International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Cloud Computing: Hybrid Cloud over Simple Cloud Computing

Prof. HANMANTHRAO KULKARNI CSE BKIT
SACHIN KULKARNI (M.Tech)

Abstract: **Cloud implementations will be hybrids of services that run on-premise with services deployed in the cloud. Cloud is also increasingly leveraged by IT. IDC estimates that public cloud adoption will account for 46 percent of new growth for overall IT spending.1 This rate and pace of adoption is very similar to the early acceptance and expanded use of virtualization technology over the last five years.So that is the scenario that we'll explore so that you can begin a gradual move into the cloud without undue fear of loss of control. You will learn how to control applications and services dynamically deployed from a variety of cloud environments into devices like user desktops, Microsoft Terminal Services and a range of mobile devices. In this paper our goal is to evolve from control of computers to control of services available to users. This takes existing Service-Oriented Architecture (SOA) and machine virtualization to the next step. The result will be increased business productivity with less overhead, as the user will be able to work anywhere on any capable device without any worry about application deployment.**

1. INRODUCTION

Cloud computing has become a necessity now adays when an enterprise plans to increase its' capacity or capabilities on the fly without investing on new infrastructure, training new personnel, buying new software licenses etc. It encompasses any subscription-based or pay-per-use service that extends the enterprise's existing IT
capabilities, in real-time over the Internet.

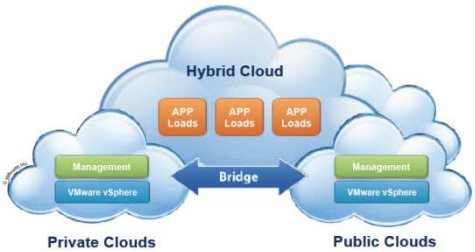

Figure 1: Hybrid Cloud Model

The market research and analysis firm IDC suggests that the market for cloud computing services was $16bn in the year 2008 and will rise to $42bn/year . The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage,
applications, and services) that can be rapidly provisionedand released with minimal management effort or service provider interaction" . Cloud computing can also be defined as "a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presentedas one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers". In recent past, various commercial models are developed that are described by "X as a Service (XaaS)" where X could be hardware, software or storage etc. Successful examples of emerging cloud computing infrastructures are Microsoft
Azure, Amazon's EC2 and S3, and Google App Engine etc.
Cloud computing also faces the data security challenges as that of any other communication models. As data owners store their data on external servers, there have been increasing demands and concerns for data confidentiality, authentication and access control.

2. DELIVERING CLOUD SERVICES ACROSS DIFFERENT ORANIZATIONS

The above are generalizations of the ways that organizations of different sizes approach the web. Small organizations and small departments within large organizations typically pick a complete software solution like email or office productivity applications.

Organization Size	**Authentication**	**Collaboration**	**Typical Cloud Use**
Small organization, up to 25 users	Workgroup	Individual	Applications like email
Medium organization up to 250 users	Domain	Federation	Platform, database, ERP
Enterprise class organization	Multiple domains	Dedicated	Load and location leveling

Axis 1 **Delivering services to three broad sizes of customer organization**

These solutions are isolated from the organization's other IT resources and offer fixed management control experiences that are a part of the total solution.
Once an organization gets to the size where they can fund a full time IT administrator they will look at more personalized cloud solutions where they have more control over the

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

application. New projects can start completely in the cloud when they have no important dependencies on existing business data. Projects which involve extensions to existing on-premise applications will have greater dependency on on-premise servers and hence are more difficult to move into the cloud. Larger enterprises will take on even more flexibility by renting virtual images on machine managed by external or internal cloud providers.

Offering	Type	Industry	Microsoft
SaaS: Application Software as a Service	Fixed apps like email, ERP,	Salesforce	BPOS, Office 365, Windows InTune
PaaS: Platform as a Service	Controlled space for apps or Database	Google, Facebook	SQL Azure, Azure App Fabric
IaaS: Infrastructure as a Service	Complete access to dynamic VMs	Amazon AWS, Private Clouds	Windows Server Hyper-V

Axis 2 **Delivering services at three broad depths of engagement (Service Models)**

This axis is focused on the vendor product solutions rather than the customer needs like the first axis. Vendors must commoditize the service offering to keep costs low, so it is incumbent on the customer to assure that the service level agreement (SLA) from the vendor will meet their performance expectations. At each step in the service offering, from software to platform and infrastructure, the customer assumes more and more of the management load in exchange for more and more flexibility in the service offering.

3. MANAGEMENT CONTROL AS A SERVICE

A big problem created by hybrid clouds is that there is a duplicated set of IT controls: one on-premise in the enterprise Active Directory, and one in the Cloud under a different name-space. That separation means that there is a synchronization problem between these broad deployment areas. All of these services need to be controlled by the customer.

That control function is sometimes described as a separate service which could also be run on-premise or in the cloud, but really it is just another application. Whether the control application is supplied by SAAS, PAAS, IAAS or on-premise is not as important as determining a control architecture and solution management software that will work for the entire organization in a hybrid environment. After a solution is chosen, the location where that solution runs will be easier to determine.

One case where management has been deployed as a service is Microsoft InTune. For a low monthly fee for each PC, it adds cloud management of the PC together with an upgrade subscription. Using the same anti-malware client code as Microsoft Security Essentials (MSE) and Forefront Endpoint Protection (FEP) it provides small to medium organizations with robust anti-malware protection to any location accessible to the Internet. For hybrid clouds, it's important to note that management is a service that needs to be hosted somewhere with collectors in all of the locations where the cloud infrastructure is deployed. Until recently management of the cloud meant management of the virtual machines that are the core infrastructure for the cloud. An example is System Center Virtual Machine Manager (SCVMM) which provides for centralized management of physical and virtual on-premise servers. But as more organizations deploy hybrid environments, the inability of existing tools to manage two disparate and often incompatible domains has become clear.

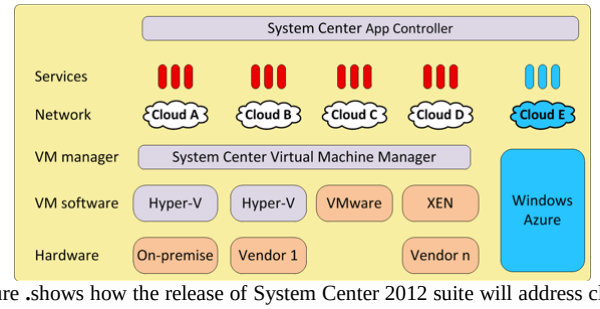

Figure .shows how the release of System Center 2012 suite will address cloud management issues

While SCVMM will be upgraded and continue to support individual cloud deployments, a new System Center product called App Controller (code name was Concero) will offer control of multiple cloud deployments, both private (on-premise) and public (Azure). For the 2010 RTM release there will be support only for public Azure and private deployments but other vendors are expected to take advantage of its extensibility. For example, Citrix has already announced that XEN virtual machines will be included in App Controller soon after RTM.

This continues a process where the cloud provider shields the IT department from all concern about deploying and maintaining the hardware of servers and routers. The cloud infrastructure as a service (IaaS) can be assumed to exist, and IT staff should focus on providing applications and services to the organization.

4. USE ORIENTED ARCHITECTURE

While the next generation of management tools is responding to the hybrid cloud trend, another important trend to address is the so-called bring –your-own-device (BYOD) trend – that is, users accessing corporate resources with personal hardware.

Again, the major management solutions are responding. For example, user-centric application delivery is enabled with SCCM 2012 and focuses on providing extreme mobility of a specific resource for a specific user. IT focus is moving from work-life balance to work-life integration. Users expected to

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

be able to work anywhere, anytime so the solutions and their architectures need to be designed with that as a primary goal.

The SLA guarantees on up-time needed to support this must be at least 99.9 percent with better guarantees possible as the technology progresses. For on-premise computing the focus has been on insulating the service offerings from cloud outages, but as users increasingly are moving off-premise, there are fewer services that must operate when the Internet is unavailable. It has been possible since Windows 2000 to offer fine-grained policy and application deployment, specified to the level of the individual user, but that capability has not been widely used because of licensing and device limitations. Device affinity is now available in SCCM 2010. If the user is not on one of their "primary devices" then the strategy is to provide them some other type of access like Terminal Services or Office 365.

Since not all devices have the same storage or other resources, application deployment options need to understand device capabilities. If the IT infrastructure is to provide user access to any document, anywhere, it needs to adapt to the device. For example, Windows Phone 7 comes with a version of Microsoft Office. So if the user is accessing a Word document from a smart phone, in some cases the Word document can be downloaded to the smart phone, but in other devices the document will need to be rendered on a web or terminal server to allow remote access to the document.

This is a different way of thinking about application deployment in which the industry is moving from managing the workstation to adapting to users and their devices. The implication is that commercially successful applications will need to be available for all common deployment mechanisms in order for management software to succeed in providing anywhere access.

5. AUTHENTICATION OF THE CLOUD SERVICES

Security breaches have taught us to ensure that both ends of any connection are well known. Microsoft Terminal Services added TLS (aka Schannel) protection to ensure that users were not spoofed by rogue servers masquerading as official sites, or creating a man-in-the-middle attack. These types of attacks are prevented by authentication of both ends of any connection.

Virtual private networks (VPN) have long been used as a gateway for securely accessing organizational assets.

If users are not part of the same security domain, the best available solution is TLS with certificates issued to all machines (or users) that need to trust each other. Today, web servers can acquire enhanced validation (EV) certificates to use in TLS connections. Users can additionally be authenticated by smart cards as a part of TLS mutual authentication. However, the difficulty of deploying certificates and private keys to end users has caused most user authentication to fall back to user names and passwords for authentication.

6. CONTROL OF THE DATA IN THE CLOUD

There are two aspects to the control of data in the cloud. The first is whether the data should be placed in the cloud at all. If the data is moved to the cloud, the second control aspect is how to prevent it from leaving the cloud. The physical location of the data may be important when corporate or governmental compliance is a factor. The management control programs will need to be able track compliance with policy restrictions.

As we observed above, it is critical that IT take a proactive approach to setting policies for corporate data and cloud computing, otherwise some other business group at your organization may effectively make the decision for you. As one example of data creep, the need for data access authorization in the cloud carries with it the idea that some authorization claim will need to be presented to those cloud servers. Next we will consider the authentication of users and then the authorization of their access to cloud resources.

7. SINGLE SIGN ON

The advantage of having a single point of control over users' access to any organizational assets should be clear. Central control of user authentication credentials allows immediate and full revocation of access to all organizational assets when that user is no longer part of the organization. Central control also provides consistent policy for attributes like password strength.

Extending centralized authentication policy to cloud resources provides not only continuity of control but also maximizes user convenience so that the user need not provide different credentials based on the location of the resource. This will be particularly important as resources migrate to the cloud over time.

The history of web started in the middle 1990's and has not resulted in a widely acceptable solution as yet. The current successes are with a federated approach using SAML which assumes that a user is already well known in one namespace and needs to establish authorized access in another. A federated ID does not provide a broad web based solution that would accommodate all of the services currently under development for cloud based services.

OAuth 2.0 is a new protocol that extends the architecture of OAuth 1.0 to allow for selective disclosure of the type needed in a world where user privacy is mandated by so many government regulations. Even though it has not reached final approval, parts of it are already supported by Microsoft and other identity solution providers. Until identity providers are more broadly deployed the only practical solution is federated identity. Stay tuned for more on web SSO in the near future.

8. CLOUD ACCESSIBLE AUNTHENTICATION DIRECTORY

As applications are placed in the cloud, the need for the databases to support those applications implies that access to

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

the data will be available to the cloud. There will be little incentive to keep the database on-premise if any significant application for the database is in the cloud.

Authentication data is a good example. The authoritative source of the authentication information is typically some HR or customer database that is synchronized with one or more IT directory servers. While it customary for the directory servers to be on-premise, it is a good idea to examine the need for authentication to cloud resources. For example, if email servers are to be provisioned in the cloud, then the implication is that the address list will also be in cloud.

Once that decision is made there is no longer much of a privacy implication to putting the entire organizational directory server in the cloud as well. The cautionary result of any decision to move applications to the cloud is that database requirements will migrate to the cloud as well. Once access to the database is enabled from the cloud, there is little reason not to move the database itself to the cloud and allow on-premise application access. As an optimization, read-only copies of any directory service will support faster response and resilience in the loss of network connectivity.

9. CLOUD ACCESSIBLE AUTHIRIZATION

If cloud accessible authentication information is not politically acceptable, then some other method for authorizing access in the cloud needs to be enabled. When authorization claims are demanded by relying servers in the cloud, the local policy can make just-in-time decisions about which data is permitted on a case-by-case basis. The SAML and OAuth2 standards have some of that capability today, but a general solution is awaiting the completion of a protocol that will enable a business model for identity providers.

Until then a federated solution with data release policy applied to each federated organization is the only solution. The key to broader availability of selective disclosure is choosing an identity provider, so that is the decision that needs the most attention as the organization moves its resource into the cloud. The reality is that SAML has only been adopted by 10-20 percent of the market according to Forrester, Gartner and others. OpenID and HTTP Federation are also very useful in federating the widest range of existing user stores and SAAS applications.

10. CONCLUSION

Cloud services will be part of the future of every IT department sooner or later, it is critical for the IT professional to get ahead of the coming onslaught. Three areas will need the most attention in advance of any move into the cloud.

1. Management of the hybrid cloud is an evolving area that will need the most attention because it is currently the least understood. Try to spend some time exploring management tools like System Center App Controller.
2. User authentication and directory services will be needed anywhere that employees or other users expect to access organization resources. Since some governments have strict rules about the locations of private data, try to determine where the authoritative data will reside and how it will be migrated to the other clouds that need it.
3. Access control and data leak prevention will become more difficult as data migrates to the cloud. As a goal, a role-based access control mechanism base on SAML claims seems to be the best bet today for providing the required functionality.

REFERENCES

[1]. Eoin Gleeson, Computing industry set for a shocking change, MoneyWeek, April 2009: from http://www.moneyweek.com/investment-advice/computing-industry-set-for-a-shocking-change-43226.aspx
[2]. Peter Mell, and Tim Grance, Draft NIST Working Definition of Cloud Computing, 2009: from http://csrc.nist.gov/groups/SNS/cloud-computing/
[3]. R. Buyya, C. S. Yeo, and S. Venugopal, Market oriented cloud computing: vision, hype, and reality, for delivering IT services as computing utilities, *Proc.* 10th IEEE International Cognference on High Performance Computing and Communications, Dalian, China, Sept 2008.
[4]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the clouds: A berkeley view of cloud computing, University of California, Berkeley, Tech Rep USB-EECS-2009-28, Feb 2009.
[5]. David Chappell, Introducing the Azure Service Platform, White paper, Oct 2008.
[6]. Amazon EC2 and S3, Online at http://aws.amazon.com/
[7]. Worldwide and Regional Public IT Cloud Services 2011–2015 Forecast, IDC, June 2011.
[8]. IDG Research, "CIO Global Cloud Computing Adoption Survey," January 2011.
[9]. "Key Issues for Securing Public and Private Cloud Computing, 2011," John Pescatore, Gartner Research.
[10]. "Cloud Security Fears Exaggerated, Says Federal CIO," Patrick Thibodeau, Computerworld, July 28, 2011. (http://news.idg.no/cw/art.cfm?id=62DE7B46-1A64-67EA-E4E3D0EB9C453EC5)