Industrial Science
ISSN : 2347-5420
Volume-1 | Issue-7 | Oct-2014

CLOUD COMPUTING : OVERVIEW,ISSUES, CHALLENGES,APPLICATIONS AND FUTURE RESEARCH DIRECTION

Priyanka S P

Department Of Information Science and Engg., Dr. Ambedkar Institute Of Technology , Banglore,INDIA.

Abstract:-As cloud computing continues to gain more momentum in the IT industry, more issues and challenges are being reported by academics and practitioners. In this paper, we aim to attain an understanding of the types of issues and challenges that have been emerging over the past years and identify gaps between the focus of the literature and what practitioners deem important. Researchers have been mainly focusing on issues related to security and privacy, infrastructure, and data management. Despite the significant overlap between the topics being discussed in the literature and the issues raised by the practitioners, findings show that some issues and challenges that practitioners consider important are understudied such as software related issues, and challenges pertaining to learning fast-evolving technologies.

Keywords: Cloud Computing; Issues; Challenges.

INTRODUCTION

Cloud computing is a new name for an old concept: the delivery of computing services from aremote location, analogous to the way electricity, water, and other utilities are provided to most customers. Cloud computing services are delivered through a network, usually the Internet.Utilities are also delivered through networks, whether the electric grid, water delivery systems, orother distribution infrastructure. In some ways, cloud computing is reminiscent of computingbefore the advent of the personal computer, where users shared the power of a central mainframe computer through video terminals or other devices. Cloud computing, however, is much morepowerful and flexible, and information technology advances may permit the approach to becomeubiquitous.

OVERVIEW

A. CHARACTERISTICS OF CLOUD COMPUTING

Cloud computing differs from local computing in many ways. The identified five characteristics in particular:

On-demand self-service

A user can directly access the needed computing capabilities from the source, no matter what specific resource is required. This can be considered somewhat analogous to a homeowner being able to changetelevision channels or radio stations at will with a remote control.

Broad network access

A user is not tied to one location but can access resources from anywhere the network (typically the Internet) is available.

Resource pooling

Many users share the same overall set of resources from a provider, using what they need, without having to concern themselves with where those resources originate. An analogy with respect to the electric grid is that homeowners do not need to know what specific power plants generated the electricity they are using.

Rapid elasticity

Users can quickly increase or decrease their use of a computing resource in response to their immediate needs. An analogy would be homeowners using as little or as much electricity at any one time as they need, within the capacity of their connections to the grid.

Measured service

The amount of usage by a customer is monitored by the provider and can be used for billing or other purposes. An analogy is metering the use of electricity, water, and other utilities.

B. DEPLOYMENT MODELS

NIST has identified four standard models, or types, of cloud computing that can be implemented to satisfy varying needs of users or providers. Those models—public, private, community, and hybrid—vary in where the hardware is located, what entity is responsible for maintaining the system, and who can use system

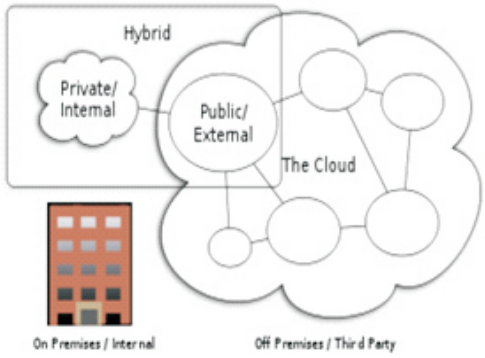

Figure 1. Types of cloud deployment models

Public

In public cloud (sometimes called an external cloud) computing, a provider supplies one or more cloud-computing services to a large group of independent customers, such as the general public. Customers use the service over the Internet through web browsers or other software applications. Providers usually sell those services on a metered basis, an approach that is sometimes called "utility computing."

Private

A private cloud (sometimes called an internal cloud) works like public cloud computing, but on a private network controlled and used by a single organization. Private clouds may provide services that are similar to those provided by public cloud providers, but with fewer purported risks. Potential disadvantages include cost and logistical challenges associated with purchasing and managing the required hardware and software. Private clouds can provide internal services such as data storage as well as external services to the public or other users.

Community

A community cloud allows a group of organizations with similar requirements to share infrastructure, thereby potentially realizing more of the benefits of public cloud computing than is possible with a purely private cloud. Because a community cloud has a much smaller user base than a public cloud, it may be more expensive to establish and operate, but it may also allow for more customization to meet the users' needs. It may also meet user-specific security and other requirements more effectively than a public cloud.

Hybrid

A hybrid cloud uses a combination of internal (private or community) and external (public) providers. For example, a user could employ a private or community cloud to provide applications and store current data but use a public cloud for archiving data. The flexibility of this deployment model may make it particularly attractive to many organizationsresources

.

C. SERVICE MODELS

Cloud computing can provide various kinds of services, ranging from fundamental computing to provision of sophisticated applications. While they can be categorized in different ways, the NIST definition uses three basic service models, which are described below.

Software as a Service (SaaS)

In the SaaS11 model, customers use applications that the provider supplies and makes available remotely on demand, rather than using applications installed on a local workstation or server. SaaS is the most readily visible service model to the end user. In many cases, SaaS applications are accessible through hardware or software "thin clients."They include web-based services such as Google Maps and Facebook, online storage, and services such as Paypal that websites can integrate into their applications.

Platform as a Service (PaaS)

With PaaS, customers create applications on the provider's infrastructure using tools, such as programming languages, supplied by the provider. One example of such an application is using PaaS to create a web-based interface for customers. Such a platform could include hosting capability and development tools to facilitate building, testing, and launching a web application. The user controls the applications created via the platform, and the provider controls and maintains the underlying infrastructure, including networks, servers, and platform upgrades.

Infrastructure as a Service (IaaS)

IaaS providers supply fundamental computing resources that customers can use however they wish. Customers can install, use, and control whatever operating systems and applications they wish, as they might otherwise do on desktop computers or local servers. The provider maintains the

underlying cloud infrastructure.

C. CONSIDERATIONS IN CLOUD COMPUTING ADOPTION

Decisions in both the public and private sector regarding whether and how to use cloud computing involve consideration of several factors, notably cost, efficiency, accessibility, agility of improvements, security, reliability, and privacy.

Improving Cost structures

The potential financial benefits from cloud computing arise largely from the capability of this approach to provide far more efficient use of IT resources. Most commercial cloud services involve a different payment and cost model than local computing. Cloud providers make infrastructure investments that can lower cost barriers for IT end users, who can access services requiring expensive hardware or software without having to invest in it. Users pay only for the computing power that they consume. This approach to pricing is sometimes referred to as the "utility computing model" because of its similarity to how utilities such as electricity, water, and gas are provisioned. The model allows on-demand scalability that can meet a user's peak service requirements without the user having to invest in infrastructure to meet such requirements.

With cloud computing, in contrast, users need not invest in resources that will often remain idle, but can acquire and pay for services only as they use them. According to some economic analyses, cloud computing using a public cloud can produce savings over local computing when demand for a service varies significantly over time or cannot be predicted.Also, as the cloud computing market continues to develop, it may result in a small number of large providers of cloud infrastructure most capable of taking advantage of the benefits of economies of scale.Additional potential financial benefits of cloud computing include the savings cloud providers may realize from locating facilities in areas with lower-than-average energy and labor costs.

Dealing with changes in the market

Today's companies must position themselves in increasingly dynamic markets. New products enter into ever shorter cycles in the market. Existing products, but also specialist expertise become outdated faster and a once acquired advancement in knowledge rapidly disappears. This forces the companies to come up with new ideas in ever decreasing time periods.

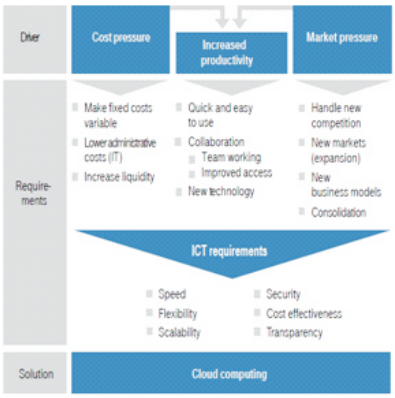

Figure 2.requirements of cloud computing

Energy Efficiency

Computers, servers, and related devices require large amounts of energy to manufacture,

and they account for a growing share of world energy consumption. "Green computing" is often cited as a potential benefit of cloud computing. It makes heavy use of data centers, which can be specifically designed for efficient power usage and cooling. Taking advantage of economies of scale, cloud computing can potentially deliver computing power to many users much more efficiently than would be possible with local computing.

Availability

Cloud computing may provide both advantages and disadvantages with respect to availability. It can improve availability by using Internet connectivity to provide mobile computing services, sothat users can access data and applications wherever they can get an Internet connection. Effective use of cloud computing depends on access to high-speed Internet or mobile telecommunications. Such broadband access is not evenly distributed within the United States. Rural access is significantly lower than that in urban areas, resulting in much greater access to cloud services in cities.

Agility

Cloud computing can be more agile than local computing in at least two ways. It can permit faster and more efficient implementation of upgrades and other technological advances. It can also provide innovators with a broader range of scalable tools for research, development, and testing than they would be able to acquire cost-effectively for a local computing environment.

In some ways, agility can be more limited under cloud computing than local computing. Differences among providers may limit portability anprovider, because of dissatisfaction or some other factor such as the original provider going out of business, portability may be a problem. The platform used by the new provider may require substantial modifications to data or other resources being moved or may even be incompatible. Provider variation may also hinder interoperability, which would be needed, for example, if users wish different providers to supply different services involving a common set of data or applications.

Security

Some aspects of security in cloud computing are similar to those with local computing involving local networks. Both are potentially subject to attacks aimed at service disruption or theft of information, including espionage. Both are subject to threats from the Internet and from insiders. Vulnerabilities specific to particular operating systems and other applications need to be addressed whether those applications are provided through cloud or local computing.

However, some aspects of cloud computing have security implications that differ substantially from those for local computing. With local computing, each user constitutes a point of attack that must be defended separately, but the impact of an attack is generally limited to that user. If a user wishes to switch to a newcloud computing, both the points of attack and the defenses are concentrated, as is the value of the target.

Reliability

Services hosted in the cloud may be distributed among several different data centers. That distribution can potentially improve reliability over use of only a local data center, especially if combined with redundancy. However, there have been cases in recent years of downtime at the IaaS level that caused widespread service interruptions. Despite the publicity such disruptions received, service downtimes in cloud computing have been rare, and many observers consider cloud hosting to be more reliable than local hosting.

Privacy

Privacy is a concern, especially for public and hybrid cloud services. The greater direct control that private clouds give to users over hardware and software may provide them more control over management of privacy.

Establishing an effective and appropriate legal structure for regulating cloud computing services is imperative, as cloud usage is expected to represent more than half of all Internet use by the end of this decade. Globally, advances in technology services such as cloud computing paired with how those services are used by consumers have increased the difficulty of maintaining the appropriate legal balance between individual rights and the needs of law enforcement. As the depth and breadth with which consumers incorporate cloud services into their daily lives increases, the need for balance becomes even more important, but also more difficult to attain.

CHALLENGES

There are a number of reasons that adoption is not occurring more rapidly: security risks, ensuring portability and interoperability, perceived lack of knowledge and expertise in the workforce, lengthy certification and accreditation processes, and perceived lack of implementation guidance are the reasons .

A.PORTABILITY &INTEROPERABILITY

Agencies expressed concern that their ability to change cloud vendors could be limited through platforms or technologies that "lock" customers into a particular product. A Treasury official explained that it is challenging to separate from a vendor, in part due to a lack of visibility into the vendor's infrastructure and data.

B.SECURITY& PRIVACY

This category includes organizational and technical issues related to keeping cloud services at an acceptable level of information security and data privacy. This includes ensuring security and privacy of sensitive data held by banks, medical and research facilities. Security and privacy issues become even more serious when governmental institutions Despite the known need for Service Level Agreements between Cloud service providers and users, standards for safety have not yet been established and more research in this area would be beneficial . Security and privacy of data spans issues such as authentication, encryption , and detection of malware, side channel attacks and other kinds of attacks use the cloud.—both internal and external to an enterprise . There exists current research on detection and handling of security breaches to guard against tampering, loss and theft of data . Further, fault tolerant mechanisms for backing up data are required when there are failures in the infrastructure, such as net-work outages.

C. INFRASTRUCTURE

This category entails issues pertaining to the hardware layer used as a backbone for cloud services as well as the thin layer of software used to operate this hardware. The main issue that dominates this category is performance including topics like SaaS placement problems, server allocation optimization .Load balancing and many other . Other issues are related to networking such as traffic management, ubiquitous connectivity ,network speed and cost , and network reliability. Another group of challenges pertain to resource management including dynamic resource provisioning , scaling , and allocation ; as well as resource stranding and fragmentation Solutions for the security and privacy challenges already highlighted at a larger scale.

Furthermore, sustainability stands out as another important issue given the amount of energy needed to operate large-scale hardware infrastructure. Quality attributes of the hardware infrastructure have also been an area of interest including issues like availability, reliability , and scalability. Other issues

under this category include infrastructure design is- sue and virtualization

D. LEGAL ISSUES

The notion of using cloud resources as a utility has brought about a number of legal issues. The most discussed issue in the literature we surveyed is related to data placement . Laws and regulations vary widely across different regions and jurisdictions as to where and how data should be stored, processed, and used. For example, the European Union requires that all personal data be physically stored within the jurisdictions of the European Union . Also, compliance requirements might vary in regards to the disclosure of data in general and sensitive data in specific (e.g. financial data, health insurance records) , in addition to variations in the regulations around transaction logging and taxation. Traceability of data and alterations made on it has also been reported as a legal concern. Another important issue is the lack of comprehensive legislation on liability in the cloud as well as identity definition (i.e. users versus systems), and issues related to authentication and authorization.

E. QUALITY

The main challenge regarding quality of service in the cloud is the definition and use of service level agreements (SLAs) is the lack of SLAs between parties in the cloud which lowers consumers' confidence in the reliability and availability of services and makes adoption more difficult.

Another challenge discussed is the quality of user experience. Especially in multimedia-intensive cloud services such as video streaming services as well as online games , video quality and network delays have a huge impact on the overall experience of using the cloud as perceived by end-users.

F. TRUST

Trust is recognized as a key obstacle in the way of adopting the Cloud and becoming dependent on its resources. Challenges arise around long-term viability (i.e., trusting that stored data will not vanish as a result of a vendor going bankrupt or getting acquired) , having full control over mission critical activities , and trusting the supply chain of a given service provider at all different levels . Trust is as an issue in cloud federations since every participant needs to trust that all others do filter out malicious users, follow the code of conduct, and report accurate resource usage and billing information.

Trust is a barrier to pro-viding effective remedies against cyber-attacks in the cloud. They mentioned lack of transparency between service providers, malicious insiders, and vulnerable shared technologies as some of the trust issues that need to be addressed.

CONCLUSION& FUTURE RESEARCH DIRECTION

Cloud computing have several benefits over traditional (non- cloud) environment and have capability to handle most sudden, temporary peaks in application demand on cloud infrastructures. Virtualization technology provides good support to achieve aim of cloud computing like higher resource utilization, elasticity, reducing IT cost or capital expenditure to handle temporary loads as well as cloud computing have various flexible service and deployment models which is also one of the main issue of adopting this computing paradigm. Virtualization concepts have open shared nature which is responsible for the violation of security polices and laws as well as degrades their computing reputation and performance. So there is need to focus on privacy and on solutions of various security problems to maintain the trust level of organization for deploying the cloud computing without any hesitation and also need of technical support for elastic scalability to serve by vertical scaling approach which is currently restricted to only horizontal scaling.

As the adoption of cloud computing is becoming increasingly common, issues and challenges are still emerging at the various levels of the cloud architecture. The main focus is on issues

related to security and privacy, infrastructure, and data management. Interoperability across different service providers also seems to be an active area of research.

REFERENCES

[1] A. Fischer Senior Specialist in Science and Technology February 3, 2014 Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management Patricia MoloneyFigliolaSpecialist in Internet and Telecommunications Policy Eric
[2] BhushanLalSahuDepartment of Computer Science SSCET, BhilaiIndia A First Look at Problems in the Cloud Theophilus Benson ⋆ , SambitSahu†, AdityaAkella ⋆ ,andAneesShaikh† ⋆ University of Wisconsin - Madison, †IBM Research
[3] RajeshTiwariDepartment of Computer Science Department of Computer Science SSCET, Bhilai SSCET, Bhilai India India :International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Volume 2, Issue 9, September 2012 ISSN : 2277 128X

[4] Lutz Schubert [USTUTT-HLRS] Keith Jeffery [STFC]:Advances in Clouds,Research in future Cloud Computing,Expert Group Report Public Version 1.0 Editors
[5] YaserGhanam, Jennifer Ferreira, Frank Maurer :Journal of Software Engineering and Applications, 2012, 5, 923-937 http://dx.doi.org/10.4236/jsea.2012.531107 Published Online November 2012 (http://www.SciRP.org/journal/jsea) EmergingIssues & Challenges in Cloud Computing— A Hybrid Approach
[6]Mladen A. Vouk Department of Computer Science, North Carolina State University, Raleigh, North Carolina, USAJournal of Computing and Information Technology - CIT 16, 2008, 4, 235–246 doi:10.2498/cit.1001391
[7] 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. Technical Report UCB/EECS-2009-28, Feb 2009.
[8] S. Cunningham and G. Holmes. Developing innovative applications of machine learning. In Proc Southeast Asia Regional Computer ConfederationConference, Singapore, 1999.
[9] K. Fitz, L. Haken, and B. Holloway.Lemur – A Tool for Timbre Manipulation.In Proceedings of the International Computer Music Conf., 1995.
[10] National Institute of Standard and US Department of Commerce Technology, "The NIST Definition of Cloud Computing," 12 October 2012. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[11] B. Kitchenham, "Procedures for Performing Systematic Reviews," Technical Report TR/SE-0401, KeeleUniver-sity, Lyme, and Technical Report 0400011T.1, NICTA, 2004.
[12] A. Greenberg, J. Hamilton, D. A. Maltz and P. Patel, "The Cost of a Cloud: Research Problems in Data Center Networks," SIGCOMM Computer Communication Re- view, Vol. 39, No. 1, 2008, pp. 68-73. doi:10.1145/1496091.1496103
[13] H. Lim, S. Babu, J. Chase and S. Parekh, "Automated Con- trol in Cloud Computing: Challenges and Opportunities," Proceedings of the 1st Workshop on Automated Control for Datacenters and Clouds, New York, 19 June 2009, pp. 13-18. doi:10.1145/1555271.1555275
[14] A. Khalid and H. Mujtaba, "Data Processing Issues in Cloud Computing," Proceedings of the 2nd International Conference on Machine Vision (ICMV '09), Dubai, 28-30 December 2009, pp. 301-304.
[15] D. Bernstein and E. Ludvigson, "Networking Challenges and Resultant Approaches for Large Scale Cloud Con- struction," Proceedings of the 2009 Workshops at the Grid and Pervasive Computing Conference (GPC'09), 4- 8 May 2009, Geneva, pp. 136-142.

Priyanka S P
Department Of Information Science and Engg., Dr. Ambedkar Institute Of Technology , Banglore,INDIA.