Cloud Services Portability for secure migration

1 K.Bhavya , # 2 K.Yamini , # 3 V.Sreenivas
Department of Computer Science and Engineering, K L University, Vaddeswaram, India.
1 Student, # 2 Student , # 3 Professor,

Abstract:

The greatest challenge that is making cloud services untrusty and insecure is portability and interoperability between clouds. Cloud is the latest environment that bring new oppurtunities to the people. The enterprises started to adopt cloud computing to reduce operating and owing cost for communication technology. Also other benefits like increased reliability, decreased latency and on demand scaling are available in cloud computing. The cloud computing industry, cloud service providers are responsible for making sure that the hardware and software components are working together to provide the service requested by the customer in the Service Level Agreement (SLA). This paper mainly consists of challenges regarding vendor lock-in problem and new ways of overcoming it. Cloud portability refers to the ability to move cloud applications from one cloud to another which reduces vendor lock-in problem. Interoperability provides exchange of information between organizations.

Keywords:
Cloud computing, Portability, Interoperability, Security, Migration.

1.Introduction:

Cloud computing is still in the early age of development and suffering from some of the problems like vendor lock-in. Actually vendor lock-in problem arises when a customer can't move the cloud applications between the clouds. Every cloud provider has its own service template. These templates will be different for different cloud providers. Vendor lock-in arises because the semantics of resources and services of cloud providers do not match with each other. Sharing of applications between the clouds will be difficult and so the customer should continue with the same cloud. Portability helps to reduce the problems due to vendor lock-in. Here we are going to discuss about the security issues in the migration of cloud services. TOSCA works to enhance the portability of cloud applications and services. TOSCA will also make it possible for higher-level operational behavior to be associated with cloud infrastructure management. TOSCA will enable portable deployment to any cloud, smoother migration of cloud applications, flexible bursting and dynamic, multi cloud provider applications. TOSCA was introduced by OASIS. TOSCA will provide its own unique service template which can be used by any cloud provider so that portability can be easier.

2.Background:

A. Cloud computing to the public:

Cloud computing is becoming a largest providing vivacious technical environment where innovative solutions and services are being created day by day. Cloud provides cheap and flexible services to the end-users. In cloud the policy of subscribe and use is implemented. So there is no need of installation of any software and the payment can be done to the extent of usage. Cloud computing according to NIST is "a model for enabling 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[3]. There are five characteristics, three delivery models and four deployment models in cloud environment architecture. The five characteristics are On-demand self-service, Location independent resource pooling, Broad network access, Rapid Elasticity and Measured service. The three delivery models are Software as a service, Platform as a service and Infrastructure as a service. Also the four deployment models are Public cloud, Private cloud , Hybrid cloud and Community cloud.

Saas (Software as a service):

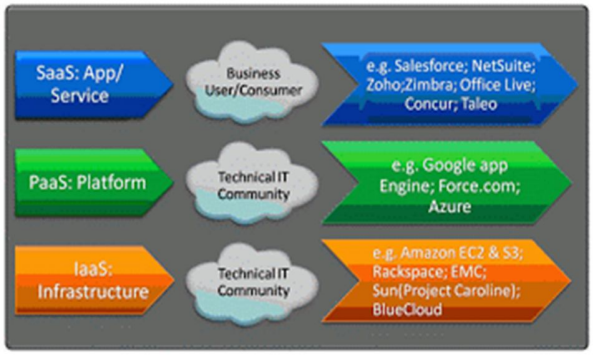
Saas is a software distribution model through which applications are hosted by a customer or service provider and made available over an internet. Saas is also known as Cloud Application Services. Through the Sofware as a service, the consumer need not to install and run the application in his PC which makes things easier for continuation and sustenance. Saas does not perform any command or control over the operating system (OS).

Paas (Platform as a service):

The second delivery model of cloud computing is also known as Platform as a Service (PaaS) or in simple it can be called as Cloud platform services. This model distributes a computing platform as service, over and over again overriding cloud communications and supporting cloud services. The consumer uses a hosting environment for their applications. The consumer is in command of the applications that utilize in the network setting, nevertheless it also does not manage the operating system (OS), infrastructure where they are in use.

Iaas (Infrastucture as a service):

The third delivery model is the Cloud infrastructure services or Infrastructure as a Service (IaaS). IaaS transport computer infrastructure by a platform virtual setting. Instead than paying for new network servers, authorize software or any network tools, cloud users need not to do it but just subscribing to any cloud provider company. This service results to the reduction of finances in any businesses.



The three delivery models

B. Portability and interoperability:

The proliferation of the cloud computing promises cost savings in technology infrastructure and faster software upgrades. The US government, along with other potential cloud computing customers, has a strong interest in moving to the cloud. However, the adoption of cloud computing depends greatly on how the cloud can address users concerns on security, portability and interoperability.

For portability, prospective customers are interested to know whether they can move their data or applications across multiple cloud environments at low cost and minimal disruption. From an interoperability perspective, users are concerned about the capability to communicate between or among multiple clouds.

Cloud providers should provide mechanisms to support data portability, service interoperability, and system portability[6]. Data portability is the ability of cloud consumers to copy data objects into or out of a cloud or to use a disk for bulk data transfer. Service interoperability is the ability of cloud consumers to use their data and services across multiple cloud providers with a unified management interface. System portability allows the migration of a fully-stopped virtual machine instance or a machine image from one provider to another provider, or migrate applications and services and their contents from one service provider to another.

It should be noted that various cloud service models may have different requirements in related with portability and interoperability[7]. For example, IaaS requires the ability to migrate the data and run the applications on a new cloud. Thus, it is necessary to capture virtual machine images and migrate to new cloud providers which may use different virtualization technologies. Any provider-specific extensions to the VM images need to be removed or recorded upon being ported. While for SaaS, the focus is on data portability, and thus it is essential to perform data extractions and backups in a standard format.

The following requirements are related to portability and interoperability for secure migration:

Service entities (for example, VMs) should be able to migrate across organizational and ownership boundaries (for example, between an enterprise and a service provider's IaaS infrastructure).

In the case of a virtualized infrastructure, VM migration should address secure deprovisioning (removal of the VM image after it is ported to a different location or service provider) and partial migration (cloud burst: secure integration between old and new locations and service providers).

Service providers should provide assurance on the consistency of control effectiveness, management,

monitoring, and reporting interfaces and their integration across old and new locations and providers.

If storage migration capabilities are provided, the service provider should have verified functionalities for secure data transfer including encryption, access control, key management, decommissioning of storage devices, and destruction of data after migration.

C. Security:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1. **Integrity**, which means guarding against improper information modification or destruction, and includes ensuring information non-repudation and authenticity;

2**. Confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3. **Availability,** which means ensuring timely and reliable access to and use of information.

TOSCA will facilitate this goal by enabling the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behavior of these services (e.g., deploy, patch, shutdown) independent of the supplier creating the service, and any particular cloud provider or hosting technology. TOSCA will also enable the association of that higher-level operational behavior with cloud infrastructure management.[1]

This capability will greatly facilitate much higher levels of cloud service/solution portability without lock-in, including:

1. Portable deployment to any compliant cloud.

2. Easier migration of existing applications to the cloud.

3. Flexible bursting (consumer choice).

4. Dynamic multi-cloud provider applications[9].

Ultimately, this will benefit the consumers, developers, and providers of cloud-based solutions and provide an essential foundation for even higher-level TOSCA-based vocabularies that could be focused on specific solutions and domains[5].

D. Migration of cloud applications:

Challenges in migration:

Moving applications to the cloud had became more complex today. All applications may not be suitable for deployment to cloud based solutions. This can result in compatability issues for application installation and running , update and un-installation processes leading to the following problems:

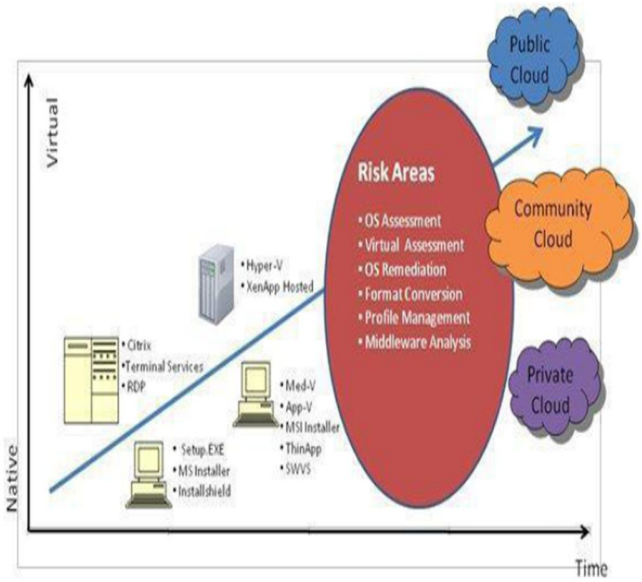
1. OS platform assessment and remediation.

2. Virtualization platform assessment.

3. Application conversion to target platform.

4. Middleware and dependency management.

5. User state and profile management.[4]



Risk areas for migration to the cloud [4].

3. Data in the cloud:

A.Data in the cloud service:

Data in the cloud can be classified into the following categories:
1. User data which means the data that the user inputs into the cloud such as emails, contacts, passwords, transactions etc.
2. Associated data which means the data associated with the user. This data helps the cloud service provider to provide better services.
3. System data: It is used by the service provider to deploy the better services to the customer.

B. Data interchange in the cloud:

Cloud providers should ensure that safeguards are in place to ensure that whatever data they put in the cloud service can be taken out later, for reasons such as integration with another cloud service, a move to a different cloud service, etc.[2] The cloud services should also provide tools, interfaces, documentation, etc. to ensure that a customer can extract, access and interchange the data if such a need arises. Such mechanisms should be designed appropriately to reflect the scale and complexities typically associated with a cloud service used by a government customer. The notion that we can easily move from one provider to another is by science fiction[8].

C. Data privacy and security:

There are different and evolving business models for cloud service providers in the cloud. Some cloud service providers rely more heavily on subscription-based revenues, while others rely on advertisement-based business models, which make the cloud service free or lower cost, in exchange for the rights to reuse user data for commercial purposes and deliver advertisements. Governments should ensure that these trade-offs are well considered and understood before making a decision to choose a particular cloud service[2].

Significant concerns have been recently raised by different stakeholders regarding data privacy, the use of data for commercial purposes and data security in the cloud. Cloud service providers should also provide transparent assurances and terms regarding data privacy; furthermore, the use of data for commercial purposes as well as security should be well understood by the government user community.

4. Conclusion:

The cloud computing environment brings unique opportunities and challenges for various customers. In order to make sure that the cloud computing services are interoperable and portable, governments should focus on setting policies around data portability. Clear policies around data ownership, control, interchange, privacy as well as security will allow governments to harvest the benefits of cloud, while mitigating risk of unreasonable dependence on cloud service providers. The main objective of this paper is to promote portability and interoperability in the migration of cloud services providing security. Cloud providers should understand the challenges in migration and should develop their applications in the way that can be portable easily.

References:

[1] OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC

[2] Shahab Ahmed, Microsoft Corporation “Data Portability: Key to Cloud Portability”.

[3] “Standards for Portability, Interoperability and security in Cloud Computing” NIH Bethesda, Mike Hogan, NIST/ILT Standards Liaison.

[4] “Migrating your application to the Cloud” by Quest Sofware, Inc.

[5] Martin Gilje Jaatun, Costas Lambrinoudakis and Chunming Rong “Special issue on security in cloud computing”.

[6] “Portability and Interoperability between clouds: challenges and case study” by Dana petcu ,Institute e-Austria Timisora and west university of Timisoara, Romania.

[7] “Interoperable and Portable Cloud Cervices” by Anton Panhelainen ,Aalto University School of Chemical Technology.

[8] “Cloud interoperability and portability remain science fiction” by David S. Linthicum , contributor.

[9] “Portable Cloud Services Using TOSCA” by Tobias Binz**:**University of Stuttgart ,Gerd Breiter**:**IBM Boeblingen Laboratory ,Frank Leymann**:**University of Stuttgart ,Thomas Spatzier **:**IBM Boeblingen Laboratory.