet key performance requirements or achieve service level agreements (SLAs).

Every new cloud service provider have their own way on how a user or cloud application interacts with their cloud leading to cloud API propagation (AV Parameswaran and Asheesh Chaddha, 2009). Interoperability is defined as the ability of a collection of communicating entities to share specified information and operate on it according to shared operational semantics in order to achieve a specified purpose in a given context (Petcu, 2011). Ensuring operational integrity across these boundaries as processing needs move into the cloud

Corresponding Author: Dileep V.K., Assistant Professor, CSE Dept., LBSITW, Poojappura, Thiruvananthapuram, Kerala, India-695012,
Mob: +91 9447323003, E-mail: dileepvk@gmail.com

is a critical consideration which can be addressed through interoperability.

What is Interoperability?

The term of interoperability has many definitions in literature (Petcu, 2011) and is often misused to include the term of portability. Interoperability is the ability of a service to interact with other services offered either by the same provider or other providers. It is more qualitative and can be defined by user experience (S.K.Garg *et al*., 2013).

Service Interoperability means customers can use services across multiple clouds using a common framework. It applies to all three Cloud Computing service models but the meaning and the requirements varies in each model. In the IaaS model clients have the ability to use the infrastructure of different clouds and control them as if they were one. A simple example is that the client has control over several virtual machines that helps to encapsulate the computational resources from different clouds. In PaaS, service interoperability is about enabling the clients to use different APIs, tools, libraries etc. from different platforms ported in different clouds in order to create applications. Finally, in the SaaS model, interoperability refers to enabling cloud applications to exchange messages or data between the clouds.

Interoperability impacts often arise within cloud computing when changing business needs drive the need for changing a service provider. Lack of interoperability can lead to being locked to one cloud service provider. The degree to which interoperability can be achieved or maintained when considering a cloud project often will depend on the degree to which a cloud provider uses open, or published, architectures and protocols. Refer for a moment to the Jericho Cloud Cube which defines a means for differentiating between cloud models. The Cloud Cube defines an axis that identifies two degrees for interoperability as “proprietary” and “open” (jerichoforum.org, 2009).

When appropriate interoperability between components is attained, companies can effectively deploy cloud solutions from a single cloud provider or from many providers as best meets their needs. Through interoperability, all components will require appropriate orchestration in order to operate correctly and securely regardless of where they are hosted or on what platform.

Issues in Interoperability (Smith, James D, 2006):

The following issues have been identified as a hindrance or challenge in the adoption and implementation of interoperability (Jean Bozman, 2010).

The virtual machine (VM) is becoming a fundamental unit of work and encapsulation, particularly for IaaS and some PaaS clouds. Customers today prefer mixed virtualization environments inside their enterprises and to be able to pick up a VM and move it, regardless of the underlying platform.

Enterprises have to make changes in their programming tools to adapt to a cloud model but, IT staffers will likely want to avoid a wholesale change.

Platform as a Service clouds provide new application frameworks and APIs that provide special cloud functionality. In order to to leverage these APIs, existing applications need to be modified which is generally a difficult and expensive procedure.

With the desire for tight coordination between on-premises and off-premises resources in a hybrid cloud, management must become more unified. This requires that clouds follow existing management standards — and that they also should be "open" to third-party management applications.

Customers will need to ensure that the cloud provides appropriate standards to support data export, along with data conversion from one format to another, as well as compatible or abstracted storage-access services.

Customers need to be aware of the restrictions and problems that license portability may have on their use of cloud, and work with their ISVs to implement new policies that are cloud-friendly.

Interoperability issues related to various cloud components (Jean Bozman, 2010):

- Hardware–When hardware must be addressed makes sure that the same or better physical and administrative security controls exist when moving from one provider to another.
- Virtualization – While virtualization can remove concerns about physical hardware, distinct differences exist between common hypervisors. Consider using open virtualization formats to ensure interoperability.
- Frameworks – Different platform providers offer different cloud application frameworks and differences do exist between them. Use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications and data should changing a service provider become necessary.
- Storage – Storage requirements will be different for different types of data. Store unstructured data in an established portable format for both reduced storage and transfer requirements. Use interoperable data compression for data moved to and from the cloud. Ensure the storage format selected interoperates regardless of the underlying platform. Check for compatible database systems and assess conversion requirements if needed.
- Security – Data and applications in the cloud reside on systems which have only limited control over. Make sure authentication controls for system and ensure compatible user account access credentials for continued and consistent system

access integrity and security. Use the way of encryption to protect sensitive data moved to the cloud. Use only interoperable encryption that protect data and files regardless of the platform, storage systems, or location where it resides. API security keys used for calls to services requiring authentication should interoperate and appropriate maintenance and protections of keys must exist on new platforms. Data integrity measures should be incorporated to ensure data remains unaltered while in the cloud. Where native document formats do not support digital signing, protect documents in interoperable formats that do.

Why Do Interoperability Matter?

Interoperability must be an important issue in the cloud migration to either public, private, or hybrid cloud solutions. They are important elements to consider for service model selection regardless of whether a migration strategy is to Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS). Failure to appropriately address interoperability in a cloud migration may result in failure to achieve the desired benefits of moving to the cloud.

Factors that should be avoided are (CSA, 2011):

- Vendor lock-in – you cannot easily move from the selected cloud to a cloud offering from another vendor in future.
- Processing incompatibility and conflicts causing disruption of service provider, platform or application differences may expose problems that cause applications to malfunction if a new cloud platform is chosen
- Unexpected application re-engineering– moving to a new cloud provider can introduce a need to rework how a process functions or require coding changes to retain original behaviors
- Costly data migration or data conversion - lack of interoperable formats may lead to unplanned data changes.
- Retraining or retooling of new application or management software
- Loss of data or application security – different security policy or control, key management or data protection between providers may open undiscovered security gaps when moving to a new provider or platform. To ensure interoperability of data in transit to, and stored within the cloud, make sure data is protected before placing it in the cloud and make sure keys remain within the hands of authorized company staff.

Interoperability in Different Cloud Models (Buyya et al., 2011) (Jean Bozman, 2010):

The primary goal of interoperability is to make it easier to adopt cloud. Compatibility is next natural step of how to achieve this interoperability. It is the ability of the application and the data to work the same way irrespective of the service model (IaaS, PaaS, SaaS) or deployment models (private, public, and hybrid) and location (internal or external to the enterprise). One of the key factors to cloud interoperability is data portability.

Infrastructure as a Service (IaaS):

The cloud provider should provide standardized hardware and computing resources that can interact with various distinct systems with minimal efforts. The Cloud provider should stick on to industry standards to uphold interoperability. The provider should be able to support scenarios such as cloud brokerage, cloud bursting, hybrid clouds, multi-cloud federation etc.

- In order to keep interoperability in IaaS, virtualization compatibility must be ensured. This includes practices of provisioning and de-provisioning of virtual machine images.
- Be aware of the practices used for decommissioning of disks and storage devices.
- Identify with hardware/platform based dependencies before migration of the application/data.
- Know options to resume service with the legacy cloud provider in part or in whole if new service proves to be inferior.
- Value costs involved for data migration
- Realize what security is provided and who maintains access to encryption keys

Platform as a Service (PaaS):

The cloud provider is responsible to provide a platform on which the consumers can build their systems. They provide with a runtime environment and an integrated application stack. It allows developers to quickly develop and deploy custom applications on the offered platforms without the need to build the infrastructure.

- Use platform components with a standard syntax, open APIs, and open standards.
- Be aware of what tools are available for secure data transfer, backup, and restore.
- Know how base services like monitoring, logging, and auditing would transfer over to a new vendor.
- Protect data using standard encryption formats and retain control of all encryption keys
- Identify with control functions provided by the legacy cloud provider and how they would translate to the new provider.
- Be aware of how testing will be completed prior to and after migration, to verify that the services or applications are operating correctly. Ensure that both provider and user responsibilities for testing are well known and documented.

Software as a Service (SaaS):

The cloud provider provides application capabilities over the cloud and the client just manages his/her operations and the information

flowing in and out of the system. The client needs only a browser and the administrative things are rests with the provider.

- Carry out regular data extractions and backups to a format that is usable without the SaaS provider.
- Realize whether metadata can be preserved and migrated.
- Understand that any custom tools being implemented will have to be redeveloped, or the new vendor must provide those tools.
- Assure the possibility of migration of backups and other copies of logs, access records, and any other pertinent information which may be required for legal and compliance reasons.

Private Cloud:

Private cloud is when consumers run private cloud within their enterprise or use private cloud offering from the cloud providers.

- Make sure interoperability exists between common hypervisors.
- Ensure standard API's are used for management functions such as users and their privilege management, VM image management, Virtual Machine management, Virtual Network management, Service management, Storage management, Infrastructure management, Information Management etc.

Public Cloud:

Interoperability in public cloud means exposing most common cloud interfaces. They may be vendor specific or open specifications and interfaces.

- Ensure that the cloud providers expose common and/or open interfaces to access all cloud functions in their service offering.

Hybrid Cloud:

In this scenario the consumer's local private infrastructure should have the capability to work with external cloud providers. A common scenario is "cloud bursting". For an enterprise to meet peak demands to better serve its customers, the enterprise could share load with external cloud providers

- Ensure that the cloud providers expose common and/or open interfaces to access all cloud functions in their service offering.
- Ability to federate with different cloud providers to enable higher levels of scalability.

Benefits of Interoperability (CSA, 2011):

- Infrastructure Abstraction – Application developers and administrators no longer need to worry about the hardware. Hypervisors gives the abstraction from underlying hardware thus removing the compatibility concerns.
- Abstraction between application, data, logic and system interfaces – provides agile application development process, portability, modularity and loose coupling. Enterprises no longer need to worry that application and data need to reside on the same location.
- Cloud Adaptability and Customization – Provides ability for the enterprises to adopt cloud and also the ability to customize the cloud environments to fit their needs.
- Vendor Lock-in – Interoperability standards provide consumers the ability to switch cloud providers without a lock-in to a particular provider.
- Openness – Transparency is one of the key requirements of cloud computing. Provides the confidence to the consumers with their business continuity planning in the event they want to switch providers.

Use Case Scenarios (Cisco Datacenter, 2009):

The use case scenarios demonstrate the performance and economic benefits of cloud computing and are based on the needs of the vast range of consumers. The goal is to highlight the capabilities and requirements that need to be standardized in a cloud environment to ensure interoperability. Cloud computing must grow as an open environment, minimizing vendor lock-in and increasing customer choice.

❖ ***Enterprise to Cloud to Enterprise (Kennedy et al., 2012):***

This use case involves two enterprises using the same cloud. The focus here is hosting resources in the cloud so that applications from the enterprises can interoperate. A supply chain is the most obvious example for this use case.

Requirements:

The basic requirements of the Enterprise to Cloud to Enterprise use case are much the same as those for the Enterprise to Cloud use case. Identity, an open client, federated identity, location awareness, metering and monitoring, management and governance, security, industry-specific standards, common APIs for storage and middleware, data and application federation, SLAs and lifecycle management all apply.

Other requirements for this use case are:

• ***Transactions and concurrency****:*

For applications and data shared by different enterprises, transactions and concurrency are vital. If two enterprises are using the same cloud-hosted application, VM, middleware or storage, it's important that any changes made by either enterprise are done reliably.

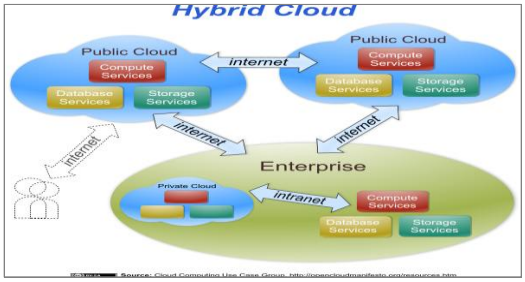
• ***Interoperability:***

Because more than one enterprise is involved, interoperability between the enterprises is essential.

❖ ***Hybrid Cloud (Kennedy et. al., 2012):***

This use case involves multiple clouds working together, including both public and private clouds. A

hybrid cloud can be delivered by a federated cloud provider that combines its own resources with those of other providers. A broker can also deliver a hybrid cloud; the difference is that a broker does not have any cloud resources of its own. The provider of the hybrid cloud must manage cloud resources based on the consumer's terms.



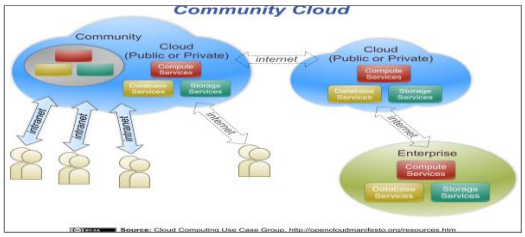
The user has no knowledge of what the hybrid cloud provider actually does.

Requirements:

• All of the requirements of the previous use cases apply here, particularly Security, Data and Application Federation and Interoperability.

• **SLAs:** A machine readable, standard format for expressing an SLA. This allows the hybrid cloud provider to select resources according to the consumer's terms without human intervention.

The requirements for a community cloud are a subset of the requirements for the hybrid cloud. A community cloud has an infrastructure shared among enterprises with a common purpose. Here is the diagram for a community cloud:



Notice that the communication between the community and the community cloud is done across an intranet. This could be a VPN, but access is not via the public Internet.

❖ Other use case scenarios (CSA, 2011)

- When you use cloud provider#1 and in turn cloud provider#1 is using other cloud providers like #2 and #3. Now the data is spread across all #1, #2 and #3 cloud providers and you don't have direct relationship with #2 and #3. The issues faced here are:

➢ Translating the data to a new format or schema.

➢ Identity management and permission on the data also need to be translated.

- The Cloud Broker

A cloud broker understands many cloud vendors and can facilitate the migration of data and identity to another cloud vendor. Cloud brokers may specialize in data migration, application migrations or identity migration.

- Cloud Identity and Access Management

When using "Identity Management as a Service" providers should provide Strong passwords and polices that can be managed by the customer. These standards should go above internal standards.

Interoperability Risks (Cloud Standards Customer Council, 2014):

There are several risks involved with Interoperability in Cloud environments.

The process of moving huge databases into the cloud and also moving data from one provider to another need right supporting tools. Several of the Public Cloud offerings are built on proprietary technologies. Cloud providers do not support Heterogeneous deployments. In order to migrate from one vendor to another, the applications may have specific performance requirements, preservation policies, or conformity. The design of application and how the distributed components interact at each data transaction can be an issue when migrating from one vendor to another as the infrastructure environment may be different. Quantitative analysis of number of users is an important factor for capacity and migration planning for the new Cloud environment. Interactive applications are sensitive to network and processing latency for usability. Ideally the selection of the new Cloud provider should be done based on a guarantee of an acceptable response time range. The specific licensing requirements for services should be evaluated upfront and negotiated with the Cloud Vendor. SaaS integration with existing systems and processes may be more difficult

than with other migration options because well-built, well-documented, or usable APIs may not be available. Too little service-level can be a significant issue for certain applications which have strict quality of service requirements. Risk management of the Cloud providers from a legal, compliance and operational perspectives is another issue when it comes to interoperability. Before a decision to migrate is made, the new Cloud vendor should be evaluated and audited for strict compliance and privacy requirements.

Suggestions (Camey et. al., 2005) (Craig Meyers, 2006):

Precise migration goals and motivations must be identified along with a detailed analysis of requirements and constraints looking at various aspects for Quality of service. Cloud migration decisions will impact the application platform decisions. The end-user profile for the intended applications or solutions is open and inclusive so that all intended end-users will have continuous accessibility to the applications ported to The Cloud. Security for the applications or services is reasonable and simplistic enough to be included in a cloud service model. Because of pay as you go and self-service characteristics, application migration to cloud providers can support a department's autonomous operations. Most cloud alternatives present lock-in challenges related to the service offered. Closed versus open can mean different things for virtualization, code and data perspectives.

The organization's sourcing principles may read out the use of single vendors over best-of-breed vendors and influence the decision when multiple migration options meet an application's requirements. It is important to go through a structured methodology and broad analysis for deciding to port applications to the Cloud. A Complete risk assessment exercise must be conducted for the services being migrated to a Cloud environment. Pre-migration audit should be conducted and that should include evaluation and ranking of all the applications or service components. Another important Pre-Portability activity is to plan fall back options. During the move to the Cloud, a clearly defined fall-back strategy and plan are available to the customer. To l*et al*one risks, follow a sound risk management strategy i.e., Assess, Isolate, Mitigate, and Map before placing applications and IT services in the cloud. Having a Cloud Exit strategy should be part of the process of deciding to migrate to cloud. Risk can also be mitigated to some extent by using internally managed multiple sources or using a cloud broker or federated clouds.

Various Standards and Technologies:

At present there are important standards and technologies emerging for interoperability in the cloud. It will take long time for these standards to mature and be supported by the majority of the providers. Following are few of the many efforts centered on the development of both open and proprietary API's that tries to address things such as management, security and interoperability for cloud (Grace A Lewis, 2012).

- Open Cloud Computing Interface (OCCI). It is a protocol and API originally initiated to create a remote management API for IaaS, allowing for development of interoperable tools for deployment, autonomic scaling and monitoring.

1. REST-based interfaces for management of cloud resources including computing, storage, and bandwidth
2. Working group of the Open Grid Forum

- DMTF's Open Virtualization Format (OVF) is a packaging standard designed to address the portability and deployment of virtual appliances.

1. Management interoperability for cloud systems
2. Developer of the Open Virtualization Framework (OVF)
3. Runs the Open Cloud Standards Incubator

- IEEE the standards body has created 2 working groups P2301 and P2302.

P2301 working group will provide a portability roadmap for cloud vendors, service providers and their consumers.

Standards-based options for application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conventions

P2302 working group will define topology, protocols, functionality and governance for cloud-to-cloud interoperability and federated operations (hybrid cloud).

Protocols for exchanging data, programmatic queries, functions, and governance for clouds

sharing data or functions or for federating one cloud to another

- Cloud Computing Interoperability Forum (CCIF) was formed to enable a global cloud computing ecosystem where organizations can work seamlessly for wider adoption of cloud computing.
- Common, agreed-on framework/ontology

for cloud platforms to exchange information in a unified manner

- Sponsors of the Unified Cloud Interface

Project to create an open and standardized cloud interface for the unification of various cloud APIs

- OpenStack – This was originally founded by Rackspace and NASA. It has grown into an open source community with global collaboration of developers and cloud computing technologists to provide open source cloud computing platform for public and private clouds.
- Open-source software for running private clouds
- Open Cloud Consortium

Frameworks for interoperating between clouds and operation of the Open Cloud Testbed

- Cloud Standards Customer Council
- Standards, security, and interoperability issues related to migration to the cloud
- End-user advocacy group sponsored by the Object Management Group (OMG) and creator of the Open Cloud Manifesto
- CloudAudit, also known as Automated Audit, Assertion, Assessment, and Assurance API (A6) is an Open, extensible, and secure interface, namespace, and methodology for cloud computing providers and their authorized consumers to automate the audit, assertion, assessment, and assurance of their environments.

The lack of interoperability has been identified as a major barrier to cloud adoption. If the interoperability challenge can be overcome it will be greatly beneficial for both the customer and provider. Standardization of API's, data models, data formats and terminology will assist in achieving interoperability. With a standard to conform to the customer will benefit from automation of cloud computing procurement procedures, simpler technical integration and flexible deployment over multiple cloud platforms.

Conclusion and Future Work:

A particular concern for cloud computing is the deployment or migration of systems to a cloud service or set of cloud services. *Application interoperability* between SaaS services and applications, and *platform interoperability* between PaaS services and platforms are important kinds of cloud computing interoperability to consider. Applications can include programs concerned with the deployment, configuration, provisioning, and operation of cloud resources. Interoperability between these programs and the cloud resource environments is important. Although cloud services are used by many, cloud is still an emerging technology, and standards are still developing, with certain areas maturing more quickly than others. IT continues to update and transform and standards thus are always being adapted, accepted and maintained. Moreover the legalities and jurisdictions surrounding cloud computing adds to the complexities of creating standards that accommodate both national and international legal requirements. Standards are necessary to enhance the trust in cloud computing and protect personal data in accordance with regulatory bodies. Many concerns could be addressed with the necessary standards in place. Standards should promote trusted and reliable cloud offerings that encourage security, interoperability, data transferability and reversibility. The development of concise cloud standard based on all the available security standards will enhance legal conformity and enforcement. Other non- cloud specific technical standards also relate to computing in the cloud. However cloud specific standards are beginning to emerge with focus on areas not already covered or efficiently covered by any existent standard. Pronounced global effort is being placed on creating effective cloud standards to address the gaps and alleviate the concerns of cloud computing. Many standards exist and more are under development addressing the gaps.

REFERENCES

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, 2009. A view of cloud computing. Comm. Of ACM, 53(4): 50-58.

Buyya, R., C.S. Yeo, S. Venugopal, J. Broberg, *et al*., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, *25*(6): 17.

Buyya, R., J. Broberg and A. Goscinski, 2011. Cloud Computing - Principles and Paradigms. Wiley.

Carney, David, William Anderson and Patrick Place, 2005. *Topics in Interoperability: Concepts of Ownership and Their Significance in Systems of Systems*. No. CMU/SEI-2005-TN-046.

CSA, 2011. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance.

Cisco Datacenter, 2009. Cloud Computing Use Cases White Paper, http://groups.google.com/group/cloud-computing-use-cases.

Cloud Standards Customer Council, 2014. Interoperability and Portability for Cloud Computing: A Guide, Cloud Standards Customer Council, November.

Craig Meyers, 2006. Risk Management Considerations for Interoperable Acquisition, August 2006, TECHNICAL NOTE, CMU/SEI-2006-TN-032.

Grace A. Lewis, 2012. The Role Of Standards In Cloud-Computing Interoperability, October 2012, TECHNICAL NOTE, CMU/SEI-2012-TN-012.

Jerichoforum.org, 2009. Jericho Forum – Position Paper: Cloud Cube Model.

Jean Bozman, 2010. Cloud Computing: The Need for Portability and Interoperability, Red Hat, Inc.

Kennedy, O.O., M.M. Geoffrey, 2012. Challenges in Achieving Interoperability in Distributed Systems:a Survey of Literature, Int. Journal Emerg. Sci., 2(4): 619-631.

Mell, P. and T. Grance, 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, 145(67): 7.

Parameswaran and Asheesh Chaddha, 2009. Cloud Interoperability and Standardization, SETLabs Briefings, 7(7).

Petcu, D., 2011. Portability and interoperability between clouds: challenges and case study. In

Proceedings of the 4th European conference on Towards a service based internet, ServiceWave', 11: 62-74, Berlin, Heidelberg. Springer-Verlag.

Smith, James D., 2006. "Topics in Interoperability: Structural Programmatics in a System of Systems", TECHNICAL NOTE, CMU/SEI-2006-TN-037.

Garg, S.K., *et al*., 2013. A Framework for ranking of cloud computing services, Future Generation Systems, 29: 1012-1023.