Security Aspects of Multi-Cloud Computing In Modern Computing Environment

Swapnila Mirajkar[1], Santoshkumar Biradar[2]

[1]*Student, Dept of Computer Engg,Dr D Y Patil College ofEngg, Ambi, University of Pune, M.S, India*

[2]*Asst. Proff, Dept of Computer Engg,Dr D Y Patil College of Engg, Ambi, University of Pune, M.S, India*

ABSTRACT:*Cloud computing has been equated to the early proliferation of electricity. Businesses and towns began connecting into a greater power grid, supported and controlled by power utilities. There came time and cost savings, along with this utility connection in addition to greater access, and more reliable availability of power. Similarly, cloud computing represents a significant opportunity for service providers and enterprises. Relying on cloud computing, enterprises can achieve cost savings, flexibility, and choice for computing resources. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" is becoming popular now days. This paper focus the aspects related to security of single to multiple clouds.*

Keywords:*Cloud Architecture, Cloud Security,Multi Clouds,Security Challenge.*

I. INTRODUCTION

Cloud Computing can be visualized as rapidly evolving landscape. Many organizations are using cloud computing deliberating its benefits, but the major issue that has arisen is security. Cloud Computing isn't necessarily more or less secure than your current environment. As with any new technology, it creates new risks and new opportunities. As data been shared with third party in cloud computing, both users and service providers should take of security issues.

As per the research security issues has become less in multi clouds as compared to single cloud. The movement towards multi clouds is gaining increased popularity now days. The multi cloud deals with the security issues like data integrity, data intrusion and service availability in the cloud effectively. Despite the fact that we cannot assure complete security in the multi clouds. This is because if the hacker attacks the server which is related to the multi cloud environment he can easily hack our valuable information. But before going to any technology user will always think about security if it involves confidential data like credit card number ,so as for cloud computing.

II. BACKGROUND

In NIST Cloud Computing is defined as "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). There are five characteristics, three delivery models and four deployment models in cloud environment architecture [1]. The five characteristics of this modern computing are On-demand self-service, Location independent resource pooling, Broad network access, Rapid Elasticity and Measured service. It has three delivery models which are : infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The deployment models are public, private, hybrid and community models[4].Each of which has its own benefits and depending on type and service requirements of organization they are used. But beside its benefits the security challenges it faces makes it difficult to use.

Fig. 1 describes cloud computing architecture. Cloud service providers are there to provide various services to cloud computing clients.

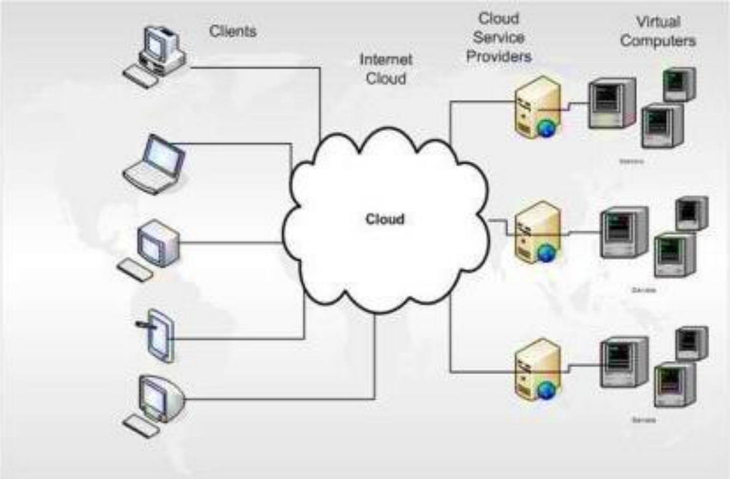

Figure 1: Cloud Computing Architecture

III. CHALLENGES IN CLOUD COMPUTING

Adopting cloud computing involves many challenges.The security requirements for cloud computing providers would appear to be the same as traditional datacenters at first glance.Internet security problems will affect the cloud, withgreater risks due to valuable resources stored withinthe cloud and cloud vulnerability. The technology usedin the cloud is similar to the technology used in theInternet. The following abstracts some of the primary security concerns that enterprises should think about when planning their cloud computing deployments[8].

Cloud providers should consider adopting as a security baseline the most stringent requirements of any customer. To the extent these security practices do not negatively impact the customer experience, stringent security practices should prove to be cost effective in the long run by reducing risk as well as customer-driven scrutiny in several areas of concern.

3.1 Virtual Machine State and Continuous Network of Urban Communities

Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. In cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

3.2Administrative Access to Servers and Applications

One of the most important characteristics of cloud computing is that it offers “self-service” access to computing power, most likely via the Internet. In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via the internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in system control.

3.3Vulnerability exploits and vm-to-vm attacks

Cloud computing servers use the same operating systems, enterprise and web applications as localized virtual machines and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. In addition, co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention systems need to be able to detect malicious activity at the virtual-machine level, regardless of the location of the VM within the virtualized cloud environment.

3.4Securing Dormant Virtual Machines

Unlike a physical machine, when a virtual machine is offline, it is still available to any application that can access the virtual machine storage over the network, and is therefore susceptible to malware infection. However, dormant or offline VMs do not have the ability to run an antimalware scan agent. Dormant virtual machines may exist not just on the hypervisor but can also be backed up or archived to other servers or storage media. In cloud computing environments, the responsibility for the protection and scanning of dormant machines rests with the cloud provider. Enterprises using cloud computing should look for cloud service providers that can secure these dormant virtual machines and maintain cohesive security in the cloud.

3.5Data Integrity

According to the 2009 Data Breach Investigations Report conducted by Verizon Business Risk Team, 64% of data breaches resulted from hacking and intrusions. Dedicated resources are expected to be more secure than shared resources. The attack surface in fully or partially shared cloud environments would be expected to be greater and cause increased risk. Enterprises need confidence and auditable proof that cloud resources are neither being tampered with nor compromised, particularly when residing on shared physical infrastructure. Operating system and application files and activities need to be monitored.

3.6Patch Management

The self-service nature of cloud computing may create confusion for patch management efforts. Once an enterprises subscribes to a cloud computing resourcefor example by creating a Web server from templates offered by the cloud computing service provider the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber. Keeping in mind that according to the previously mentioned Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor supplied patches. If patching is impossible or unmanageable, compensating controls such as “virtual patching” need to be considered.

3.7Encryption and Data Protection

Nature of the cloud ismulti-tenant and service providers have privileged access to the data in those environments.Thus confidential data hosted in a cloud must be protected using a combination of access control, contractual liability and encryption. Of these, encryption offers the benefits of minimum reliance on the cloud service provider and lack of dependence on detection of operational failures.

There is the need to encrypt multi-usecredentials, such as credit card numbers, passwords, and private keys, in transit over the Internet. Use encryption to separate data holding from data usage encrypting data on backup media. This can protect against misuse of lost or stolen media.[6][7]

3.8Policy and Compliance

Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as PCI, HIPAA, and GLBA in addition to auditing practices such as SAS70 and ISO. Enterprises need to prove compliance with security standards, regardless of the location of the systems required to be in scope of regulation, be that on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources.

Examples such as virtual machine sprawl-- when the number of virtual machines being created is growing more quickly than an enterprise’s ability to manage them-- adds complexity.Creating an identity for an individual virtual machine and tracking that virtual machine from creation to deletion creates challenges for even the most mature virtualized environments.

IV. SECURITY ASPECTS OF MULTI CLOUDS:

In multi clouds the security levels are enhanced and the solutions for security risks like data integrity, data intrusion and service availability have been answered. But if the hacker knows the cloud provider that the user is accessing his data then he can easily hack the data. So the existing techniques in the multi clouds provide the security upto a certain level but not completely. The Depsky System model which consists of cloud of clouds can solve the security problems by using the secret sharing algorithm [2][4].

According to Jaya Prakash*et al.* [3] a multi cloud system must be developed so that the data is replicated into different cloud providers to reduce the service availability risk or loss of data. The multi clouds are cloud of clouds in which every single cloud contains its own interface. But there is a chancethat if the attacker finds the main server from which the users access their data then he can easily hack the data. To overcome this security risk, one of the solution is using a multiple unrelated cloud architecture in which many clouds from different cloud providers which are not related to each other[2].

Another is using multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. Assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. This depends on Shamir's secret sharing algorithm with a polynomial function technique[4].

V. CONCLUSION

Using cloudcomputing israpidlyincreasing now a days but Using cloudcomputing israpidlyincreasing now a days but Customersdonotwanttolosetheirprivateinformationasaresultofmaliciousinsidersinthecloud .There are number of security challenges in cloud computing environment ,some are discussed in the paper . Security is the important factor that everyone thinks before choosing a cloud provider when it is related to critical data. Many of the security issues can be handled effectively by using multicloud than that of single cloud.

REFERENCES

[1] (NIST), http://www.nist.gov/itl/cloud/.

[2] Akhila, B.V.SriRam ,Dr.N.Srinivasu , Nikita Mahajan , "Security Through Multiple Unrelated Clouds in Cloud Computing", International Journal of Computer Trends and Technology (IJCTT) - volume4Issue4 –April 2013

[3] S. Jaya Prakash, DrK.Subramanyam, U.D.S.V. Prasad, "Multi Clouds Model For Service Availability And Security", Department of Computer Science and Engineering,K.L.University, Vaddeswaram.

[4] Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom, "Cloud Computing Security From Single to Multi Clouds, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.

[5] William R. Claycomb, "Tutorial: Cloud Computing Security" Lead Research Scientist CERT Enterprise Threat and Vulnerability Management Team

[6] " Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", Prepared by theCloud Security Alliance December 2009, Mohammed A. AlZain, Ben Soh and Eric Pardede, "MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing", Department of Computer Science and Computer Engineering, LaTrobe University, Bundoora 3086, Australia.

[7] "Security in Private Database Clouds", An Oracle White Paper, July 2012.

[8] "Making virtual machines cloud ready " , A trend Micro white paper , August 2009.

[9] "A Multi-Level Security Model for Partitioning Workflows over Federated Clouds" by Paul Watson, Technical Report, September 2011.