Chapter 11
Improving Privacy and Security in Multicloud Architectures

Piyush Kumar Shukla
University Institute of Technology RGPV, India

Mahendra Kumar Ahirwar
University Institute of Technology-RGPV, India

ABSTRACT

In this chapter we described the concept of multicloud architecture in which locally distributed clouds are combined to provide combined services of locally distributed clouds to the users. We started with basic of cloud computing and reached to multicloud through single cloud. In this chapter have described four architectural models for multicloud. Architecture models are Repetition of applications, Partition of System architecture into layers, Partition of Security features into segments and Distributing of data into fragments with these models security of the data resides in the datacenters of the cloud computing must be increased which leads to reliability in data storing of data.

CLOUD SERVICE MODELS

The services provided by the cloud computing are divided into three universally accepted categories these are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Basically these three service models are interrelated to each other and designed 3-tiers architecture.

Infrastructure-as-a-Service (IaaS): This is first and base layer of 3-tier architecture. It is used to provide network for connecting users and servers and also provides virtual machines to start, stop, access and configure virtual servers and storage blocks. Pay-per-use service is implemented at this layer of 3-tier architecture. Examples of IaaS are Amazon EC2, Windows Azure, Rack space, Google Compute Engine etc. Infrastructure-as-a-Service like Amazon Web Services provides virtual server instance API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because

DOI: 10.4018/978-1-4666-8387-7.ch011

this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed; it's sometimes referred to as utility computing.

Platform-as-a-Service (PaaS): This is second or middle layer of 3-tier architecture. In this model a platform is provided to users which typically include operating system, programming languages, execution environments, databases, queues and web servers. Examples are AWS Elastic Beanstalk, Heroku, Force.com and Google App Engine. Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and GoogleApps are examples of PaaS. Developers need to know that currently, there are not standards for interoperability or data portability in the cloud. Some providers will not allow software created by their customers to be moved off the provider's platform.

Software-as-a-Service (SaaS): This is third or upper layer of 3-tier architecture. This model provides "On-demand software's" to users without installation setup and running of the applications. Users have to pay and use it through some client. Examples are Google Apps and Microsoft office 365.In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere. 3-tier Architecture of cloud computing has been illustrated in figure -1.

In case of public cloud services provisioning at SaaS layer creates number of issues among which security and privacy are most critical aspects when considering adoption of cloud computing. SaaS also faces challenges on the outsourcing of services, data, applications and processes in case confidentiality and sensitivity.

An idea to reduce the risk for data and applications at SaaS layer of public cloud is to use multiple distinct clouds simultaneously. In this paper four distinct cloud models are provided which can offer services to users according to their security and privacy benefits.

Cloud Types

There are four types of clouds: private cloud, public cloud, community cloud and hybrid cloud from the physical location of user's point of view.

Private cloud: A *private* cloud is one which is setup by single organization and installed services on its own data center. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. The types of cloud has been illustrated in figure 2.

Public cloud: A *Public* cloud services are offered by third-party cloud service providers and involve resource provisioning outside of the user's premises. A public cloud sells services to anyone on the Internet. Currently, Amazon Web Services is the largest public cloud provider.

Community cloud: The *Community* cloud can offer services to the cluster of organizations.

Hybrid cloud: A *Hybrid* cloud is the combination of any two or more types of above mentioned cloud types.

A cloud can be of any type but the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Single Cloud

Cloud computing is a conversational expression used to describe a variety of different types of