International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

CLOUD COMPUTING CHALLENGES

Richa Singh[1], Shakti Bhati[2], Dr. Ajay S. Singh[3]
[1,2] 2 Yr-B.Tech (CSE), Galgotias University,India
[3]Professor, SCSE,Galgotias University,India

Abstract — Cloud computing can be described as a method of accessing and managing data and information from an online server instead of saving information on a system. This field has taken great advancements in providing data on various types of users from business ventures to commercial usage. Although yet it is not considered an equal replacement for data sharing. In this paper we discuss the different types of challenges that have been faced in cloud computing. To research, analyze different issues faced during cloud handling, several research papers have been studied to scrutinize this subject. We discuss various challenges faced in interoperating between different service models.
Keywords—cloud computing; security issues; Service oriented computing; distributed computing.

I. INTRODUCTION

In this internet age, cloud computing is emerging as the new buzz word. cloud computing has become one of the biggest modes of data sharing and providing information service platforms for multinational companies in recent times since it gives people the advantage of accessing data from any system. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. The definition of cloud computing given by U.S. NIST (National Institute of Standards and Technology) states that:

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.

I.Foster, Y. Zhao, I. Raicu, S. Lu. in "Cloud Computing and Grid Computing 360-Degree Compared", IEEE Grid Computing Environments (GCE08) 2008, co-located with IEEE/ACM Supercomputing 2008[3], defined Cloud computing as a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet Cloud computing has major benefits and advantages that has driven the adoption of this paradigm.

1)A consumer can avail self-service on demand without resorting to human interactions to access the resources. 2) The resources are delivered over a broad network which can be accessed through various platforms according to the need of the client. 3) The resources shared in such a way can be utilized by multiple users using either the multi-tenancy or virtualization model. 4) Resource provisioning is flexible to meet the needs at any time. Scalability and load balancing is taken care by the cloud. 5) Despite sharing and pooling resources, cloud infrastructure can measure the usage of these resources for each individual consumer through its metering capabilities. Users of cloud services are charged according to their usage of resources, and they can be further pay lower price if the application is optimized.

The figment of infinite computing resources that is given by Cloud Computing on interest to end clients is entrancing to an extensive variety of science and building applications, especially to information and/or register serious experimental work process applications.

II. CHALLENGES

Number of issues has been encountered while transferring work systems to cloud computing models. A lot of emphasis has been laid on leakage of data while large amount of file transfers take place between the clouds severs and hardware system. A lot of challenges have been faced by consumers for the availability of service providers in the industry.

Since cloud computing is still not much familiar in the industry, its adoption is associated with numerous challenges. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations as shown in Figure 1.

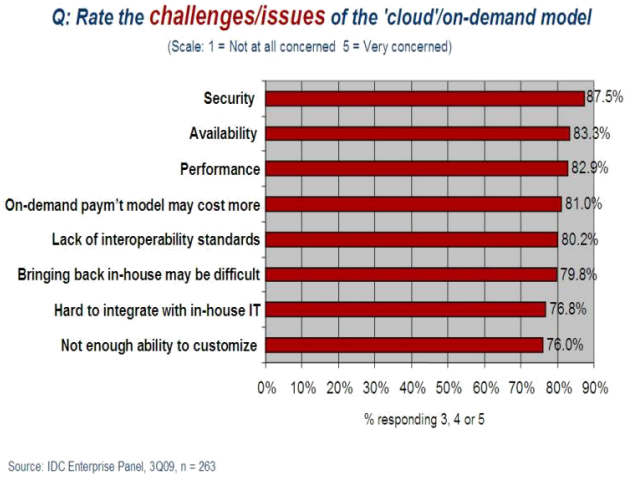

FIGURE 1. Results of IDC survey ranking security challenges, 2008[4]

A. *Security*

Security has been the major concern regarding cloud computing. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Hackers can initialize their attack using cloud as it provides more reliable infrastructure at cheaper rates.

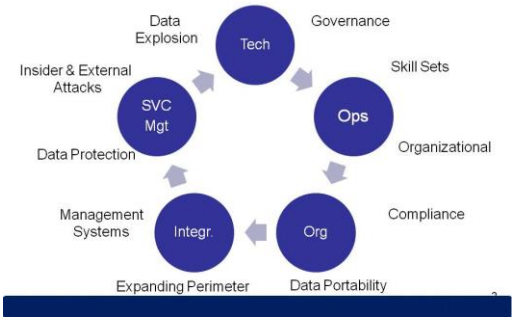

FIGURE 2. Major cloud security risk areas[7]

Traffic hijacking-
Another significant cloud computing security threat is account or service traffic hijacking. COUD computing adds another risk to this scene, as per CSA(cloud security alliance) If a hacker accesses your credentials, he or she can spy on your activities and exchanges, control information, return misrepresented data, and redirect your customers to illegitimate locals. Your record or sevice instances might turn into another base for the attacker. From here, they might influence the force of your notoriety to dispatch consequent attacks. As an example,CSA pointed to an XSS attack on Amazon in 2010 that let attackers hijack credentials to the site.

Data breach-
A virtual machine could utilize side-channel timing data to concentrate private cryptographic keys being used by different VMs on the same server. A malignant programmer wouldn't be persuaded to go to such lengths to pull off that kind of deed, however. On the off chance that a multi-tenant cloud administration database isn't composed legitimately, a solitary blemish in one customer's application could permit a hacker to get at that customer's information, as well as each other customer's information too.

PSB's examination found that just a small amount of human services suppliers (12%) store persistent wellbeing records in an public or hybrid cloud, and even less (10%) monetary administrations firms store client financial records in an public/hybrid cloud environment. Ensuring client information is the top worry in both business sector portions.

B. Costing model
The computation and communication maintain a reciprocating relationship when it comes to costing variation. Shifting database to a cloud model reduces infrastructure expense but transferring data from a certain cloud model (public and community) relatively increases. This issue becomes a major problem if the data has been distributed on more than one cloud model. The cost of integrating data can be substantial as different cloud model use propriety protocols and interfaces, which bounds the user to access different clouds using provider-specific APIs and manage data transfer to and from the various clouds. This grows on to become and efficiency problem when data is to be distributed on to different clouds decreasing the performance of the system and leading to cost inflation.

Network bandwidth accounts represent a significant part of the expense of moving information: Cloud suppliers may charge upload and download charges. Furthermore, despite the fact that information and frameworks are being facilitated off-site, there are inner work costs. Individuals think there are no labor costs with the cloud, yet as you scale up to handle workload, a significant number of cloud instances have a complexity for management, much the same as dealing with a large number of servers. Another huge expense is for long term information storage in the cloud. When you consider the rates of growth of data throughout the following three years, the life-cycle expense of data can be truly high. You keep on paying for that consistently when information is put away in the cloud.

In any case, these expenses are just startling in the event that you don't completely grasp the cloud model. When you consider CPUs, limit and capacity [needs] and outline that after some time, you can get a really decent handle on what the expenses are and if you can do it more cost-adequately on the internal level.

C. Charging model:

The multi-tenancy architecture which is implemented by various cloud service providers has complicated the procedure of cost evaluation. Regular data centers calculate their costs based on consumption of static computing. Moreover instantiated virtual machine has become a unit of cost analysis. But the software as a service providers have to re-design and re-construct the software for the next user to implement multi-tenancy which follows heavy customization of the software. All this customization adds up to large expenditure. Therefore managing between the expenses invested and the cost saved by multi-tenancy becomes obstructing in sustainability and yielding profit from the service

D. Interoperability

Cloud service providers cater different techniques for users to interact with the cloud. Therefore this has affected the development of cloud environment because the providers often impose vendor locking which takes away the freedom of choosing a different cloud simultaneously to distribute data on different clouds and increase the efficiency of the workplace. The essential objective of interoperability is to acknowledge consistent fluid information past various clouds and local applications. It is important for cloud computing for the optimization of IT assets and standardization. Interoperability has not emerged as a major concern for industry cloud vendors.

Verging on each cloud has an interesting infrastructure for giving system administrations in the middle of servers and applications and servers and storage. Contrasts are likely in system tending to network administrations, firewalls, switches, routers, identity administrations, naming administrations and other resources. Target cloud providers are almost certainly going to have a network architecture that differs from the source cloud network architecture. One reason for this is their desire to support multi-tenant environments.

Cloud providers make their own choices about security policies: who has access to what resources, rules for updating software, and policies for using data and disks, and so on. Application users and owners usually have little choice in cloud security matters. Applications need to operate within certain security zones, and cloud providers may not support the same security zones, or they may make changes that disrupt the application's security requirements.

E. *Service level agreement*

A guarantee from vendors regarding delivery of service is vital for clients to ensure the quality, availability, dependability, and performance of the computing resources when clients have moved to cloud. Customarily, these are provided through Service Level Agreements (SLAs) negotiated between the service providers and clients. Here we face two issues, first is the specifications of SLA to meet the expectation of the consumers and can be simply implemented by cloud. Secondly, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA metaspecifications which will raise implementation problems for cloud providers.

III. CONCLUSION

Cloud computing is emerging as new revolutionizing phenomena but it still have some potholes. A few challenges regarding adoption of Cloud computing was analyzed. There is a need to understand the threats and challenges one might face while using the new technology and work should be done to eliminate it. It can still be used in many sectors to ease up the workload.

REFERENCES

1. Tharam Dillon and Chen Wu and Elizabeth Chang " Cloud computing :issues and challenges" 2010 24th IEEE International Conference on Advanced Information Networking and Applications
2. Kuyoro S. O., Ibikunle F. & Awodele O. "Cloud Computing Security Issues and Challenges " International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011
3. I.Foster, Y. Zhao, I. Raicu, S. Lu. "Cloud Computing and Grid Computing 360-Degree Compared", IEEE Grid Computing Environments (GCE08) 2008, co-located with IEEE/ACM Supercomputing 2008
4. IDC survey ranking security challenges, 2008
5. Ted Samson. "9 top Threats to cloud computing security", infoworld.com.
6. Brendon Ziolo. "overcoming cloud security challenges".networkcomputing.com
7. FIGURE 2. "risks of cloud computing".slideshare.net
8. Penn Schoen Berland (PSB) survey for alkatel-lucent ranking cloud model adoption.
9. Cloudtweaks, "top five challenges of cloud computing",cloudtweaks.com
10. Bob Violin, "the real costs of cloud computing".computerworld.com
11. Bill Claybrook, "cloud interoperability: problems and best practices".
12. Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0,"
13. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC'09 IEEE International Conference on Services Computing, 2009, pp 517-520.
14. ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].
15. N. Leavitt. "Is Cloud Computing Really Ready for Prime Time?" Computer, vol. 42, pp. 15-20, 2009.

