



## **CLOUD MARKETING**

*(Profit by Saving Time, Money & Resources)*

**Krunal Fulchand Parate**

MMS (Marketing)

Dr. VN Bedekar Institute of Management Studies, Thane

Mumbai University

### **ABSTRACT**

*Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So, it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.com and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyses the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.*

**Keywords:** Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Grid Computing



## **INTRODUCTION**

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis.

In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers. Cloud computing appeared as a business necessity, being animated by the idea of just using the infrastructure without managing it. Although initially this idea was present only in the academic area, recently, it was transposed into industry by companies like Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new start-ups to enter the market easier, since the cost of the infrastructure is greatly diminished. This allows developers to concentrate on the business value rather on the starting budget. The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs. Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser.

## **OBJECTIVE OF STUDY**

- To study different type of tools in Cloud computing and their process
- To know about how the marketing is done through Cloud Computing
- The market capitalization of SEO, PPC, Sales Force.
- To Learn the operation of Cloud Marketing
- To Know about the cyber security & Safety of cloud computing

## **RESEARCH METHODOLOGY**

The given research paper is based on the secondary source of data collected from various newspapers and magazines, journals on Marketing and latest news.

### **REVIEW OF LITERATURE**

[Michael et al. 2010] Cloud computing is the IT liberation model that provides infrastructure and computer resources as service. In an organization, the information is shared by implementing the private cloud. The achievement of an organization is based on the important advantages such as simplifying management, reducing costs and accelerating processes. In a broad diversity of designs, the cloud computing technologies can be implemented under different services and deployment methods. In the organization cloud computing is used to transfer the existing server infrastructures into dynamic environments. By adopting the cloud computing, the business activities can be carried out with little difficulty and greater efficiency. Cloud computing offers many advantages to different ranges of customers and it is simple to acquire.

[Meiko et al, 2009] Generally, cloud computing provides the dynamical and scalable resources as a service over the internet. Cloud is used for reducing the capital and operational expenditure, and provides economic growth. This is happened in realism and however, there are some confronts are explained by the cloud. It is described as a valuable consideration for an enterprise IT integration. Even the adoption of cloud computing has many advantages and still it faces a number of risks. The security of cloud is one of the important issues in the cloud computing. By considering the above views of authors it can be concluded that cloud computing provides dynamical and scalable resources over the internet. Cloud provides economic growth and reduces the capital and operational expenditure. It defines as a valuable consideration for IT integration. It has a number of advantages but still it faces some risks. Sometimes cloud cannot provide security for the customer's property. It considers important disadvantages of cloud computing.

[Chang et al, 2005] Usually, in the cloud computing, the significant data of the customer can be stored in data centres. Actually, Data centres means where the data should be stored on the centralized location by having a large size of data storage. The data processing is done on the servers. The important data should be handled by the cloud provider. Therefore, the customers have to trust the cloud provider on the data security as well as on availability. For this, the legal agreement which is called as SLA (service legal agreement) should be provided by cloud computing between cloud customer and cloud provider. The provider can gain trust of the client through this agreement, so, SLA should be consistent. In the cloud environment, the whole security depends on the security levels of the cloud. This concept of cloud computing is promising to change the future of the computing by providing many benefits in the field. And the main obstacle in achieving this is nothing but the disadvantage of the security concern.

[McKinsey, 2009] Basically, cloud computing is the self-motivated specification of the IT capabilities (hardware, software, or services). Clouds are hardware based services that offers computing, networking and storage capacity. It has exclusive features that need risk measurement in parts such as data honesty, revival, and privacy. A security perimeter is set up to create a trust boundary where customer's valuable information is stored and proceed. The network provides transportation to which works in a similar manner, and which consist of other trusted end hosts. The confidential information may be processed outside and identifies trusted areas as these computing environments often have unclear boundaries as to where data is stored and processed and when the security perimeter becomes unclear in the sense. Privacy issues which frequently happen in the cloud are not only raised by public cloud and also have its own security concerns.

### CLLOUD COMPUTING BUILDING BLOCKS

Different models of cloud computing Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

**Software-as-a-Service (SaaS):** SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support. SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data centre space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

**Platform as a Service (PaaS):** "PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end- users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

**Infrastructure as a Service (IaaS):** Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, Go Grid.

There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

**Private cloud:** Private cloud can be owned or leased and managed by the organization or a third party and exist at on premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems.

**Public Cloud:** A cloud infrastructure is provided to many customers and is managed by a third party and exist beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance.

Customers are only charged for the resources they use, so under-utilization is eliminated.

Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine.

**Hybrid Cloud:** A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

**Community Cloud:** Infrastructure shared by several organizations for a shared cause and may be managed by them or a third-party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook which is showing in figure.





Cloud computing entities Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows

**Cloud Providers:** Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centres) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centres hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers.

**Cloud Service Brokers:** Includes technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

**Cloud Resellers:** Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region. Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller. In the next section, key benefits of and possible threats and risks for Cloud Computing are listed.

#### **FINDINGS**

- Cloud computing is having certain issues, problems & risk associated with it. Some problems with clouds are Information Security, Compatibility, Standardizing Cloud Technology, and Monitoring.
- Information Security is one of the most major issues of cloud computing. It is completely based on the internet which makes it at risk of hack attacks. But it's also true that now a day all the modern IT systems are connected to the internet.
- In cloud computing it's easier for companies to quickly recover from such attacks because of its distributed network system. Compatibility with all IT systems in a company is another issue with cloud computing.
- Cloud Computing is most cost-efficient option for companies. But problem is to replace much of its existing IT infrastructures in order to make the system compatible on the cloud. Hybrid cloud is one of solution for this problem. Lack of standardization in the system is another issue of cloud computing.
- There is no proper standards for cloud computing are set yet so it's almost impossible for a company to find out the quality of services.
- All the data is handled by service provider when cloud computing responsibility is taken by service provider. Monitoring of processes is another issue of cloud computing.

## **CONCLUSION**

The cloud computing is divided into three sections namely cloud application, cloud platform, and cloud infrastructure. It has some issues in their operation they are: operational security, privacy, reliability, accessibility, non-reputation, failures in the security provision, other customer attacks, legal and regulation issues, and perimeter security model broken. The fuzzy keyword is extensively prolonged the system usability by means of giving back the alike files when the users penetrating contributions equals the predefined keywords correctly. The significance of the fuzzy search has increased focus in the conditions of the plain text search in information recovery zone.

Cloud Computing has lots of benefits of cloud computing like Increase volume output or productivity with lesser manpower. Which reduces cost per unit of project or product. It helps to access to our information with minimal spending on technology infrastructure. It gives access of out information worldwide where they have an Internet connection. It helps to get more work done in less time with less manpower. It saves money sending on hardware, software or licensing fees. Cloud is accessible 24X7 and 365 days from anywhere which makes our life much easier! It is cost saving because we pay for what we use.

Easy on installation and maintenance, we can get almost unlimited storage, it is highly automated and Flexible with better mobility. Resources are shared and back up and restoration is available in both automatic and manual mode. Cloud computing increases collaboration by allowing all employees wherever they are to sync up and work on documents and shared apps simultaneously, and follow colleagues and records to receive critical updates in real time. Businesses using cloud computing only use the server space they need, which decreases their carbon footprint. Using the cloud results in at least 30% less energy consumption and carbon emissions than using on-site servers. And again, SMEs get the most benefit: for small companies, the cut in energy use and carbon emissions is likely to be 90%.

## **REFERENCES**

- Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006
- Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
- Arshad, J, Townsend, P. and Xu, J. (2013). A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416-428. doi: 10.1016/j.future.2011.08.009
- Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
- Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103.