Addressing Security issues for Enterprises Migrating to HYBRID Cloud Computing Model

Sanjay[1]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India
sanjay.kanti@gmail.com

Shabnam Sangwan[2]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India
shabnam022@gmail.com

Sachin[3]
Deptt. of CSE
Sat Kabir Institute of Technology & Management (SKITM)
Bahadurgarh, Haryana, India
sachind12@outlook.com

Sunita Sangwan[4]
Deptt. of CSE
P.D.M. College of Engineering (PDMCE)
Bahadurgarh, Haryana, India
sunita2009@gmail.com

***Abstract*:** Although on premises deployment has been a reliable platform to deploy in house applications & production software's like email, ERP, Web servers, database for long, but managing the datacenter, applications, & specially the upgrade path for the newer version of software was always a challenge for the enterprises. Today, considering the rapid growing market of cloud computing, many organizations are keen to adopt the cloud platform. Cloud computing technology drawn the attention of IT world and is now days changing the focus of enterprises too.

For enterprise with confidential data, major concern has become the security of the data while migration & then storing it on cloud. An organization can only decide to adopt cloud considering the benefits to risk ratio. This paper is focused on the security issues of cloud computing for migrating the enterprise data like email services, BI applications to Cloud. Before analyzing the security issues, the definition of cloud computing and brief discussion on available cloud models Iaas, Saas PasS are described. The Final section has solution suggested to migrate enterprise identities, roles & permissions to cloud. Federation between the organization & cloud servers is the suggested approach for user data & credential sharing to access applications on cloud

Keywords*: Cloud Computing, Identity Management, Cloud Security Issues, Public key Infrastructure, Enterprise Applications, Domain Identities, Tenant, Federation*

*****

I. INTRODUCTION

The continued growth of the cloud services market has result from the adoption of cloud services for production systems and workloads, in addition to the earlier development and testing scenarios that have led as the most prominent use case for public cloud services to date.[1] The cloud computing model has gone through various evolution phases starting from Mainframe, (a large computer store all data of all application) to PC, a small personal computer & finally to Cloud Computing, an ideal solution for both small & larger enterprises.In Cloud computing the organizations save huge hardware cost in deploying Client/Server architecture model, overall client side requirements and complexity. Since the cloud computing has become the widely accepted model for medium to large organizations, the security issues has become the prime consideration of this new model. Organizations consider the security of their data in transit while migration to Cloud & then the mechanism to access data by end users from cloud.

In this paper we have attempted to identify the security challenges in a hybrid cloud environment and suggested an approach to access the data in Hybrid cloud using authentication & authorization from on premise directory solutions. The concept of federation between on premise datacenter directory service & cloud is detailed. This paper proposes a security solution, which leverages organizations from the security of their user identity/login credential, by creating a federation trust. The research methodology adopted towards achieving this goal, is based on Microsoft Active directory federation services. [2]

II. ABOUT CLOUD COMPUTING

As mentioned in the NIFT "Cloud computing 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] . Like an administrator while testing an application can demand for additional resources like RAM or processor cycles & release with minimum efforts. Considering from the user point of view, they see cloud as a single application, device, or document. All hardware, network devices are invisible to user. Amazon is the widely known cloud services provider along with providers like Apple, Cisco, Citrix, IBM, Joyent, Google, Microsoft, Rackspace, Salesforce.com and Verizon/Terre mark. The virtualization is one, of many, multi-tenancy strategies in cloud computing. Although not all cloud service providers uses Virtualization but this is also an emerging technology along with Cloud computing. Since we have large number of options of cloud service provider these day, below are some guidelines by NIFT as characteristics of cloud computing [2,]:

A. Characteristics of Cloud Computing

Measured Service/Pay as you use. Services provide to customer should be metered as per the services purchased by customer.

Economies of scale and cost effectiveness: Datacentres should be provisioned considering environmental factor & availability of resources like power stations, low cost land etc. Future scale should be considered in cloud Datacenter design. [2]

On-demand resource availability. Customer should have flexibility to choose the hardware & software requirement for the services they have purchased. These facilities to be provided to end user or administrator with service provider's intervention. Also releasing the resource should be automated.

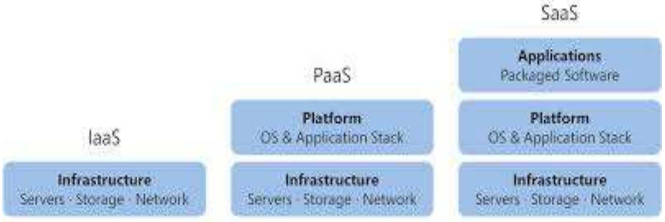
No End device dependency: Customer should have option to access services from various mode e.g., mobile phones, laptops, and PDAs.

Resource pooling. In Multitenant scenarios the resources are pooled across various customers & customer is not even aware of the Geo locations. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Unlimited Scalability in no time: Cloud setup has to be so flexible that customer should be able to increase the utilization without any resource limitation. Cloud setup should be flexible to quickly scale out and rapidly released to quickly scale in.

B. Cloud Computing Service Models:

Based on the service provided the cloud providers provide three different services based on different capabilities such as SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) [3]



1. **Infrastructure as a Service (IaaS):** In this Model the cloud service provider gives the basis infrastructure like storage, server, and network connectivity. Customer can login to the cloud services & install their own applications Eg. Microsft Azure IaaS model

2. **Platform as a Service (PaaS):** Platform as a Service (PaaS) fills the needs of those who want to build and run custom applications as services. . Installed application are provided by cloud provider & customer can custom those application as per their requirement. No need to get worried about the Operating system patching, OS failover/outage etc. Typical examples are Google App Engine,Office 365, Mosso ,AWS: S3.

3. **Software as a Service (SaaS):** Software as a Service (SaaS) is a software delivery business model in which an application is installed by service provider and makes it available to customers on a subscription basis. SaaS customers use the software running on a pay-as-you-go basis. Like Microsoft o365 is most widely used SaaS model for Email, Lync, SharePoint & other applications. Subscriptions are given on monthly basis or yearly basis. [3]

C. Cloud Computing Deployment Models

Four deployment models have been identified for cloud architecture solutions, described below:

1. **Private cloud.** Generally created by the organization or third party. Any private Datacenter run by a large enterprise can be called a private cloud if it takes advantage of the unified resource model enabled by broader virtualization and takes advantage of highly automated processes for operating the system.
2. **Community cloud.** The cloud infrastructure created by several organizations and supports a community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.
3. **Public cloud.** The most widely used model these days. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Azure, Amazon Web Services, Google App Engine and Force.com are a few examples of public clouds.
4. **Hybrid cloud.** In hybrid model two or more clouds are bound together Few of the services and workloads are run in one cloud while few run in other cloud. [5,3]. E.g. certain component email services run in on premise private cloud while few users created in Azure cloud

III. Hybrid Model Security Checks For Enterprises

The hybrid cloud model can be the best deployment model for the large organizations with high number of applications & large database size. In a scenario when the large database and business critical applications cannot be migrated to cloud overnight, hybrid deployment becomes the only option for organizations moving to cloud. Organizations can decide to be in hybrid deployment for short term duration or may be forever based on the organization policies. As truly said in below lines

"The hybrid cloud model makes a lot of sense in large organizations," says Janel Garvin, CEO of Evans Data,

"As security concerns lessen, many might move more of their computing resources out to the cloud. But some may keep a hybrid model for years to come."[7]

According to the recent survey conducted by symantec [6] 83% of enterprises rated security as important criteria to be considered in hybrid clouds. 79% said backup and recovery and 76% rated continuous data protection as one of their top initiatives. Let us examine the security challenges that appear when the enterprise decides to move their components to a hybrid cloud.

"The hybrid cloud model makes a lot of sense in large organizations," says Janel Garvin, CEO of Evans Data, a market research firm in Santa Cruz, Calif. "As security concerns lessen, many might move more of their computing resources out to the cloud. But some may keep a hybrid model for years to come."[7]

MIGRATING TO THE CLOUD – Prior to take a final call to migrate data to cloud, all organizations access the data migration mechanism, reliability of migration channel, internet connectivity service provider, security threats during the data migration & finally the security of data in the cloud after migration. All the possible scenarios are discussed with the application owners, IT leads & the cloud service providers. After evaluation of the migration feasibility, a draft plan is published to all stakeholders. All well proven security technologies and best practices like secure tunnels and VPNs are measured before concluding the final plan.[8]

Following are the prime security considerations in Hybrid deployment Model: [9]

Identity management: The very first question arise in terms of identity management is weather to use an on premise identity management system or cloud based identity management solution. Federation enable a customer to use on premise user identity to access applications hosted purely in cloud or in hybrid model. Cloud based identity management are purely managed on cloud and customer is allowed to access & create identities

Cloud Datacenter Security, certification & compliance: Be it a hybrid setup of private – public cloud or private – private cloud, all the security measures in the Datacenter are evaluated by the customer. There are various well known auditing standard like SAS 70, SSAE 16, SOC 2 and SOC 3 for data centers . [17]. Customer may have internal compliance & audit points which are examined with the cloud datacentres. There are legal guidelines by the government for Public sectore units which need to be consulted before planning the hybrid migrations

Application Security & integrity: – Customer like banking sectors may have applications which store critical user data like credit card details, password & PIN number. The more critical the data is, more worried the customer will be before considering cloud based solutions. Security measures to be placed to block unauthenticated & unauthorised access to these application databases.

Data Migration/Synchronizing Channel: In hybrid deployments data keep synchronising between the datacentres. For example in hybrid based database solutions, where customer is looking for a disaster recovery solutions, one copy of database can be placed in Private & one in Public cloud. Real time synchronization happen in between. TLS & VPN based security mechanism should be placed to avoid data hacking.

Legal & SLAs: The customers should negotiate in terms of liability, intellectual property, and end-of-service (when data and applications are ultimately returned to the customer). In addition, there must be some considerations for acquiring data from the cloud that may be involved in litigation.[15] These issues are discussed in Service-Level Agreements (SLA).

IV. PROPOSED SOLUTION OF SECURING IDENTITY MANAGEMENT IN HYBRID MIGRATION & DEPLOYMENT

User Identity management & Application authentication:

On premise Directory Servers: To all application, whether they run in on premise or in the cloud, an authentication mechanism is build. All applications are accessed through a unique identity for a user. Based on the credential provided by user, the application consider its authentication & authorisation to access that application.

There are various authentication servers like Microsoft Active directory, Novell directory, IBM Tivoli etc. which can be configured to store user credentials. LDAP an open source directory access protocols is used to access/lookup directory servers. [10] Applications are configured to integrate with these directory servers and only authenticated users from these directory servers can be allowed to access these applications.

Every Cloud providers either provide an identity management solution configured in cloud or sometime integrate the organization's identity management system, using federation or SSO technology. The decision is taken based on the organizations decision after considering the aspect of securing the Identity management.[14]

Concept of Federation Identities:

When an application is migrated to HYBRID cloud, the on premise authentication (user credential) won't work, since the cloud will have separate directory servers and authentication mechanism. To overcome this situation the possible solutions could be

1) *Either migrate on premise directory server to hybrid cloud (which organizations may not accept due to security compliance)*

2) *Or Configuration federation between on premise & hybrid cloud (Proposed solution in this research)*

Types of identities in Hybrid cloud Deployment scenario:

- Cloud Identities; Created on identity management solutions on Cloud itself
- Federated Identities. Created on premise Directory server & federated using organization federation relationship.

Federation of identity allow the use of identity information across independent security domains. The goal is to enable users of one domain to securely access data or systems of another domain without entering credentials again. In addition to use the same ID across multiple autonomous domain, it also enable SSO (single sign on concept) which enable an organization to identify and authenticate a user once, and then use that identity information to get access of multiple applications. [15]

Hybrid cloud Scenario: Following hybrid scenario to be thoroughly examined to reach the final conclusion on federation Identities. Microsoft Office 365, Azure being the largest growing hybrid deployments is used as test case for validating the hybrid deployment with Federated Identity management solution.

In the scenario, ADFS farm & ADFS proxy servers are deployed in the on premise solution & a federated trust is created between on premise private cloud & Microsoft office 365 public database. Services accessed from the Microsoft Datacenter are **based on PaaS model.**

A Federation Trust created between the on-premises Active Directory and the cloud solution when using Federated Identities in a Hybrid cloud solution. This Federation Trust enable users from the on-premises Active Directory to access the cloud services. [13]

Below diagram detail the hybrid deployment scenario:

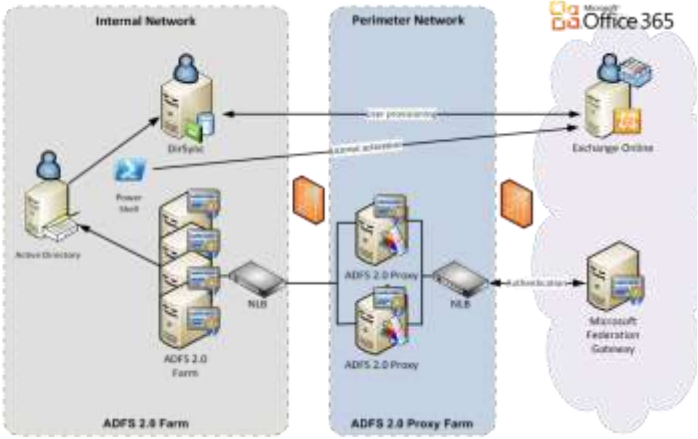


Fig.2: Networks

V. Conclusion

Prior to taking a final decision of moving to cloud model & finalizing which cloud model to accept, this is essential for an organization to consider all the security issues they may face based on the company security compliance. In government organization like Public sector banks, PSU & other government aid companies, they abide by the laws publish by governing authorities. Considering the confidentiality of data while migration & after migration in cloud, it is advisable to understand all the security standard followed by the cloud service provider. The customer has to look for the possible solutions, that can be carried out to protect their applications, services and data.. In this research we have explained the various challenges in Hybrid migration & Hybrid deployment scenario and have suggested a solution for securing the Authentication mechanism using federated ID solution for the Identity management. The concept of SSO (single sign on) help organization users to keep the single password for the on premise & cloud applications. Many federation services are available in the market to enable the federation in hybrid deployment scenarios.

VI. Future Scope

Federation identity in case of hybrid security is explained here and the future work can be carried out for the optimization of security work as an idea to ensure the data confidentiality in migration & hybrid deployments.

Acknowledgment

I would like to thanks my guide Ms. Shabnam Sangwan, who suggested me to work and research. Her recommendations, innovative ideas and constructive criticism contributed to make the success of this report. Her numerous suggestions, comments, and advice have made this entire paper possible.

References

[1] Gartner.com http://www.gartner.com/newsroom/id/2352816

[2] Federation Identities in Microsoft : https://technet.microsoft.com/en-us/magazine/ff721824.aspx

[3] NIST Definition of cloud computing : Authors: Peter Mell and Tim Grance Version 15, 10-7-09 National Institute of Standards and Technology, Information Technology Laboratory

[4] G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, in: Theory in Practice, O'Reilly Media, 2009.

[5] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009).

[6] R. Buyya, S. Pandey, and C. Vecchiola, Cloudbus toolkit for market-oriented cloud computing, in Proceedings 1st International Conference on Cloud Computing (CloudCom 09), Beijing, 2009, pp. 3_27.

[7] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.Principles of Information Security By Michael Whitman, Herbert Mattord

[8] Symantec 2010 State of the Data Center Global Data. Technical report. http://www.symantec.com/content/en/us/about/media/pdfs/ Symantec_DataCenter10_Report_Global. pdf.

[9] http://www.csoonline.com/article/2127157/cloud-security/hybrid-cloud-computing-security--real-life-tales.html

[10] http://ww2.frost.com/files/1614/2113/3098/Whitepaper-VMware_Bluelock_Security_In_The_Hybrid_Cloud.pdf

[11] http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol [Wikipedia directory access protocol description]

[12] http://cloudtimes.org/2013/02/21/analyzing-security-challenges-in-the-hybrid-cloud/

[13] https://www.simple-talk.com/cloud/software-as-a-service/cloud-identities-versus-federated-identities-in-office-365/http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[14] http://en.wikipedia.org/wiki/Cloud_computing_security [Security & Privacy section]

[15] http://en.wikipedia.org/wiki/Single_sign-on [concept of federation identity management]

[16] R. Buyya, S. Pandey, and C. Vecchiola, Cloudbus toolkit for market-oriented cloud computing, in Proceedings 1st International Conference on Cloud Computing (CloudCom 09), Beijing, 2009, pp. 3_27.http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx

[17] http://www.datacenterknowledge.com/archives/2011/03/03/sas-70-ssae-16-soc-and-data-center-standards/ [datacenter standards]