(43)

ISSN 2249-3867

"Education Through Self Help Is Our Motto"
- Karmveer

Research Dimensions

S. P. Rajguru
Editor-in-chief

A Multi-Disciplinary Peer-Reviewed International Research Journal

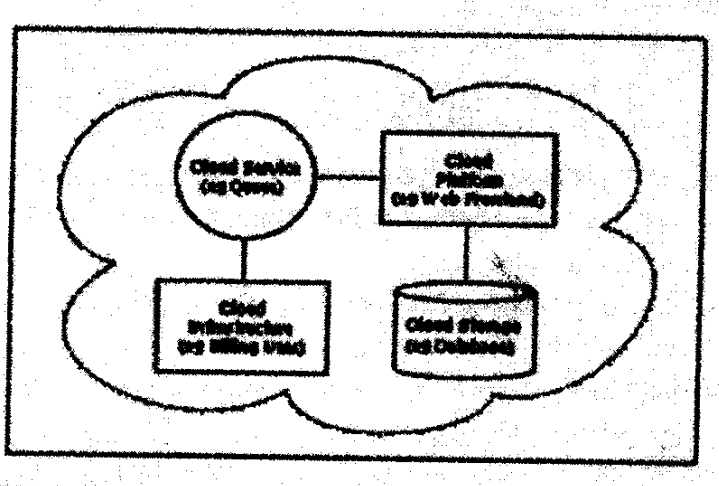
Rayat Shikshan Sanstha's
LAXMIBAI BHAURAO PATIL MAHILA MAHAVIDYALAYA
SOLAPUR (MAHARASHTRA)

RESEARCH DIMENSIONS ISSN 2249-3867
A Multi-Disciplinary Peer-Reviewed International Research Journal
Volume 1 Issue 2 Jan. 2012

CONTENT

Cloud Computing : A Case Study

- Mrs. K. S. Pawar
Asst. Prof. Dept. of B.C.A.
College of Computer Application for Women, Satara,
- Dr. R. D. Kumbhar,
Head, Dept. of B.C.A., KBPIMSR, Satara.



I. INTRODUCTION:

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, wherein end-users consume power without needing to understand the component devices or infrastructure required to provide the service. The concept of cloud computing fills a perpetual need of IT: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities. The National Institute of Standards (NIST) definition of Cloud Computing is the most useful, comprehensive, and popular definition - 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

II. ARCHITECTURE OF CLOUD:

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple *cloud components* communicating with each other over a loose coupling mechanism such as a messaging queue. As of now, the majority of cloud computing infrastructure consists of reliable services delivered through data centers and built on servers with different levels of virtualization technologies. The services are accessible anywhere that has access to networking infrastructure. The cloud appears as single point of access for all the computing needs of consumers.

Fig. 1: Cloud Architecture

III. DEPLOYMENT MODELS OF CLOUD COMPUTING

Public cloud The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Public cloud or external cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who bills on a fine-grained utility computing basis. In simple, for use by multiple organizations on a shared basis and hosted and managed by a third party service provider. It is very useful. It's free of cost.

Private cloud Private cloud is infrastructure operated solely for a single organization. It may be managed by the organization or a third party and may exist on premises or off premises. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from lower up-front capital costs and less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

Community cloud Community cloud shares infrastructure between several organizations from a specific community with common concerns (e.g. mission, security requirements, compliance, jurisdiction, etc.). A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. Community clouds are whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the benefits of cloud computing are realized. Community cloud offers a higher level of privacy, security, and/or policy compliance. In addition, it can be economically attractive as the resources (storage, workstations) utilized and shared in the community are already exploited and have reached their return of investment. Examples of community clouds include Google's Web App hosting service.

Hybrid cloud Hybrid cloud infrastructure is a composition of two or more clouds

(private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

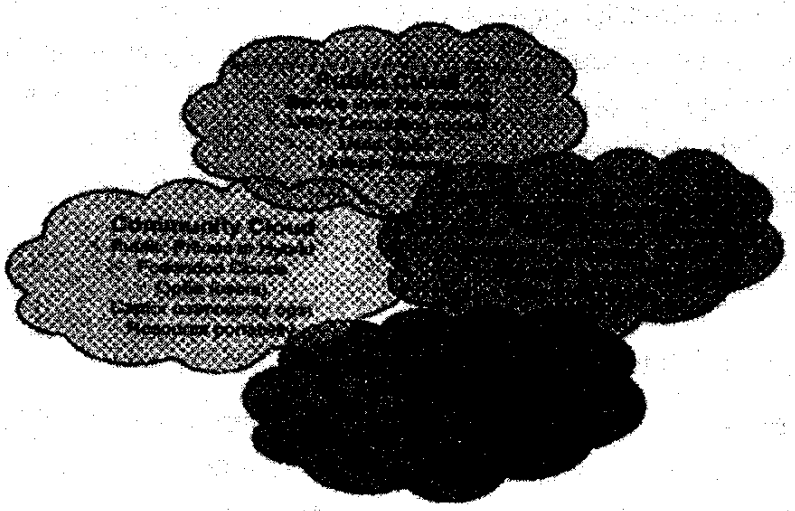


Fig. 2: Deployment Models of Cloud Computing

IV. CHARACTERISTICS OF CLOUD COMPUTING Cloud computing exhibits the following key characteristics:

1. On-demand self-service: A consumer can independently provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

2. Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

3. Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

4. Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

5. Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

6. API accessibility: Application programming interface accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers.

V. BENEFITS OF CLOUD SERVICES

1. Agility

From a business perspective, there is much more to consider today beyond your ability to manage your core business and deliver great and timely products and services. Today, competitive pressures, marketing challenges, budget issues, and more are considerable requirements. Your ability to manage situations quickly and efficiently is the key. The biggest benefit of cloud computing to business today can be framed in terms of agility. Cloud services can offer huge savings in terms of time (for example, when IT capabilities must be delivered quickly). Scaling up or down with cloud services does not usually require additional hardware or software. Cloud services offer minimal setup time, minimal time to scale, and less cash outlay. This is because as a business model, cloud service providers generally host massively scaled systems' capacity that can be switched on upon request. Suppose, for instance, that you need to scale rapidly for a new project or a seasonal rush. Companies can model these situations using internal resources, but likely at some point they will need to expand beyond that capacity. A decision is made whether to use an external provider to fill the gap; in the world of cloud services, this is called '*cloud bursting*'.

2. Business Focus

By using the best service from a cloud service provider, a business can potentially focus more energy and talent on optimizing existing revenue streams and aggressively pursuing the development of new ones. For example, cloud services can enable businesses to gather information, ideas, feedback and so forth from a much wider set of sources (such as customers, partners) than was ever possible by traditional means. This approach is known as '*crowd sourcing*'.

3. Cost and Budget Control

Although the initial costs of using cloud services may appear less, a better expectation should be that cloud services offer more control over costs or better budget management capabilities. Most cloud services enable you to pay on a monthly, weekly, or per-use basis. Choosing a cost-effective cloud service provider can result in significant savings, but more important is finding a cloud service provider than can accurately report usage patterns to you so that you can confirm the accuracy of your billing based on use. One noted advantage of using public cloud services is the use of operational expenditure (OpEx) over capital expenditure (CapEx). Having flexibility of where to spend OpEx versus CapEx enables an organization to better manage expenditure such that the costs occur over time rather than in one big lump sum, which enables for better cash-flow management.

4. Security

Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than under traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

5. Optimal Infrastructure

The ability to host multiple capabilities in the same hardware, software, or service allows for the follow-on benefit of optimized use of the infrastructure. Multi-tenancy enables sharing of resources and costs across a large pool of users and thus allowing for **centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.), **peak-load capacity** increases (users need not engineer for highest possible load-levels), **utilization and efficiency** improvements for systems that are often only 1020% utilized. Multitenancy can occur at any or all levels of the architecture, as follows:

- **Virtual layer:** Virtualization provides the ability to create specific environments for each process, application, or operating system. This model isolates everything above the virtual layer itself but allows for the use of pooled resources below that layer, most commonly hardware such as networking, processor, memory, input/ output, and storage resources.

- **Application layer:** The user interfaces of most web applications allow for specific fixed graphical and behavioral elements alongside customized elements associated with a

specific organization, individual, or function. If one component or functional element fails in the delivery of the interface, it is easier to replace because those elements derived from other parts of the application and can be easily reconstructed.

- **Database layer:** Data for multiple applications, through to multiple customers, can be stored in the same database, and thus allow for the focus on optimal data structures rather than entire infrastructures to support each individual requirement.

6. Scalability and Capacity Management

The capability to scale quickly to extreme capacity is not a common attribute or goal of traditional data centers and IT departments. Cloud computing promises the capability to scale massively in terms of systems, connections, bandwidth, storage, and more on an almost immediate basis. The converse is also important, where the service will shrink back down just as quickly if the need is no longer there. These benefits support cost management goals and enable you to grow in line with your requirements in a linear rather than a reactive mode.

7. Governance and Compliance

Governance is the process used to ensure that regulations, rules, and mandates are followed within an organization. Compliance refers to the facility to monitor and validate that the organization is meeting the governance requirements. Although cloud services introduce potential challenges in matching these requirements, the opportunities to improve an organization's governance and compliance stance can be greatly improved.

8. Device and location independence

Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

VI. SERVICE MODELS OF CLOUD COMPUTING

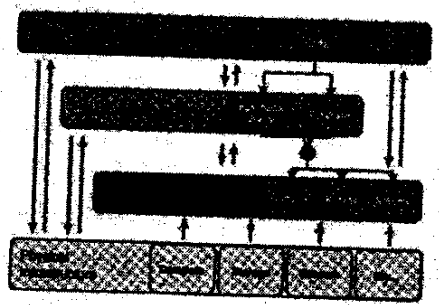


Fig. 3: Cloud Computing Service Models

Each service model of cloud computing offers different levels of capabilities and responsibilities to the provider and the consumer of the service. In addition, these service models may utilize a custom architecture, or the physical infrastructure, to exist. These services may rely on a service offering from a lower service model. In this way, cloud services in the higher levels, those being platform and software, may be entirely built atop other cloud services. The most compelling way to think about these models is that if everything has a set of APIs from the lowest to the highest levels, the service-orientated nature of cloud services becomes very clear, as follows:

1. Software as a service (SaaS):

The Software as a Service Cloud service providers offer specific application services delivered over the Internet on some form of on-demand payment system. Examples include Salesforce.com and WebEx. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. A SaaS application runs entirely in the cloud, i.e. on servers at an Internet-accessible service provider. The on-premises client is typically a browser or some other simple client. The most well-known example of a SaaS application today is probably Salesforce.com, but many, many others are also available.

2. Platform as a service (PaaS):

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. The Cloud service providers export application development platforms that broadly fall into two categories:- Those that export application development platforms for certain domains or class of applications (for example, the Google AppEngine and Force.com) - Those that export general purpose application development platform (for example, Microsoft's Azure). In either case, applications developed using these platforms benefit from elasticity offered by infrastructure-as-a service Cloud providers. For instance, the Google AppEngine is directed at traditional Web applications; applications developed using the AppEngine API can scale automatically with increase in the number of resources, as well as achieve high availability through replication.

3. Infrastructure as a service (IaaS) :

These cloud service providers offer computational services to consumer such as provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. These computational resources are managed by the provider to Cloud users on an on-demand basis. Examples of IaaS providers include Amazon Web Services and Flexi scale. IaaS providers allow users to dynamically grow and shrink their resource allocations to match their demands. However, the responsibility of utilizing this elasticity effectively rests with the Cloud user. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

VII. SECURITY ISSUES ASSOCIATED WITH THE CLOUD

Cloud computing security is also referred to as "cloud security". It is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud-based" (a.k.a. security-as-a-service). Many commercial software vendors have offerings such as cloud-based anti-virus or vulnerability management. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues.

1. Data and information security

In the area of multi-tenant data, you need to trust the cloud provider that your information will not be exposed. For their part, companies need to be alert about how passwords are assigned, protected and changed as examples. Cloud service providers typically work with numbers of third parties, and customers are advised to gain information about those companies which could potentially access their data. However, realistically, this could be easier said than done. An important measure of security often overlooked by companies is how much downtime a cloud service provider experiences. Ask to see service providers' reliability reports to determine whether these meet the requirements of the business. Exception monitoring systems is another important area which companies should ask their service provider about. An important consideration for cloud service customers, especially those responsible for highly sensitive data, is to find out about the hosting company used by the provider and if possible seek an independent audit of their security status. Customers typically do not seem to be as stringent about data and information security as one might think they should in many cases.

International Volume 1 Issue 11 ISSN: 2249-7862

2. Physical and personnel security Cloud computing

providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented.

3. Application security

Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures (application-level firewalls) are in place in the production environment.

4. Privacy

Providers ensure that all important data (e.g. credit card numbers) are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and testimonials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

5. Distributed cloud computing issues

Different customer's checkout and credit card transaction capabilities may be carried out using different servers in different data centers or even by different cloud providers. This may be happening with or without the customer's knowledge. This type of computing distribution is a very common cloud provider model. Cloud providers may have dozens of servers in dozens of data centers in dozens of Countries. If communications between the various cloud provider services is not strongly encrypted and extremely secure, your data and information could be at risk.

6. Security standards

In SaaS, the applications are constantly being twisted and revised, a fact which raises more security issues for customers. Companies need to know, for instance, whether a software change might actually alter its security settings. The cloud is still very much a new frontier with very little in the way of specific standards for security or data privacy. IBM, Cisco, SAP, EMC and several other leading technology companies created an 'Open Cloud Manifesto' calling for more consistent security and monitoring of cloud services. There are various web standards exists. Companies in the cloud computing should know about that standards. Chief among these is ISO27001, which is designed to provide the foundations for third party audit, and implements OECD principles governing security of information and network systems. The SAS70 auditing standard is also used by cloud service providers.

7. Every breached security system was once thought secure breach

SaaS (software as a service) and PaaS (platform as a service) providers all announce the strength of their systems, often claiming that security in the cloud is tighter than in most enterprises. But the simple fact is that every security system that has ever been breached was once thought infallible. Google's Gmail service was collapsed in Europe, while Salesforce.com is still suffering from a attack in 2007 which trapped a staff member into exposing passwords. While cloud service providers face similar security issues as other sorts of organizations, analysts warn that the cloud is becoming particularly attractive to cyber crooks. The richer the pot of data, the more cloud service providers need to do to protect it.

VIII. CONCLUSION

Ultimately, cloud services offer opportunities to source complete or partial services for all IT and business processes. Cloud services are changing business models and industries and are creating new opportunities for all. Cloud computing provides a level-playing field for smaller organizations. It allows smaller organization access to computing infrastructure without making any significant initial investment. ***To succeed with cloud services, business and IT leaders must recognize and deal with the fact that the role of IT is changing to include much more comprehensive supply chain management and vendor management. If cloud services are to be used, the traditional IT team makeup is incomplete and so must be enhanced with more legal, contractual, and business expertise. Those familiar with outsourcing are in a much better place to manage this new approach to delivering business value.***

References :

1) Sun Microsystems, White paper First Edition "Introduction to Cloud Computing Architecture", (June 2009)

2) Benoit Hudizia, "Cloud Computing : Principles and Paradigms", (January 2011)

3) Subra Kumaraswamy, Tim Mather & Shahed Latif, "Cloud Security & Privacy: An Enterprise Perspective on Risk and Compliance" (Sept 2009)

4) Antonopoulos, Nick, Gillam, Lee, "Cloud computing Principles, System and Applications", 1st edition, (Nov 2010)

5) George Reese, "Cloud Application Architectures", O'Reilly Media, Inc., (April 2009)

6) Velte A., Velte T., Elsenpeter R., "Cloud Computing: A Practical Approach", McGraw-Hill Osborne (June 2010)

7) Rhoton John, "Cloud Computing Explained", 2nd Edition, Recursive Press, UK (March 2009)

8) NOC_Designs, The "No Network is 100% Secure" series- Cloud Computing A white paper (2011)