Business of Cloud Computing: Issues in Accounting, Auditing and Taxation

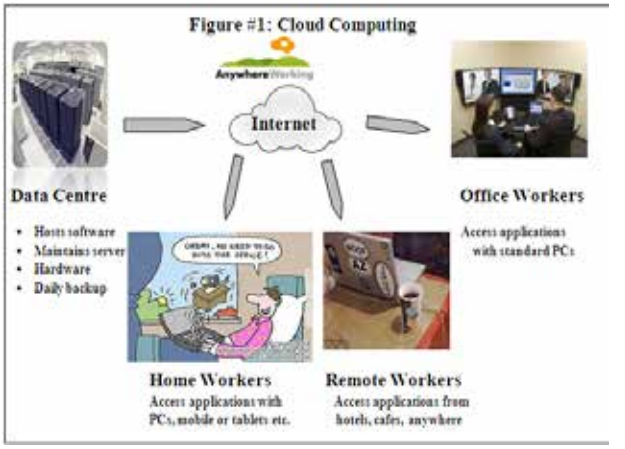
Cloud computing is an innovative IT architecture, which has leveraged users from hardware requirements, while reducing overall client-side requirements and complexities. In this paper, we attempt to demystify the unique security challenges introduced in a cloud environment and clarify issues from a security perspective. *Cloud* is a metaphor for *Internet and cloud computing* that refers to various IT resources (infrastructure, platform, applications) being delivered over the internet as a service. Cloud computing heralds an evolution of business that is no less influential than e-business. By 2015, cloud computing will generate $200 billion to $250 billion in economic activity; in India itself, it will grow at a CAGR of 40%. Given these huge figures and to carve out a niche, it becomes imperative for us to comprehend the term. This paper attempts to conceptualise cloud computing in a non-technical manner, outlining its business model and meticulously deliberate the legal, accounting, auditing and taxation issues relating to it. Read on…

1. Introduction to Cloud Computing

Cloud is the condensed state of vaporised water from the earth; it then comes back to the earth in the form of rains, but in terms of IT, it is used only as a metaphor for the internet. Most probably, it was derived from the diagrams of clouds used to represent internet in the textbooks. *Cloud computing* refers to a range of servers located remotely which not only host computing applications but also deliver software, infrastructure and storage on the internet.

Computing refers to the use of computers to process data and perform calculations. In that sense, *cloud computing* means internet-based computing in which a large group of remote servers are networked so as to allow sharing of data-processing tasks, centralised data storage and online access to computer services or resources.

Figure #1: Cloud Computing



Ravindra Singh Parwal

(The author may be contacted at savant_ravi@yahoo.co.in.)

Though the phrase *cloud computing* may appear to be new, in technology, it is not a new concept; it is a culmination of many primary technologies such as grid computing, utility computing, SOA, Web 2.0 and other existing ones. Remote computing has been here since 1960s. What is new is the scale. We are using it without even knowing it. Simplest illustration is an e-mail that we use, e.g. Google mail, Yahoo mail, Hotmail, etc. Also, the use of Google docs in place of MS Word document or MS Excel sheet is also a part of cloud-computing environment. But, everything we use on internet is not cloud computing. When we download a song from iTunes onto our computer, we are using internet but not necessarily the cloud. When we store music in a remote server, such as Amazon's or Google's, and have device dependent access to it, we are using both the internet as well as the cloud.

An expounding and most widely-used definition of the term has been given by Mell and Grance (2009) from National Institute of Standards and Technology, U.S. Department of Commerce: *Cloud Computing is a model for enabling ubiquitous, convenient, on demand 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.*

Further, they summarise the five-point essential characteristics of cloud computing:

1. *On-demand self-service*: user can use computing capabilities *as and when required*, that too with no human interaction.
2. *Broad network access*: capabilities are available over the internet and can be accessed through standard mechanisms such as computers, mobile phones and tablets.
3. *Resource pooling*: providers bundle the capabilities to server multiple consumers using a multi-tenant model; different users (tenant) share the same underlying resources without even having knowledge of its location, e.g. resources like storage, processing, memory and network bandwidth.
4. *Rapid elasticity*: capabilities can be easily scaled up and down according to the demand of users; unlimited capabilities are available infinitely for users and these can be apportioned in any quantity at any time.
5. *Measured service*: use of resources is monitored, controlled and reported by employing a metering capability appropriate to the type of service, e.g. storage, processing, bandwidth and active user accounts.

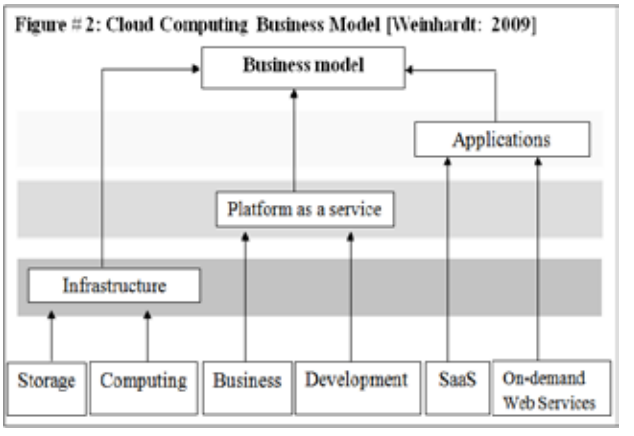
Further, a cloud can be a public cloud or a private cloud—a public cloud is open for use by general public and generally at no or low cost and exists on the premises of the cloud provider; and on the other hand, private cloud infrastructure is for the exclusive use by a single organisation at a certain price to be paid on *pay-as-you-use* basis and may exist on or off premises.

To sum up, *cloud computing* is a way of using computers in which data and software are stored mainly on a central computer (cloud), to which users have access through internet. While definitions, taxonomies and architectures are interesting, it is more important for us to understand the business model for cloud computing. We need to understand how suppliers of cloud technology will come together to deliver on the promise of cloud computing.

2. The Business Model

The first thing is that cloud computing is not a separate sector or industry. In terms of purchase of business processes, it can be called as an advanced stage of outsourcing where IT infrastructure is purchased instead of outsourcing of business processes.

Figure # 2: Cloud Computing Business Model [Weinhardt: 2009]



In terms of delivery mechanism, there can be three types of service models, which can be used to describe various business models for cloud computing:

1. *Infrastructure*: the user enters into an agreement with the cloud service provider for the provision of data *storage* and various other *computing resources* including processing, sharing and networks, where

it can run its software and applications. It is referred to as Infrastructure as a service (IaaS), e.g., Examples are: Amazon web service, EC2, Gogrid, etc.

2. *Applications*: the user is provided with the use of applications running on the cloud infrastructure. Applications are accessed through a thin client interface (like web browser) or a programme interface. It is termed as *Software as a service (SaaS)*. Christof Weinhardt (2009) distinguishes between SaaS applications and the provisioning of rudimentary Web services on demand. The most prominent examples are: Google Docs and sales force.
3. *Platform as a service (PaaS)*: the cloud provider hosts libraries, programming languages, services and tools onto the cloud infrastructure with which the user is able to create or acquire applications. Weinhardt classifies platform as business platform and development platform.

The most important and interesting part of the service models is that the users do not manage or control the underlying cloud infrastructure including network, servers, storage, etc., or even individual application capabilities. They don't even know where their data is stored, but they are using it *as-and-when-required*.

Further, a cloud can be public or private—a public cloud is open for use by general public and generally at no or low cost and exists on the premises of the cloud provider; and on the other hand, private cloud infrastructure is for the exclusive use by a single organisation at a certain price to be paid on pay-as-you-use basis and may exist on or off premises.

While providing the cloud-based services, various actors are involved in the channel, identified as *vendors*—supplying cloud services, service providers—providing connectivity mechanisms, distributors and aggregators—acting as intermediaries for consolidating solutions, systems integrators—building cloud infrastructures (IaaS), VARs (value-added resellers) & MSPs (managed service providers) brokers and managing cloud-customer relationship, and solution providers—implementing cloud applications (SaaS & PaaS).

The biggest technical barrier a cloud auditor may face is they may not be permitted to access systems and data on the cloud; moreover it is often unknown where the data is being stored. This raises various concerns for the auditor and the worst thing is that the professional organisations such as IAASB, AICPA, CICA, ISACA or the corresponding Indian board AASB of ICAI, still have not define cloud audit requirement specifically, although progress is being made in this arena.

3. How to Regulate

In relation to cyber laws, regulations in India are still at its nascent stage and a lot of work is to be done. For instance, we do not have data privacy, data security and data protection laws. The only legislation we have is the Information Technology Act, 2000, which is focussed on legal recognition of electronic documents, e-commerce and cyber crime in general and is not a data privacy protection *per se*. Yet, Sections 43, 43A, 65, 66 and 72 of the Act deal with penalty and compensation against breach and misuse of data in India:

Section 43	Damage to computer, computer system etc. Unauthorised copying, extraction, database theft, and digital proofing.	Compensation to the affected person upto ₹ 1 crore
Section 43A	Failure to protect data	Compensation to the affected person
Section 65	Tampering with computer source documents	Imprisonment upto 3 years or fine upto ₹2 lakh or both
Section 66	Hacking with computer system	Imprisonment upto 3 years and fine upto ₹2 lakh or both
Section 72	Breach of Confidentiality and Privacy	Imprisonment upto 2 years or fine upto ₹1 lakh or both

The Supreme Court has time and again equated the *Right to Privacy* with the fundamental Right to "Protection of life and personal liberty". The Apex Court observed that *"...the concept of liberty in Article 21 was comprehensive enough to include privacy..."* Despite this, phone-tapping and e-surveillance is done without a court warrant and beyond the judicial scrutiny. In the cloud computing environment, the police or a government officer can get access to data just

by approaching the cloud service provider. In addition to that, there are several other issues that may arise due to the complex business model and involvement of a gamut of intermediaries such as national security—as it involves huge cross-country data flows, localisation rules, jurisdiction, etc.

In a nutshell, the present regulatory framework does not offer a complete solution to the issues that emanate from the business of cloud computing technology. An efficient regulatory framework would give confidence that the service providers will provide the service securely and reliably. But, there should not be a cloud-specific legislation as it could weigh down the potential of the budding cloud computing.

4. Accounting Issues

Traditionally, companies need to invest heavily in IT-architecture, whereas with the use of cloud services they can now manage their IT demands according to the requirement. They exploit the cloud service on pay-per-use basis. This shift from a capital expenditure (CAPEX) model to an operating expenditure (OPEX) model raises various concerns for accounting, e.g., how a transaction is treated, when to recognise the revenue, implications in budgetary process, etc. Answers to these questions need to be answered by a proper authority, undoubtedly, the ICAI; however, in the present scenario, the following treatment could be given to the cloud transaction:

1. Under IaaS model, transaction between the cloud service provider and user can be classified as 'Leases'. Typically, as per AS 19, it is an operating lease and the treatment shall be:
   a) *In the books of user*: Lease payment shall be recognised as expense in profit and loss accounts P & L account on straight line basis over the term of contract.
   b) *In the books of vendor*: Asset shall be recognised and lease income shall be recognised as income in P & L using straight line method. Further, depreciation as per AS 6 shall be claimed.
2. Under PaaS or SaaS model, it would be a *service contract* where a cloud vendor provides multiple services like customisation of the platform, hosting, support, etc. In order to have a classification of the contract, various components of the contract are to be looked into. The vendor shall recognise revenue either by the application of *Proportionate Completion Method* or by the *Completed Service Contract Method*.
   Under IFRS, revenue recognition from each component begins once the initial configuration is completed and delivery of the cloud computing services commences.

5. Auditing Issues

The principal issue in auditing cloud based services is the lack of understanding of how the cloud differs from the traditional enterprise IT. The biggest technical barrier a cloud auditor may face is they may not be permitted to access systems and data on the cloud; moreover it is often unknown where the data is being stored. This raises various concerns for the auditor and the worst thing is that the professional organisations such as IAASB, AICPA, CICA, ISACA or the corresponding Indian board AASB of ICAI, still have not defined cloud audit requirement specifically, although progress is being made in this arena.

Cloud and Numbers:

- Cloud Computing will expand from $46.4 billion in sales in 2008 to more than $150 billion by 2013 [Gartner]
- by 2015 it will generate $200 billion to $250 billion in economic activity [Gartner]
- cloud market in India is expected to cross $1.08 billion by 2015 from $110 million in 2010 [Zinnov]
- cloud computing market in India will grow at a compound annual growth rate of 40 % by 2014
- it will account for 5 % of the total investments in India by 2015 [Gartner]
- the use of the private cloud model by two or more states could result in savings of up to 50% in the ₹1,378 crore allocated for state data centre projects [Govt. of India estimates]

AICPA provides a standard SAS-70, by which a service organisation can demonstrate the effectiveness of their internal controls. Under SAS-70, a certified

Is the offering a taxable or non-taxable service? Is it a data processing or information service? Is it a sale or a lease of tangible personal property? While a significant number of nations have addressed cloud services from a SaaS point of view, very few have addressed tax classification from an IaaS or PaaS standpoint, and very few have updated their statutes and regulations to address this emerging use of technology.

independent service auditor performs an audit and issues a report that may be shared with audit teams of the service auditor's clients. With effect from 15th June, 2011, a more inclusive statement SSAE–16 has been issued, which provides a more in-depth range of options in their reporting. This SSAE–16 replaces SAS–70. The major difference between SAS–70 and SSAE–16 is that the latter is an attest standard whereas former is an audit standard.

The SSAE–16 is in line with the ISO reporting standard ISAE–3402, issued by the IAASB of IFAC. The IFAC in its second publication of *Guide to Practical Management for Small and Medium Sized Practices* issued a guidance on cloud computing.

The ICAI has also issued standards which are at the level of the standards issued by the IAASB of IFAC. Two of the standards, namely SA–402 *Audit Considerations Relating to an Entity Using a Service Organisation and SAE–3402 Assurance Reports on Controls at a Service Organisation* serve the purpose. SA–402 establishes standard for an auditor whose client uses a service organisation. It also provides types of report of the auditors of the service organisation which may be obtained by the auditor of the client.

The Auditor of the *organisation using the services of a cloud provider* shall:

a) Obtain an understanding of the nature and significance of the services of the *cloud provider*;
b) Assess the effect of the services on the user entity's internal control; and
c) Design and perform the audit procedures responsive to the risk of material misstatements.

If the user auditor is unable to obtain a sufficient understanding from the user entity, the user auditor shall obtain that understanding from one or more of the following procedures:

(a) Obtaining a Type 1 or Type 2 report, if available;
(b) Contacting the service organisation, through the user entity, to obtain specific information;
(c) Visiting the service organisation and performing procedures that will provide the necessary information about the relevant controls at the service organisation; or,
(d) Using another auditor to perform procedures that will provide the necessary information about the relevant controls at the service organisation.

If the user auditor is unable to obtain sufficient appropriate audit evidence regarding the services provided by the service organisation relevant to the audit of the user entity's financial statements, she/he shall modify.

The Auditor of the cloud provider shall:

a) Obtain reasonable assurance about whether, in all material respects, based on suitable criteria:
   (i) The service organisation's description of its system fairly presents the system as designed and implemented throughout the specified period;
   (ii) The controls related to the control objectives stated in the service organisation's description of its system were suitably designed throughout the specified period;
   (iii) Where included in the scope of the engagement, the controls operated effectively to provide reasonable assurance that the control objectives stated in the service organisation's description of its system were achieved throughout the specified period;
b) Report on the matters in (a) above in accordance with the service auditor's findings.

6. Taxation Issues

As per a global cloud survey, *approximately 45% of the respondents are neither evaluating the tax implications of cloud nor do they know if these factors are being evaluated within their organisation*. A major challenge in the taxation of cloud offerings is in the tax classification of cloud services themselves. Is the offering a taxable or non-taxable service? Is it a data processing or information service? Is it a sale or a lease of tangible personal property? While a significant number of nations have addressed cloud services from a SaaS point of view, very few have addressed tax classification from an IaaS or PaaS standpoint, and very few have updated their statutes and regulations to address this emerging use of technology.

It may be difficult to arrive at any concrete conclusion on the appropriate tax treatment of the new business model as it involves multiple (and intricately connected) features or transactions. In certain situations, an argument may be raised that payments for certain forms of cloud computing services may be classified as fees for technical services, the tax implications of which are similar to that of royalty. But in standard structures where the client does not exercise any control over the cloud server and merely procures certain platform, infrastructure or support services, the consideration paid to a foreign service provider should normally be treated as business profits. This would be taxable in India only if the service provider has a permanent establishment (PE) in India.

There are various issues with the emerging technology like nexus of taxation, applicability of service tax, VAT, etc. It is very necessary for the policy makers to ensure that tax and other regulatory factors should not become an impediment to the growth of innovation and technology.

7. Conclusion

Cloud computing in India is estimated to create about one lakh job opportunities for people specialised in cloud computing by 2015. It is poised to become one of the largest revolutions in this era for the IT industry, but yet it is in the budding stage. A lot of work needs to be done, ranging from a proper legal framework to taxation rules and accounting and auditing issues as well. Recently, the Bangalore Branch of ICAI organised a National Conference on Cloud Computing to analyse and understand the impact of cloud computing on the CA profession. Chartered accountants must be familiar with the basics of cloud computing in order to discuss potential risks and benefits with their clients effectively.

In 2012, the telecom regulator TRAI also called for papers on *Regulatory Framework for Cloud Computing* for a conference to explore the various challenges that exists in cloud computing. It has also recommended its National Telecom Policy 2012 where it has suggested a setup of an efficient cloud computing environment. Strategies suggested by TRAI are as follows:

1. Adopt best practices to address the issues related to Cloud Services
2. Create a secure network for cloud computing covering encryption and privacy
3. Create a legal and security frame work covering network security, law enforcement assistance and preservation of cross-border data flows for deployment of Cloud Services
4. TRAI to devise appropriate mechanisms to provide interoperability among cloud computing service providers.

The ball is now in the court of our Government. Let us see how they react to these suggestions. ■