Telecom Regulatory Authority of India

Consultation Paper

on

Cloud Computing

10th June, 2016

Mahanagar Door Sanchar Bhawan,
J.L. Nehru Marg, (Old Minto Road)
New Delhi – 110 002, India

Stakeholders are requested to send their written comments, preferably in electronic form, by 08th July 2016 and counter-comments by 22nd July 2016 to Shri A. Robert J. Ravi, Advisor (QoS) TRAI on the email address advqos@trai.gov.in. Comments and counter-comments will be posted on TRAI's website www.trai.gov.in. For any clarification/ information, Advisor (QoS) may be contacted at Tel. No.+91-11-23230404, Fax: +91-11-23213036.

CONTENTS

CHAPTER-1

INTRODUCTION

1.1. The rapid evolution of processing power, storage technologies and availability of high quality broadband speed and big data have enabled the realization of a new computing model called cloud computing. In cloud computing, resources such as computing power &infrastructure, application platforms, and business processes are provided through the internet as general utilities to users in an on-demand fashion. A consumer can access and use these resources and services from anywhere and anytime through internet connection. The end user may not be aware of the equipment that is being used to provide him this service. Business enterprises are now increasingly seeking to reshape their business models to gain benefits from this new paradigm of resource sharing.

1.2. In a cloud computing environment, the traditional role of service provider is divided into three: the infrastructure providers who manage platforms in the internet cloud and lease resources according to a usage-based pricing model; service providers who rent resources from one or many infrastructure providers to serve the end users and service providers who offer cloud services.

1.3. According to the National Institute of Standards and Technology (NIST, USA), US Department of Commerce, Cloud computing is defined as "*a model for enabling ubiquitous 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.*"[1]

[1]The NIST Definition of cloud Computing, Peter Mell and Timothy Grance, September 2011

1.4. **Attributes:** Cloud Computing has four attributes mentioned below:-

(a) Data Intensive: The focus is on data rather than computation. Therefore, input/output (I/O) is more important resource metric than CPU utilization. Such data intensive cloud computing systems store enormous amounts of data at data centres and use computer nodes for computation services.

(b) Resource Pooling: Resource pooling or multi-tenancy characteristic of a software program enables an instance of the program to serve different consumers (tenants) whereby each is isolated from the other. IT resources can be dynamically assigned or reassigned; according to consumer demands. A cloud provider pools its IT resources using multi-tenancy models that frequently rely on the use of virtualization technologies.

(c) Scalability & Rapid Elasticity: Cloud computing platforms are usually highly scalable and elastic due to their inherent resource sharing behaviour. Scalability is the automated ability of a cloud to scale IT resources, as required in response to runtime conditions or as pre-determined by the cloud consumer or cloud provider. Elasticity is often considered as scalability supported with optimized utilization of resources as well as cost optimization.

(d) On demand access: A cloud consumer can unilaterally access cloud-based IT resources giving him the freedom to self-provision these resources. Once configured, usage of the self-provisioned resources can be automated, requiring no further human involvement by either the cloud consumer or cloud provider. This results in an on-demand usage environme*nt. In other words, it deploys pa*y-as-you-go approach with no upfront commitments.

1.5. **Service Models:** There are three main service models in cloud computing, as under:

(a) *Software as a Service (SaaS):* It is a software distribution model through which a consumer can use the provider's applications (software) running on a cloud infrastructure. The applications are accessible from various client devices such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure, with the possible exception of limited user-specific application configuration settings. Software testing takes place at a faster rate and IT operational costs are drastically reduced.

(b) *Platform as a Service (PaaS):* The service provides the consumer hardware and software infrastructure to deploy onto the cloud infrastructure consumer-created or acquired applications and tools supported by the provider. The consumer does not manage or control directly the underlying cloud infrastructure but has control over the deployed applications and possibly application hosting environment configurations. Such services enable the integration of web services and databases.

(c) *Infrastructure as a Service (IaaS):* It provides the consumer ability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run one's own software, which can include operating systems and applications. It provides substantial amount of flexible computing and storage infrastructure through virtualization.

There are also other service models like Data as a Service (DaaS), Identity and Policy Management as a Service (IPMaaS), Network as a Service (NaaS), Video as a Service (VaaS) or Hardware as a service (HaaS) amongst others.

1.6. A cloud system can be operated in one of the following four deployment models.

(a) *Public cloud:* The cloud infrastructure is made available to the general public or a large industry group and is owned by a third party selling cloud services. The cloud provider is responsible for the creation and on-going maintenance of the public cloud and its IT resources.

(b) *Private cloud:* The cloud infrastructure is operated solely for an organization managed privately. Private cloud enable an organization to use cloud computing technology as a means of centralizing access to IT resources by different departments or branches of the organization.

(c) *Community cloud:* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). Membership in the community, however, does not necessarily guarantee access &control of all the cloud's IT resources.

(d) *Hybrid cloud:* The cloud infrastructure is a composition of two or more cloud environments (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology enabling data and application portability.

The cloud model diagram and detailed description of Cloud Computing Reference Architecture is included in **Annexure-I**.

1.7. Established business enterprises as well as Small and Medium Enterprises (SMEs)[2] in India are now using online portals to sell their products domestically and abroad. These online platforms have allowed Indian SMEs to tap International customers in an extremely convenient, cost-effective, and profitable way. SMEs' IT requirements

[2] Regulation on cloud in India By Patrick S. Ryan, Ronak Merchant, and Sarah Falvey

are often not as complicated and extensive as those of large enterprises. Thus, they find it easier to outsource these functions to a cloud provider and focus on their core business. The low barrier to entry, minimum risk, lower capital expenditure on hardware and software make cloud computing an extremely viable option for most of the enterprises.

1.8. Though the cloud computing industry is poised for a leap, recent trends show that the SMEs are still reluctant to adopt the cloud. The barriers to the entry are security of data, interoperability amongst the cloud service providers in case of shifting the cloud computing services, initial investments required for shifting to cloud services, the quality of service for delivery over the cloud and the legal and regulatory issues associated with the industry.

1.9. Considering the large capital investments required for building the cloud infrastructure and the relevance of computing services for the global economy, a handful of companies might be able to achieve a dominant position in the cloud service offerings. This can be harmful to the interest of users when resource usage is dictated by corporations, risking the autonomy of users. Therefore, concerns regarding emergence of cloud computing monopolies have to be taken into account. Monopolistic market would also restrict small players to enter the market which may prevent innovation and evolution.

1.10. **National Telecom Policy:**

One of the key strategies of the National Telecom Policy (NTP)-2012 is to make it possible for millions of Indians to access services electronically in self-service mode using mobile phones and the Internet or through assisted service points such as Common Service Centres etc. Following strategies have been laid down in NTP-2012 with reference to Cloud Services:

(a) To recognise that cloud computing will significantly speed up design and roll out of services, enable social networking and participative governance and e-Commerce on a scale which was not possible with traditional technology solutions.

(b) To take new policy initiatives to ensure rapid expansion of new services and technologies at globally competitive prices by addressing the concerns of cloud users and other stakeholders including specific steps that need to be taken for lowering the cost of service delivery.

(c) To identify areas where existing regulations may impose unnecessary burden and take consequential remedial steps in line with international best practices for propelling the nation to emerge as a global leader in the development and provision of cloud services to benefit enterprises, consumers and Central and State Governments.

Reference by Department of Telecom (DoT):

1.11. Subsequent to issue of National Telecom Policy-2012, DoT through its letter dated 31.12.2012 has sought recommendations from TRAI on Cloud based services in the country broadly under following categories:-

- Regulatory framework for Cloud Computing
- Security over the Cloud
- Cost benefit Analysis
- Quality of Service of the Cloud Services
- Inter-operability amongst the cloud players
- Incentivisation for conceptualization and implementation of India based Cloud Services
- Legal framework for multiple Jurisdictions/Areas of operation
- Implementation Strategies of Cloud Services in Government (Central & States/UTs) Organizations and other strategic networks.

Subsequently, DoT, through its letter dated 22ndJune 2015, in response to TRAI's request for clarification, also informed TRAI about DeitY's initiative towards "Implementation Strategies of Cloud Services in Government (Central & State/UTs) Organization". DeitY has constituted a Task Force to recommend the policy framework and implementation roadmap for adoption of cloud services by Government users in India and working group for making government as the enabler for cloud eco-system and adopting a Cloud policy intervention for legal and regulatory framework.

1.12. With a view to bring out all relevant aspects of the issues and to provide a suitable platform for discussions, TRAI has initiated this consultation paper to engage the industry and all the stakeholders on the key issues referred by Department of Telecom.

1.13. While examining the various dimensions and areas of cloud computing, it is important to understand the **Current Trends in Cloud Computing** as the cloud computing industry advances worldwide. These issues are discussed in **Chapter-2**.

1.14. **Security** over the cloud is vital for cloud adoption. Without security, no cloud service could be effectively offered, though they may satisfy the need for manageability and interoperability. Specially, the SMEs should have confidence that their data is secure in the cloud. Security is needed not only for data but also for services and application to avoid their usage beyond trust boundaries. Transfer of data, sharing of information and use of third party systems are areas of concern. The extent to which the data is secure is now limited to the security controls and policies applied **by both the cloud consumer and cloud provider.** Accordingly, the security related issues are discussed in **Chapter-3**.

1.15. **Interoperability issue** is crucial to ensure that cloud service offerings are based on industry standards and are interoperable so that competition and fair value proposition in industry can be enforced. At present, due to lack of established industry standards within the cloud computing industry, public cloud are commonly proprietary to a great extent which pose a challenge on cloud consumers in case they want to move from one cloud provider to another. The consumers should be free to switch the cloud service providers if they are not satisfied. Interoperability may be needed at infrastructure level, platform level and software/application level.

1.16. **Quality of Service** standards are significant from the point of view of users of cloud computing services. The cloud largely depends on a fast and reliable connection to the Internet. This makes the quality of the cloud services highly reliant on the capabilities of the users' network connection. Further, in the absence of network connectivity, access to the services becomes impossible, necessitating offline data synchronization, which in many ways negates on many of the advantages that cloud computing offers.

1.17. The issues involved in interoperability and quality of cloud services are discussed in **Chapter-4**.

1.18. **Legal and Regulatory framework** s important for the orderly growth of the industry and to create confidence in the consumers. Regulations should be in place to protect the interest of both the cloud service providers and the consumers. Regulations are also required for standardization of technical parameters associated with cloud computing networks. Legal framework under which the cloud operates becomes very important. The various legal and regulatory issues are discussed in **Chapter-5**.

1.19. **Implementation of Cloud Services** is relevant considering the various cost benefits that Cloud Computing offers to the companies to achieve economies of scale. To accelerate the growth of cloud services **in India** and ensuring an enabling environment for organisations especially SMEs to adopt cloud services, for which certain incentives and regulations may be required. The various implementation issues are discussed in **Chapter-6**.

1.20. The **Issues for consultation** are compiled in **Chapter-7**.

Chapter 2

Current Trends in Cloud Computing

2.1. Cloud computing accounted for about 33% of the total IT expenditure in 2015 across the world[3].Analysts project that from 2013 to 2018, the cloud computing market will grow at a 9.7 percent annual rate. Also, by 2019, cloud IT infrastructure spending is expected to be $52 billion, or 45% of total IT infrastructure spending[4]. While new innovative and successful vendors are emerging; traditional big vendors are also investing massively in developing and acquiring on demand solutions. In the SaaS segment, the strongest markets in terms of size and growth are Content, Communication and Collaboration (CCC), Customer Relationship Management (CRM), Integration-as-a-Service, Enterprise Resource Planning (ERP), and Supply Chain Management (SCM). The use of SaaS, PaaS and IaaS has been evolving and becoming popular during the past years. Cloud server technologies to grow include fatter servers that allow larger instances or more virtual machines (VMs) per server; in-memory database instances with as much as 2 TB DRAM and remote direct access memory (RDMA) over Ethernet[5].

2.2. The need to house big data is certainly motivating developers to find new ways to meet demand optimally. Cloud security will remain a hot-button issue, as hackers claimed major retail breaches at some of the retail establishments like Target and Home Depot, the iCloud hack and, most recently, the Sony Pictures' attack.

[3]Worldwide Quarterly Cloud IT Infrastructure Tracker, April 21st 2015

[4]http://www.networkworld.com/article/2175333/cloud-computing/idc--cloud-will-be--107b-industry-by-2017.html

[5]http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-technology-trends-in-2015

2.3. Important points emerging from the current trends in cloud computing include the following:

- The proportion of cloud IT infrastructure[6] sales in the cloud industry climbed to 33.8% in last quarter of 2015, up from 28.7% a year ago. The revenue from infrastructure sales to the private cloud sector grew by 18.8% to $2.9 billion, while sales to the public cloud rose by 25.9% to $4.6 billion.
- Strong year-over-year growth in both private and public cloud segments is reported, with server sales leading the charge in the private cloud sector, growing at 24.3%. Meanwhile, in the public cloud, sales of Ethernet switches are growing fastest of all equipment types, rising by 37.8%. Public cloud spending on storage grew 26.7% year on year.
- Sales in Japan grew fastest at 47.1% year over year, followed by Asia/Pacific (excluding Japan) at 35.3%, Western Europe at 22.1%, Canada at 22.0% and the United States at 20.1%. However, sales in Central and Eastern Europe fell by 10%[7].Gartner predicts that by 2018 the Asia Pacific and Japan (APJ) region will account for $11.5 billion in total cloud services spending.

2.4. As per survey conducted by RightScale in January 2015, 93% of the organizations surveyed experimented with IaaS. 82% of enterprises had adopted hybrid cloud strategy, up from 74% in 2014. 88% had switched to public cloud while 63% started using private cloud. 13% of organizations surveyed run more than 1000 Virtual Machines in public cloud as shown in figure 2.1 below.

[6]latest *Worldwide Quarterly Cloud IT Infrastructure Tracker* from IDC , January 2016

[7]http://www.businesscloudnews.com/2016/01/15/global-spending-on-cloud-infrastructure-up-23-says-idc/

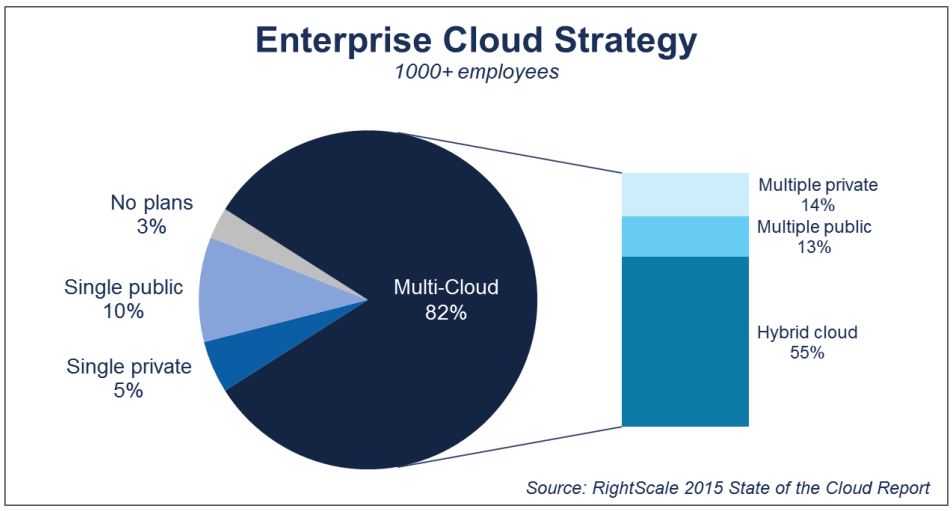

Figure 2.1: Enterprise Cloud Strategy trends

A. Cloud Computing Trends in India

2.5. In India, Cloud Computing offers huge potential for industries to grow and is opening up new windows of opportunities. Verticals such as retail, railways, manufacturing, banking, education and healthcare have started switching their on-premise applications to cloud services for optimised reach and performance as well as elasticity and scalability.

2.6. In 2015, revenue of public cloud services was driven by high rates of growth in key market segments, cloud infrastructure as a service (IaaS), cloud management and security services and cloud application infrastructure platform as a service (PaaS). IaaS made the largest contribution as the spending was estimated to be $104.8 million. As per Gartner report[8], 53 per cent of organizations in India indicated they are using cloud services, with another 43 per cent indicated their plans to begin using cloud services in the subsequent year. The overall cloud computing market reached $ 1.08 billion by the end of 2015. IT/ITeS, Telecom, BFSI, Manufacturing and Government

[8]http://www.gartner.com/newsroom/id/2964917

sectors contributed largest to the cloud market in India, with nearly 78% of the total market.

2.7. Few market predictions for cloud computing in India in upcoming years are as follows:-

- The accelerated penetration of smart city technologies will drive up demand for Internet of Things (IoT) devices to 1.6 billion units next year, up 39 percent from this year, according to research firm Gartner. It also predicts that smart homes will take 21 percent of total demand for IoT devices in 2016 and will record rapid growth in the next five years. This will proportionally boost up the cloud services.
- The public cloud service market in India will grow from $ 838 Million in 2015 to $ 1.9 billion by 2018.
- Forrester expects the software-as-a-service (SaaS) market in particular to roughly double in value, between 2014 and 2020, when it will be worth $1.2 billion. By 2018, Indian spending will reach $735 million for SaaS (from $249 million in 2014), $295 million for IaaS (from $77 million), and demonstrate strong gains in sub-sectors like PaaS and Business-Process-as-a-Service as well, according to Gartner.[9]
- Social, mobility, analytics and cloud (SMAC) are collectively expected to offer a US$ 1 trillion opportunity in 2016. Cloud represents the largest opportunity under SMAC, increasing at a CAGR of approximately 30 per cent to around US$ 650-700 billion by 2020.[10]

[9] http://www.gartner.com/newsroom/id/2869417

[10] December 2015 report by indiainbusiness.nic.in, Investment and Technology promotion division, MoEA, GoI

2.8. According to the TechSci Research report, "India Cloud Computing Market Forecast and Opportunities, 2020", the cloud services market in India is forecasted to grow at over a CAGR of 22% during 2015-2020. Rising availability of cloud services at economical price models and the ease of implementation are the major growth drivers for cloud services in India. In addition, increased government spending on new e-governance projects based on cloud technology and National Optical Fibre Network (NOFN) are also likely to drive the market for cloud computing services in India over the coming years.

2.9. Small and Medium size Enterprises (SMEs) account for more than 45% of the manufacturing output in India. With more and more SMEs coming up, cloud computing market is expected to escalate. Organizations in India seeking IT outsourcing services are increasingly turning to public cloud services as an alternative to traditional Information Technology Outsourcing (ITO) offerings. The total spending for cloud as a percentage of the total IT spends as such are expected to rise from 1.4% in 2010 to 8.2% in 2016.The private cloud deployments could result in potential savings of up to 50% on the IT investments on average, as compared with a legacy IT model, with cost optimization in areas such as telecom and networking, facilities and fabric, hardware, software, internal labours and external IT services.

B. Cloud Cost Benefits:

2.10. The fundamental driver for the move towards cloud is the huge potential for cost savings as discussed below. In any business entity, the benefits of cloud services are seen from financial and operational perspectives to evaluate savings and efficiency in the enterprise. From a financial perspective, capital expenditure (Capex) and information technology (IT) cost optimization are the perceived advantages. Removal of entry barriers, business continuity, mobile workforce, IT

agility and quick return on investments are possible advantages on operational front.

2.11. The reduction in ICT spending is manifold due to increased efficiency of Infrastructure usage i.e. from data centre consolidation, aggregation of demand and multi tenancy. Cloud technology standardizes and pools IT resources and automates many of the maintenance tasks done manually today. The most common economic rationale for investing in cloud-based IT resources is in outright elimination of up-front IT investments, namely hardware and software purchases and ownership costs. This elimination of up-front financial commitments allows SMEs to accordingly rationalise capital expenses.

2.12. The potential for cost savings varies, depending on the organization's computing and storage needs and how readily they can be served in the cloud. In some cases, data stored in the cloud may be more secure, since it is stored separately from the device and is secure even if the computer at user's end malfunctions. However, the potential benefits of cloud computing for SMEs need to be weighed taking into account the organizations needs in terms of privacy, security, regulatory compliance, existing hardware/infrastructure and many other crucial factors.

C. Modes of Cost Savings[11]

2.13. Cloud computing offers the users economies of scale and efficiency that exceed those of a mainframe, coupled with modularity and agility beyond what client/server technology offered. The following figure 2.2 depicts the cloud benefits.

[11]http://www.microsoft.com/en-us/news/presskits/cloud/docs/the-economics-of-the-cloud.pdf

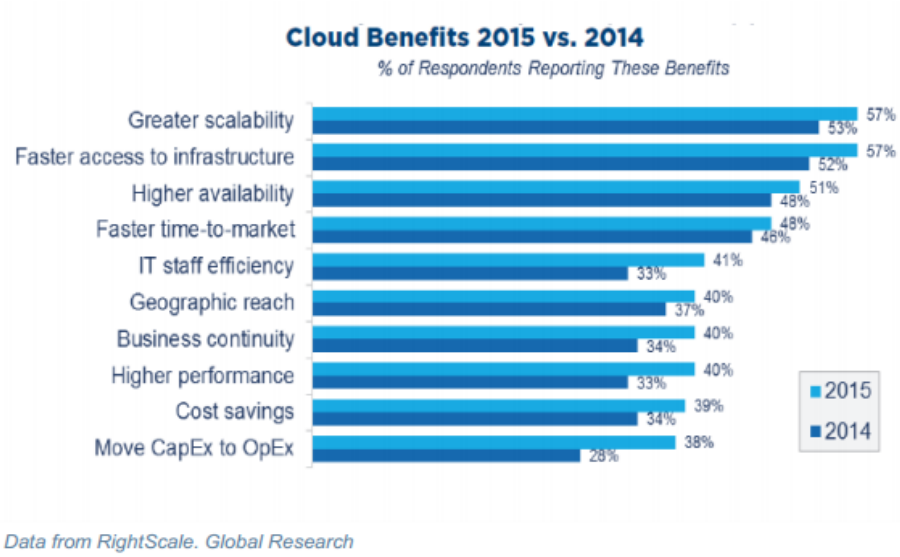

Figure 2.2: Comparative Analysis of Cloud Benefits

2.14. Cloud Computing allows core IT infrastructure to be brought into large data centres that take advantage of significant economies of scale in three areas:

- *Supply-side savings*- Large-scale data centres (DCs) with lower costs per server.
- *Demand-side aggregation*- Aggregating demand for computing smoothens the overall variability allowing server utilization rates to increase.
- *Multi-tenancy efficiency*- When changing to a multitenant application model, increasing the number of tenants (i.e. customers or users) lowers the application management and server cost per tenant.

2.15. **Supply-Side Economies of Scale:** The economies of scale at the supply side emanate from the following areas:

a) Cost of power- Electricity cost is rising to become the largest element of Total Cost of Ownership (TCO), currently representing 15%-20%. Power Usage Effectiveness (PUE) tends to be

significantly lower in large facilities than in smaller ones. While the operators of small data centres may have to pay the prevailing local rate for electricity, large providers can pay much less than the national average rate by locating its data centres in locations with inexpensive electricity supply and through bulk purchase agreements. Stable round the clock availability of electricity required in cloud data centres is essentially one of the biggest concerns.

b) Infrastructure labour costs- While cloud computing significantly lowers labour costs by automating many repetitive management tasks, larger facilities are able to lower them further still. While a single system administrator can service approximately 140 servers[12] in a traditional enterprise, in a cloud data centre the same administrator can service thousands of servers. This allows IT employees to focus on higher value-add activities like building new capabilities and working through the long queue of user requests every IT department contends with.

c) Security and reliability cost- While often cited as a potential hurdle to public cloud adoption, increased need for security and reliability leads to economies of scale due to the largely fixed level of investment required to achieve operational security and reliability. Large commercial cloud providers are often better able to bring in expertise to handle this problem than a typical corporate IT department, thus actually making cloud systems more secure and reliable in addition to cost savings. Cost of architecture - Operators of large data centres can get discounts on hardware purchases of up to 30 percent over smaller buyers. This is made possible by standardizing on a limited number of hardware and software

[12] 'THE ECONOMICS OF THE CLOUD'- Microsoft report (November 2011)

architectures. With cloud, infrastructure homogeneity enables economies of scale.

2.16. **Demand-Side Economies of Scale:** The overall cost of IT is determined not only by the cost of capacity, but also by the degree to which the capacity is efficiently utilized. The impact of demand aggregation on costs of actually utilized resources (CPU, network and storage) should be assessed. In the non-virtualized data centre, each application/workload typically runs on its own physical server. This means the number of servers scale linearly with the number of server workloads. In this model, server utilization has traditionally been extremely low, around 5 to 10 percent. Virtualization enables multiple applications to run on a single physical server within their optimized operating system instance so the primary benefit of virtualization is that fewer servers are needed to carry the same number of workloads. If all workloads had constant utilization, this would entail a simple unit compression without impacting economies of scale. In reality, however, workloads are highly variable over time often demanding large amounts of resources one minute and virtually none the next. This opens up opportunities for utilization improvement via demand-side aggregation and diversification.

2.17. **Multi-tenancy Economies of Scale:** If the applications running on the cloud are written as multitenant applications, multiple customers can use a single instance of the application simultaneously, without interfering with each other. Multi-tenancy offers fixed application labour amortized over a large number of customers for software, hardware and services. And fixed component of server utilization amortized over large number of customers.

Question 1. What are the paradigms of cost benefit analysis especially in terms of:

a. **accelerating the design and roll out of services**
b. **Promotion of social networking, participative governance and e-commerce.**
c. **Expansion of new services.**
d. **Any other items or technologies. Please support your views with relevant data.**

Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organisation?

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

Chapter 3

Interoperability and Quality of Service

3.1 As cloud computing becomes popular and competition between CSPs increase, the customers should have the freedom to switch between service providers for ensuring sectoral growth. The customers should not be locked on a single cloud provider. This would give customers the freedom to switch providers as their computing needs grow or shrink, and the ability to build more complex business applications to optimize their business requirements.

3.2 The ability to have multiple machines sharing resources on a single physical server and the ability to treat a machine as a file, opens up new possibilities. Virtualization is a first step toward moving applications to the cloud. While, the lack of standards isn't stopping customers from moving to the cloud, it is likely to slow them down. Interoperability and standardisation is a major concern after security towards faster adaptation of cloud.

3.3 *Interoperability* is essentially the ability to communicate across different systems. It requires that the communicated information is understood by the receiving system. In cloud computing, it means the ability to write code that works with more than one cloud service provider simultaneously, regardless of differences between the providers. *Portability* is the ability to run components or system written for one environment in another environment; this includes both software and hardware requirements.

3.4 *Need for interoperability:* Every cloud Service provider creates its own processes for a user or application interaction with the cloud leading to cloud Application Programming Interface (API) propagation. It leads to the issues such as vendor lock-in, portability and inflexibility to use multiple vendors in the cloud including the inability to use an

organization's own data centre resources seamlessly. There is a need for consistent data handling and predictable performance across disparate cloud providers within a cloud ecosystem enabling hybrid cloud. Such scenarios give rise to interoperability issues at business, security and functional interfaces.

3.5 In the one of the models of interoperability, the EU 4-level model[13], exchange of information between two systems can be considered as taking place on four levels which are layered so that the higher layers utilize the lower layers:-

(i) Technical interoperability is associated with the protocol used for information exchange – for example the use of the REST HTTP protocol over TCP/IP. The concern is the basic exchange of data between some endpoints.

(ii) Syntactic interoperability concerns the format of the data that is exchanged – examples here include Extensible Markup Language (XML) data structures or JavaScript Object Notation(JSON) data streams. The concern is the data being exchanged.

(iii) Semantic interoperability pertains to the meaning and structure of the data exchanged – examples here can include XML schemas (for the structuring) alongside directories or ontologies that describe the meaning of elements in the structures.

(iv) Organizational interoperability refers to the context in which the data is exchanged – that is, the sending system has an expectation that the receiving system will use the exchanged data in a specific way, typically as part of a larger overall process.

[13]2014 CSCC- Interoperability and Portability for Cloud Computing- A guide

3.6 The National Institute of Standards and Technology (NIST, USA) has proposed the following interoperability requirements:

(a) *Data Portability*: It relates to the capability of moving data in and out of the cloud service environment. Typically, it is the cloud service customer data which is the concern for data portability. However, some of the cloud service derived data may also be of concern in relation to some cloud services and should not be overlooked. For cloud service customer data, data portability is usually of most concern for SaaS cloud services, since for these services, the content, data schema's and storage format are under the control of the cloud service provider. Hence, the customer will need to understand how the data can be imported into the service and exported from the service. For IaaS and PaaS services, it is typically the case that the cloud service customer is in control of the content and schemas for the data, with the service offering basic storage capabilities such as a file system or object store and therefore, data portability might not be a concern.

(b) *System/Application Portability*: It involves Virtual Machine (VM) Images Migration. It relates to the capability of moving the App code to or from the cloud service. This typically only applies to IaaS and PaaS services, since in the case of a SaaS service; the App code belongs to the cloud service provider. One of the most important factors for application portability is represented by the *App environment*. To port code from one cloud service to another, the target app environment must be usable by the application being ported.

Figure 3.1 gives a schematic idea of these types of interoperability in cloud computing.

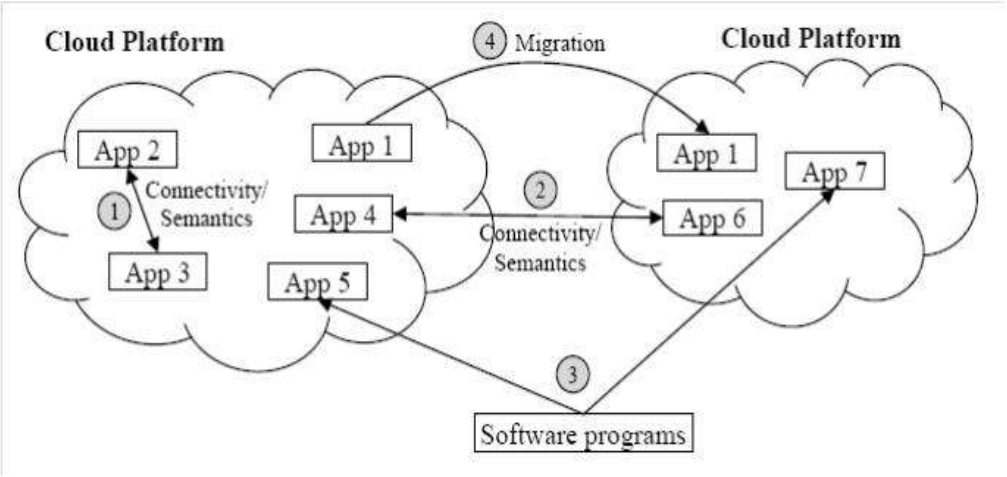

Figure 3.1: Types of interoperability between various applications on Cloud[14]

A. Challenges in Cloud interoperability

3.7 There are a number of issues that need to be dealt with before trying to move an application from one cloud to another. It is essential that virtualization technology is the same for both the vendors or else the virtual machine has to be converted to the other format. In such a case, performance level of the application and its interoperability with management, network and storage components needs to be addressed. The target cloud also needs to support the source cloud platform. On the similar lines, due to a lack of established industry standards within the cloud computing industry, public clouds are commonly proprietary to various extents. For cloud consumers that have custom-built solutions with dependencies on these proprietary environments, it can be challenging to move from one cloud provider to another.

3.8 Operating system versions and hypervisor versions that do not match can produce multiple conflicts. Cloud providers define the relationship between servers and storage, imposing constraints on each that perhaps did not exist with the original application. The application

[14]"Cloud Computing Interoperability Approaches –Possibilities and Challenges", Magdalena Kostoskaet. al.,

may have been designed to utilize certain storage technologies to achieve performance goals - storage technologies that the target cloud does not employ.

3.9 Almost every cloud has a unique infrastructure for providing network services between servers and applications and servers and storage. Differences are likely in network addressing, directory services, firewalls, routers, switches, identity services, naming services and other resources. Target cloud providers are usually going to have a network architecture that differs from the source cloud network architecture.

3.10 For system portability as mentioned in section 3.6 (b), an application description is required along with the description of the platform services. There can be four types of semantics[15] describing applications:

(a) *System Semantics:* Semantics pertaining to system characteristics like load balancing and deployment.

(b) *Data Semantics:* Semantics pertaining to data like manipulations restriction and storage.

(c) *Non-Functional Semantics:* Semantics pertaining to QoS characteristics like performance and security.

(d) *Logic & Process Semantics:* Semantics pertaining to core functions of the application like programming language, runtime, and exception handling.

[15]"A Survey on Approaches for Interoperability and Portability of Cloud Computing Services", Kostas Stravoskoufoset al.

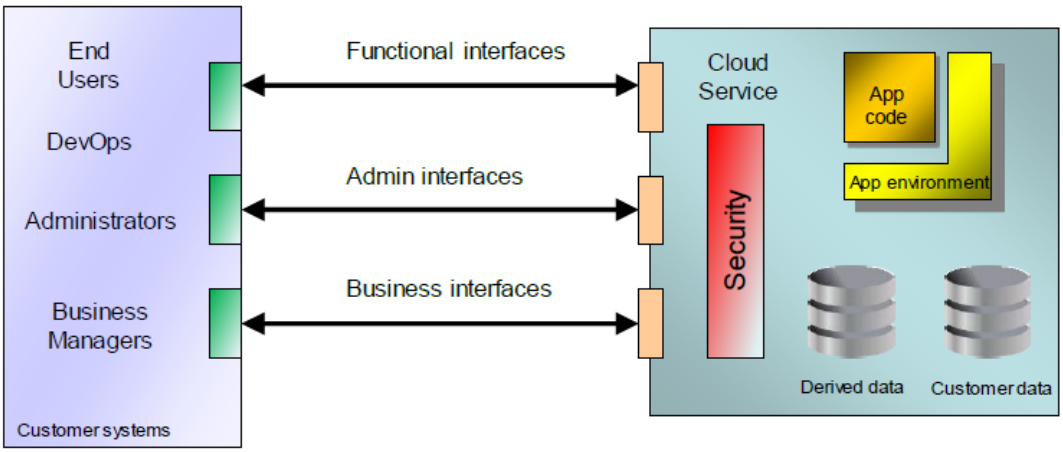

Figure 3.2: Elements of interoperability for Cloud Services[16]

The interoperability requires secure translation of these semantics while porting from one cloud to another. These semantics need to be addressed across various interfaces involved in deployment of cloud. Such interfaces are depicted in figure 3.2.

3.11 The greatest level of interoperability is likely to be found for IaaS cloud services, where functionality is often broadly equivalent and there are a number of standard interfaces - some formally standardized such as CDMI, others being de-facto standards in the marketplace. PaaS cloud services have lower levels of interoperability. There are few interface standards for PaaS functionality, although there are some open source platforms that are becoming popular in the marketplace and where different cloud service providers use the same open source platform, their interfaces are either identical or closely equivalent. It is SaaS applications which present the greatest interoperability challenge today. There are very few standard APIs for SaaS applications - even switching from one SaaS application to another SaaS application with comparable functionality typically involves a change in interface.

[16]2014 CSCC- Interoperability and Portability for Cloud Computing- A guide

3.12 Migrating an application across two different cloud environments means separating it from its original ecosystem; this may require re-engineering based on the components/parts that the target cloud provides. The data movement and the encryption of data also needs to be handled while it is in transit, when it is received by the target cloud and using new services that may not have been used originally or were not available in the source application. Differences between the source and the target cloud result in a sequence of integration issues and require rebuilding the application and application stack in the target cloud.

3.13 During closure of business, cloud provider should be obligated to support porting of its customers to another provider. If cloud provider is unable to do so then a regulatory mechanism may be required to port customers to another provider. Similarly, in case the service ceases i.e. the cloud provider is prohibited from providing cloud service due to any legal issue or government decision, a regulatory mechanism is needed to deal with issues that emerge thus.

B. Approaches for Cloud interoperability

3.14 There are many approaches being pursued currently but they are not suitable for all applications. Addressing this problem may require the development of interoperability standards. While standards may not be critical during the early evolution stage of cloud computing, they will become increasingly important as the field matures. **Annexure-II** discusses some of the international cloud standards.

3.15 Interoperability and standardization have huge impact on the cloud adoption and usage and thus, the industry is witnessing high amount of energy and thrust towards these from different stakeholders viz., users, vendors and standard bodies. It is also evident that there are multiple initiatives by stakeholders from industry, academia and users. The flip side is that this could lead to the possibility of several

standards emerging and possible lack of consensus, duplication and overlaps among the various groups involved.

3.16 Though initiatives like OCCI (Open Cloud Computing Interface) are trying to come up with standards in a quick timeframe, it takes time for standards to mature and for reference implementations to become available. Till then, the users will be using APIs/platforms from cloud computing vendors, whichever they feel is most suitable for their requirements. When standards emerge and these vendors want to use the services of other vendors, then they will need to use brokers/adapters for interoperability. Third-party vendors are going to be instrumental in solving cloud interoperability issues and if a cloud has the proper API, they may make it interoperate with other cloud. New users however will be able to natively use the standard API. There will also be vendors developing orchestration layers to build business processes/workflows using the cloud services provided by different vendors. This could lead to a scenario in the long run where multiple standards co-exist and customers may use brokers/adapters for interoperability for using services from multiple cloud service providers, which may lead to complexities and overhead costs.

Question 4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

C. Ensuring Quality of the Cloud Service

3.17 Everything in cloud computing is delivered as a service, so it is essential to ensure quality of cloud service for customer satisfaction. Specifically, in an effort to deliver guaranteed services in cloud computing environment, the relationship among the maximal number of customers, the minimal service resources and the optimised level of services is required to be explored. In cloud computing solutions, it is possible to specify compute, network, and storage requirements, to be shared by tenants in the same infrastructure. But, due to dynamic nature of virtualization environment and the workloads (Virtual Machine and software stack), performance turns unpredictable affecting the quality of service (QoS) available to the end customer. The balancing act between resource utilization and workload performance in a cloud environment affects both the Cloud Service Provider (CSP) and the stakeholders of a cloud service - cloud customer and the end user.

3.18 QoS is perceived by users based on various key parameters like high availability (guaranteed access to data), performance (throughput), security, resilience, reliability, self-service portals, response time and customer support, metering and billing accuracy, support in compliance of regulations etc. There have been several instances of outages in public cloud (Amazon EC2, Rack space, Google & Gmail, Twitter, Sony Playstation network) resulting in failure to meet these quality requirements. Hence, there is a need for cross portfolio integration and a framework for ensuring quality of service. Since cloud environments tend to be highly dynamic with network, compute and storage resources in a constant state of flux, the QoS of a cloud service should be monitored and managed at multiple layers from Network to Application. CSPs also need to specify and ensure quality of service on their entire service portfolio.

3.19 The generic quality of service requirements for cloud computing models are given below:

a) Ability of applications to handle varying levels of service accesses by end users.
b) Ability to scale up databases and guaranteed access to data with acceptable performance.
c) Ability to scale up computation power, network, and storage and support infrastructure based on the needs.

3.20 Once QoS controls are available, cloud providers offer a range of services and price points that provide more choice to customers and back these services with service-level agreements (SLAs) that go beyond uptime and mean time to repair (MTTR) specifications.

3.21 The terms and conditions of contract between the Service Provider and its Client are defined in **Service Level Agreements (SLA).** The SLA is a legally binding contract negotiated and agreed between a customer and a service provider. It containsthe QoS as agreed including response time, throughput, error rate, availability etc. It may include other non-functional requirements such as timeliness, scalability and other terms and conditions as well. Service provider is required to execute service requests from a customer within negotiated quality of service requirements for a given price.

3.22 The following compliances are necessarily required to ensure transparent audit capabilities and service availabilities:

(a) ***Loss of Service****:* Cloud computing environments are vulnerable to service outages, primarily due to interconnection between services like SaaS using virtualized infrastructures provided by an IaaS. This calls for the need of strong disaster recovery policies and provider recommendations to implement customer side redundancy.

(b) ***Audit****:* It allows security and availability assessments to be performed by the providers and customers. Transparent and

effective methodologies are necessary for continuously analyzing service conditions. Transparent APIs need to be offered for automated auditing and other useful functionalities.

(c) ***Service Conformity****:* Certain QoS parameters should relate to how contractual obligations and service requirements are offered based on the SLAs pre-defined and basic service and customer needs.

D. Key Parameters of QoS in Cloud Environment

3.23 **Availability**: Availability can be defined as a design by which the downtime of systems, network, storage and infrastructure are standardised thereby assuring uninterrupted services to its stakeholders. Typically, the availability is reported as number of "nines". For example, "six nines" 99.9999% means a downtime of 31.5 seconds a year and "four nines" 99.99% means a downtime of 52.56 minutes a year. A definition of high availability also takes into account the system down time due to scheduled maintenance. In order to ensure that systems in a cloud are always available, survival against multiple levels of failures should be designed. In case of IaaS, the high availability aspects are driven more from a hardware point of view to keep the systems in a healthy state. In other delivery models it is viewed from a software point of view like unavailability of services is related to downtime of applications deployed on the cloud, and unavailability of data is related to the downtime of associated storage infrastructure.

3.24 **Performance:** Any of the unavailability cases can result in services being available with insufficient processing power to meet acceptable performance levels. High Availability without acceptable performance levels would not help the customers using the cloud. Hence, a Quality of Service (QoS) definition of a cloud should define availability along with associated performance. The user perception of performance of

cloud also depends on the performance of network links connecting the user to Cloud.

3.25 **Response time**: In a cloud computing environment typically real-time scalable resource such as files, data, programs, hardware, and third party services are accessible to users from a Web browser via the Internet. The users pay only for the used computer resources and services with penalties imposed by means of customized service level agreement (SLA).

3.26 The Cloud QoS system must be able to manage several simultaneous services within specific response time limitation for each service. Scalability through dynamic ("on-demand") provisioning of resources on a self-service, near real-time basis, without users having to engineer for peak loads is desirable. In order to keep the response times alike even during peak periods, the cloud should be able to scale-up to the computation power, memory, storage and network resource demands. For example, during the end of month operations in a bank or online ticket reservations during holidays, demand for processing power and service availability could increase multi-fold.

3.27 **Metering and Billing/Charging performance**: Cloud is a pure utility renting computing model, where the resources can be utilised as per the need of the client. In such a scenario the accounting of resources used and billed needs to be substantiated by the cloud service provider by preserving the complete logs and all such other details which are essential for the complete satisfaction of the client. The satisfaction of the client with the billing performance may comprise of timely receipt of the bill, accuracy and completeness of the bill, clarity in bills/ presentation of the billing information in terms of transparency and understandability, and a transparent process of resolution of billing complaints.

3.28 The cloud service provider (CSP) should be able to provide a SLA measuring tool to the client so that the parameters agreed upon between the client and the CSP can be monitored by the client using the SLA tool. The billing will obviously depend on the performance or the extent to which the SLAs are met.

3.29 The Cloud Computing Innovation Council of India has recommended the following for adoption of standards for SLAs in cloud computing services:[17]

- Standards to be developed to represent SLA concerns and objectives of CU and CP, negotiations of SLAs with CPs, evaluation and assessment of SLAs, monitoring execution of SLAs, and formation of domain specific and generic QoS parameters.
- SLA parameters and SLA characteristics should be defined precisely in a single document. The metrics for SLA should be linked with SLA parameters and should be understandable by CP and CU.
- SLA technology managers and decision makers should collate on the finalizing of the SLA.
- Standard SLA template should be created and followed throughout the SLA lifecycle.
- SLA evaluation, execution, and violation should be automated.
- SLA soft and hard parameters to be identified as per domains.
- KPIs to be mapped with SLAs and other measures.

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.

[17]Cloud Computing Innovation Council of India white paper 2.0

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

Question 9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.

Chapter 4

Security over the Cloud

4.1 Migrating an on-premise application to the cloud may present the enterprise with a number of security risks and threats like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands. Making sensitive information available on the internet requires a considerable investment in security controls and monitoring access to the content. In the cloud environment, the enterprise may have little or no ability to store or backup processes and, as the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of file access and deletion becomes a significant challenge. Organized criminals and hackers see this as a new frontier to steal private information, disrupt services and cause harm to the enterprise cloud computing network. Internet browser is the first stage where security measures should be implemented because vulnerabilities in the browser open the door for many follow-on attacks. Security has therefore been indicated as the biggest for public cloud adaptation as shown in figure 4.1. Gartner predicts that by 2020, 95 percent of cloud security failures will be due to fault at the customer's end. This means the technology will be strong and secure, and that the only way data can be compromised is due to lack of understanding at the user side.

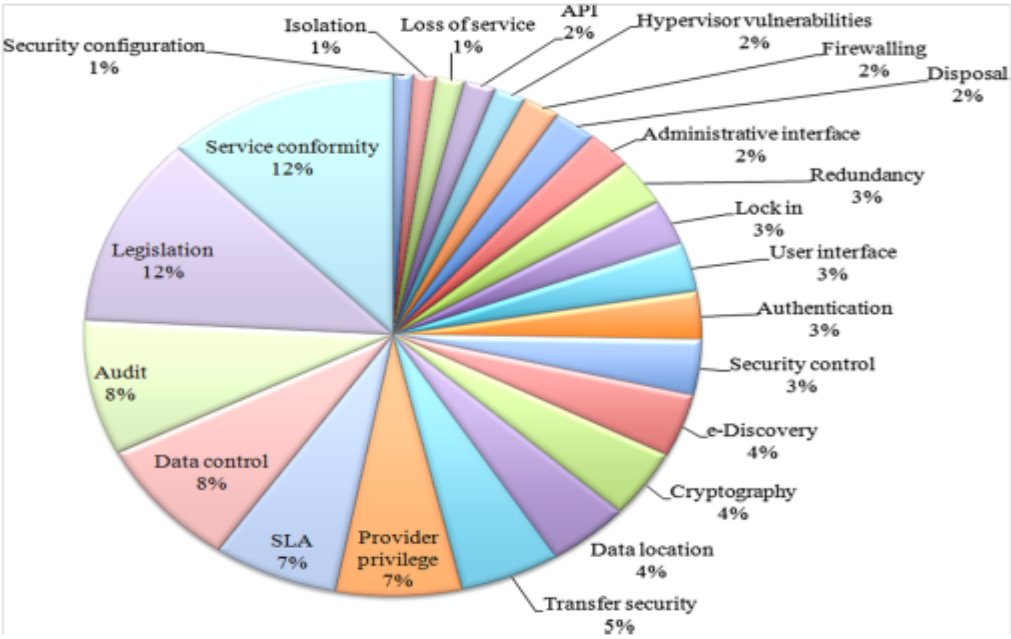

Figure 4.1: Security concerns for public cloud adaption

4.2 Some of the major security issues in cloud computing are discussed below :-

a) **Ease of subscription:** Infrastructure as a Service (IaaS) providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. The relative anonymity behind these registration and usage models could be misused by spammers, malicious code authors & other criminals and they may be able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from these kinds of attacks; however, recently hackers have begun to target IaaS vendors as well.

b) **Vulnerability of Application Programming Interface (APIs):** Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. Furthermore,

organizations often let third parties to build upon these interfaces for offering value-added services to their customers. This not only introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their systems integrate with others.

c) **Multi-tenancy Issues:** Infrastructure as a Service (IaaS) vendors deliver their services through a scalable model by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., Central Processing Units, Graphical Processing Units etc.) are not designed to offer strong isolation properties for a multi-tenant architecture. To address this issue, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or access to the underlying platform.

d) **Account or Service Hijacking:** Attack methods such as phishing, fraud and exploitation of software vulnerabilities are used for security hijacking. SaaS model is highly vulnerable to such attacks. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to a customer's credentials, he can eavesdrop on activities and transactions, manipulate data, return falsified information and redirect clients to wrong sites.

e) **Disaster Recovery issue**:-Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to failure. The ability of a Cloud service Provider (CSPs) to do a complete restoration, and the time required for it is an important consideration in case of a disaster. The cloud shall remain available to a user even in catastrophic situations and shall have the capability to recover to a safe mode.

f) **"Distant" Client & Risk Unawareness:** Cloud deployments are driven by groups for anticipated benefits who may lose track of the security aspects. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts and security design are all important factors for a company's security. Documentation of information about users who have access to infrastructure may also be pertinent in addition to network intrusion logs, redirection attempts and other logs.

g) **Cross Border or *Data location* Security issues:** One of the top security concerns of enterprises is the physical location of the data especially if they are located in another country because the laws of the host country apply to the machine and data residing on it. That becomes an issue if the host country does not have adequate laws to protect sensitive data or if the host nation becomes hostile and depends largely on the government concerned. The primary location of the data and any backup locations must be known to ensure these laws and regulations are followed.

As an example, the data protection laws of the European Union (EU) member states are extremely complex. The transfer of personal data outside these regions needs to be handled in very specific ways. For instance, the EU requires that data controller must inform individuals that the data will be sent and processed in a region outside of the EU. The data controller and end processor must also have contracts approved by the Data Protection Authority in advance. This will have different levels of difficulty depending on the region that's processing the data. The United States and EU have a reciprocal agreement, and the U.S. recipient only has to self-certify its data procedures by registering with the U.S. Department of Commerce.

It is therefore necessary to ensure that any cloud providers that are outside the jurisdiction have adequate security measures in place. This includes their primary and backup locations, as well as any

intermediate locations if data is being transferred between jurisdictions.

h) **Governance Associated Security issues[18]:** Cloud providers operating in international markets are concerned that an interest in ensuring security can sometimes lead to arbitrary reactions by governments. Especially when there is a major security breach, governments are more likely to pursue tighter regulation which may inhibit the development of the market. In terms of international cooperation on data security policy, a set of OECD guidelines (Organisation for Economic Co-operation and Development)offer basic principles. These Guidelines for the Security of Information Networks and Systems provide suggestions for how participants in information systems and networks can better anticipate risks, design and adapt security policies, and respond to threats, while preserving the rights of individuals.

i) **Stakeholders in cloud**: It is the responsibility of both service providers and end customers to ensure that applications, codes and data is safe and secure within the cloud environment. It is also significant that all those involved, understand their roles and responsibilities and are accountable. This also depends on the service delivery model (SaaS, PaaS, IaaS) and what services are contracted from CSP amongst others. All these have to be captured in the contract and Service Level Agreement (SLA). For example, in a SaaS model where a CSP provides applications, it is the service provider who is responsible for security of application and components being offered. CSPs have to implement fool-proof data access and security mechanisms to prevent any form of intrusion. However with most organizations undertaking customization of SaaS applications, it is for the end customers to ensure that the developed code is adhering to the best practices and have tested for

[18] Policy Challenges of Cross-Border Cloud Computing-Renee Berry and Matthew Reisman

security loopholes before being deployed. PaaS and IaaS on the other hand pose a different problem. In both these scenario's users have access to application code and underlying hardware. The role of CSP is only to provide hardware and API's to develop applications. Though security framework is to be defined by CSP, customer organization has to ensure that the platform is secured – both in terms of runtime engine and applications that are being developed and deployed. PaaS also supports the use of third party application components and even web services and hence, customer and third party application provider have to ensure security of the platform.

4.3 The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the following seven major threats (i) Abuse and Nefarious Use of Cloud Computing, (ii) Insecure Application Programming Interfaces, (iii) Malicious Insiders, (iv) Shared Technology Vulnerabilities, (v) Data Loss/Leakage, (vi) Account, Service & Traffic Hijacking and (vii)Unknown Risk Profile. Detailed security taxonomy for the same is shown in figure 4.2.

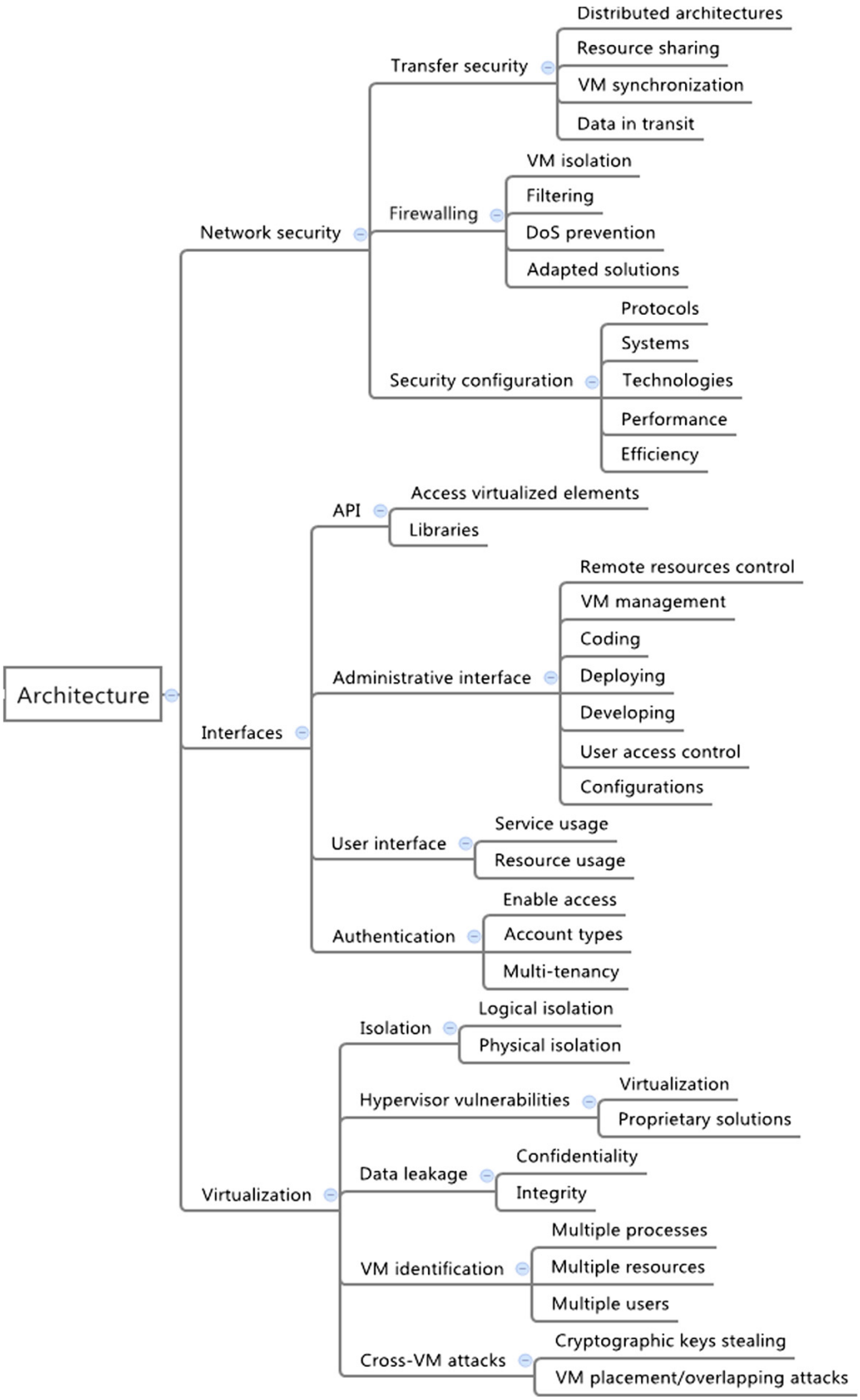

Figure 4.2: Security Taxonomy Architecture

4.4 To address the threats in cloud computing, some of the security aspects are broadly categorised as given below:-

(a) Infrastructure Security: The first level of security needed is at physical level, to ensure that cloud data centres and compute nodes are physically secure. The security of infrastructure and provisioning of secured environmental conditions is a basic requirement.

(b) Network security: In public cloud, security considerations increase multi-fold with respect to connectivity to cloud, security policies to be enforced and risks associated in data transfer to or from cloud. It is very important to optimize service availability by mitigating risks to network components. Guaranteed availability and performance of network links is a must for ensuring that resources in cloud are accessible from within the organization and outside.

(c) Application and Process security: It is essential tokeep applications secure, protected from malicious or fraudulent use and hardened against failure as customers require secure cloud applications and provider processes. Some of the vulnerabilities include (but are not limited to) cross-site scripting, Structured Query Language (SQL) injection and code hacking. Malicious users (hackers) with help of ever-evolving tools and technologies, scan for applications hosted on internet to exploit vulnerabilities, including complete hacking and defacing the website to capturing business and client sensitive information like credit card details, bank account information etc., leading to financial frauds. Two main root causes of such attacks are deficiency of security methodologies and design flaws. Coding practices and security processes followed as part of Systems Development Life Cycle (SDLC) should incorporate sufficient security into application code. Cloud Service Providers should use a combination of security layers – host access, perimeter and layered network security, federated access control, encryption – to protect applications hosted on cloud.

(d) Data security: All sensitive or regulated data needs to be properly segregated on the cloud storage infrastructure, including archived data.Compromising data by deletion of records without backup of original content, unlinking a record from a larger context, loss of encoding key and access to sensitive organizational data, pose a definite threat to the users. Lack of proper data protection techniques and legal laws are major factors that deter an organization or a user to utilize Cloud services.

4.5 Data security in cloud computing must necessarily be safeguarded when processing personal data. Confidentiality, availability and integrity of data must be ensured by means of appropriate organisational and technical measures. These also include the protection of systems and data from the risks of unauthorised or arbitrary destruction, arbitrary loss, technical faults, forgery, theft and unlawful use, as well as from unauthorised modification, copying, access or other unauthorised processing. The data collector must remain legally responsible for the observance of data security, even if he assigns data processing to a third party. It has the following four types:-

- *Data Integrity:* Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the cloud. Keeping data in the cloud means users may lose control of their data and rely on cloud operators to enforce access control.

- *Data Availability:* Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.
- *Data Location:* In general, cloud users are not aware of the exact location of the data center and do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have data centers around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architectures.
- *Data Privacy:* The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors that expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks.

Figure 4.3 below highlights the organization of data security issue in cloud computing:-

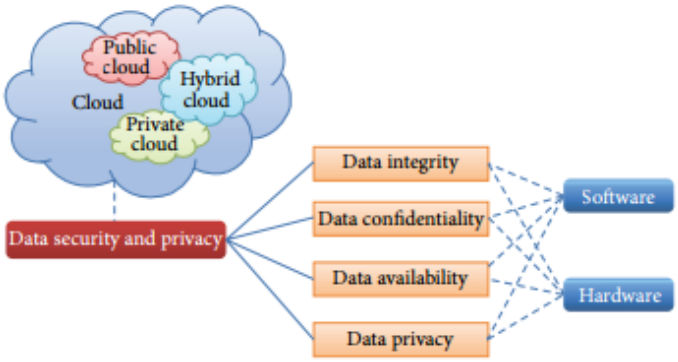

Figure 4.3: Organization of data security and privacy in Cloud Computing[19]

4.6 In a cloud computing environment, the ownership of data (for storage) is entrusted to the cloud provider and data streams are visible to the cloud provider in unencrypted form. This raises concerns regarding data being vulnerable to be sold, altered or compromised as presently there is no common security standard. There exist Privacy and Security Risks from Meaningful or Trusted Entities i.e. Cloud providers themselves may commoditize the data they hold, and take over a level of control. Information, wherever it is resident, is vulnerable to lawful access by national security agencies. Personal data or Internet Service Provider (ISP) data, stored in the Cloud might be accessed above and beyond what is intended by lawful access legislation.

4.7 Some of the methods to ensure security and avoid such threats in cloud computing deployments are discussed below:-

[19]Data Security and Privacy in Cloud Computing, Yunchuan Sun et al. Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2014, Article ID 190903.

a) Termination/exit provisions are required to be defined so as to ensure that the data remains with the actual owner only, in case the Cloud Service Provider (CSP) closes its operations or whenever the user so desires. It is essential that no left over image or part of data is withheld by the Cloud provider and complete data is made over as per the instructions of the user in a format that could be imported in to a replacement application by the user/ client. The assignment of a user's data without its specific consent is also a concern, for example, the CSP can't assign the data to another provider in the event of an acquisition.

b) Maintaining data segregation and confidentiality in the cloud can be achieved by using encryption, which is effective but it isn't a cure-all solution. For Encryption to be effective, its decryption must be segregated securely from the cloud environment ensuring that only a trusted-entity can decrypt the data. This requires a separate mechanism for storing keys, either in-house or with a second provider. Within the Cloud, an internal mechanism can be provided to add another layer of security. This includes generation of cryptographic keys for each customer.CSP should encrypt data, both at rest and in transit. It should harden the Virtual Machine so that exposure to attacks on virtualization layer is minimized. It should also provide virtual environments with a physical separation for cloud service users with special security requirements.

c) Data security can be further enhanced by implementing firewall to isolate confidential information. Sensitive information not essential to the business should be securely destroyed in a verifiable manner by the user and a secure network protocol should be used when connecting to a secured information store.

d) In general, organizations often cite the need for flexible Service Level Agreements (SLAs) that can be adapted to their specific situation, building on their experiences with strategic outsourcing and traditionally managed services. Hence, a comprehensive

management of security incidents/activities, business continuity and compliance with all security mandates and policy enforcements shall enhance security in Cloud environment. Establishment of 3rd party (External) audits for compliance shall also be required.

e) The mechanism for lodging complaints regarding security breach with the Cloud service provider by the user and the subsequent remedial and corrective measures taken thereupon shall be provided. All such complaints shall be logged and stored for a specified period of time for external audit.

4.8 Some of the other common attacks in today's cloud based services like DOS attacks, Theft of Service attacks, Cross Virtual Machine attacks are discussed in details in **Annexure-III.**

Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

Question 11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider(CSP); and (b) End users?

Chapter 5

Regulatory and Legal Framework for Cloud Computing

5.1. Cloud computing requires careful scrutiny by regulators because of its multi-dimensional nature. Current laws of many countries do not necessarily or specifically apply to cloud computing communications. The European Union (EU) has data protection laws, but they do not address concerns in cloud computing as they apply only to personal data. In USA, cloud computing has been formally defined by NIST. New Zealand had issued a cloud computing code of practice in June, 2012. The data protection laws in India are governed by Fundamental Right to Privacy under Article 21 of the constitution and Data protection covered under Section 43A of the IT Act read with the Rules, 2011.

A. Legal and regulatory concerns in Cloud Computing

5.2. Various legal and regulatory concerns in Cloud Computing environment are required to be identified and addressed, to create confidence in the consumers as well as in the cloud service providers. Any large establishments (like educational, health, banking etc) will not be able to move to cloud till the issues relating to legal, privacy and data protection in the context of cloud computing are addressed. Legal frameworks should be mandated for the concerns associated with cloud services as discussed below.

5.3. *Data Privacy and Data Protection*: The World Economic Forum has noted that 90% of suppliers and users of cloud services think risk to privacy is a "very serious" impediment to wide adoption of cloud services. The data and information uploaded onto the cloud by users is of a broad-based nature that is beyond the scope of "personal data" that is the subject of current data protection regulations world-wide. Currently, it may be difficult to determine if the cloud provider is

meeting data protection standards. This is especially true when the cloud services are being provided for free where it might be more difficult getting information on the security of the services. In the case of paid services, however, a user might be able to negotiate terms of the agreement to make sure the data will be properly protected. Further, data protection is dependent on the jurisdiction in which the service provider is located or the data is stored – the level of protection will be based on local laws or service provider's sole discretion if no laws, are available.

5.4. **Data Ownership:** The data ownership and rights rest with the customer (the originator of the data) irrespective of the location where the data is stored. Unless in cases, where the rights and ownership have been legally transferred to the CSP by the customer under the appropriate law. However, the terms and conditions of service offered by CSP may sometimes suggest some medium of ownership rights, even without legal transfer. This may lead to data security threats emerging from the possibility of misuse of data by CSP for marketing or data mining purposes.

a) *Lock-in:* Users have potential dependency on a particular service provider due to lack of well-established standards (protocols and data formats). Hence, it becomes vulnerable to migrations and service termination if there is no regulation or law to deal with them.

b) *Data Location:* Customer data held in multiple jurisdictions depending on geographical location are affected, directly or indirectly, by subpoena law-enforcement measures.

c) *e-Discovery:* As a result of law-enforcement measures, hardware might be confiscated for investigations relating to a particular customer, affecting the confidentiality of all other customers

whose data was stored in the same hardware. Data disclosure is critical in these cases.

5.5. **Multi- Jurisdiction Issues:** Any information stored in the cloud eventually ends up on a physical machine owned by a particular company or person located in a specific country. A cloud provider may, without notice to a user, move the user's information from one jurisdiction to another jurisdiction or even sub-contract the cloud services. The legal location of information placed in a cloud could be one or more places of business of the cloud provider; the location of the computer on which the information is stored; the location of a communication that transmits the information from user to provider and from provider to user; a location where the user has communicated or could communicate with the provider or possibly other locations.

5.6. **Disclosure and Cross-border movement of data**: The laws of user's country may restrict cross-border transfer/disclosure of certain information. Data on the cloud may be subject to third party/government access without user's knowledge. Data stored in another country may be more accessible to the government under local law.

5.7. In sync with the issue of privacy of data shared with the cloud is the matter of whether or not such information is permissible to be shared under the legislation of the user's country or transferred outside the country's borders. For example, in the United States (US) there are laws that restrict disclosure or sharing of certain information such as that concerning tax returns, health records etc. Questions such as what disclosure is and whether using the cloud to store information amounts to it being disclosed also arise in the process.

B. Current Legal Framework in India

5.8. As discussed earlier, dedicated cloud computing regulation or legislation is not available in many countries. There are, however, some laws relating to cloud services. However, application of old law to new technologies can be unpredictable or unsatisfactory. This has given rise to demand for enactment and formulation of specific laws or regulations in cloud computing. Various developments are taking place in this regard across the world. Details about some of the international legal frameworks are discussed in the **Annexure-IV**.

5.9. Although there is no specific right focused on personal data protection in India, there are several primary sources of Indian legislation that refer to this right for Indian citizens. The sources are discussed in subsequent paragraphs.

5.10. Under the **Indian Telegraph Act, 1885** 'telegraph' is "any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means". This definition could be construed to include cloud computing – the cloud is a means to send and receive data operating by way of a closed network or the Internet. Therefore, a cloud service provider would be seen as establishing, maintaining and working telegraphs for the purposes of the Telegraph Act, under a license to be issued by the licensor.

5.11. The **Civil Procedure Code 1908** bases the territorial jurisdiction on two principles. First being the place of residence of the defendant; the second the place where the cause of action arises. However, no clear guidelines have been provided as to how this would be determined, especially in cases involving cyber-crimes.

5.12. Similarly Cloud computing is also falling under the ambit of 'telecommunication service' under Section 2(k) of the **Telecom Regulatory Authority of India Act, 1997** which covers "service of any description" that is made available to users "by means of any transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, visual or other electromagnetic means".

5.13. **Information Technology Act of 2000:**The Information Technology Act of 2000 has explicitly stated penalties for the breach of data and privacy, at least in the domain of computers and cyber-crime. The Act is focused on e-commerce and cybercrime in general and data protection and data privacy are covered under it. Cloud computing and virtualisation service providers in India are required to comply with Internet Intermediary liability prescribed under this act.

5.14. Four sections namely sections 43, 65, 66 and 72, of the Information Technology Act specifically deal with penalties against breach and misuse of data in India. Section 43 protects the consumer from damages to the computer or the computer system. It foresees civil liability for actions including but not limited to unauthorized copying, extraction, database theft and digital profiling. Section 43A of the IT Act read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 protects sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall compensate the person so affected. It is pertinent to note that an obligation to maintain effective data protection measures is imposed.

5.15. A key component of Information Technology Rules, 2011 is that any organization processing personal information in India requires written consent before undertaking certain activities and must implement reasonable security policies and procedures. These rules apply to organizations operating in India and are independent of whether the data originates in India or if it pertains to Indian citizens. It also enforces a disclosure obligation for privacy policies wherein an organization must clearly explain the purposes of processing the involved personal information. These laws make Internet Intermediaries responsible for harmful content on the Internet.

5.16. Section 65 protects consumers against the tampering of computer source documents. It is applicable to intentional actions like concealing, destroying or altering of computer source code and is punishable by either or combination of a fine of up to two lakh rupees and imprisonment of up to three years.

5.17. Section 66 states that if any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Section 72 imposes a fine of one lakh rupees and an imprisonment term of up to two years for any breach of confidentiality and privacy of a person's material. Section 72A deals with punishment for disclosure of information in breach of lawful contract. It states that any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person

shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees.

5.18. The IT Act also provides for extra-territorial jurisdiction whereby the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality insofar as the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

5.19. Since the cross-border nature of cloud computing gives rise to instances of multiple jurisdictions, regulation may unilaterally impose Indian jurisdiction on issues arising from use of cloud services by Indian persons (along the lines of the wide-reaching jurisdiction conferred by the IT Act). Similarly, the usage of the cloud services by Indian person or provision of cloud services may be placed under a restriction that any and all Indian data on the cloud may be subject to Indian laws, thereby covering the issue of cloud being subject to the laws of the location of the server or service provider. Section 75 (2) of IT Act states that this Act shall apply in offence or contravention committed outside India by any person if the act or conduct constituting the offence involves a computer, computer system, computer network located in India. However, this provision does not look to offer a comprehensive solution.

5.20. The Government of India proposes to bring out legislation namely "The **Right to Privacy Bill**" which aims to provide for the 'right to privacy' to the citizens of India. It is said that intellectual property issues in the cloud continue to be one of the "cloudiest" legal areas for customers and suppliers alike because IPR and data protection laws vary from country to country. This makes the application of laws difficult since the question of jurisdiction creates confusion in the

cloud computing environment since there are plenty of different ways in which copyright-infringing content can be uploaded onto the cloud, given the vast number of services, which are provided, in the cloud. To deal with this problem, it needs to be ensured that every party involved is well aware of the regulations and the rights of the country in which the data/work is so stored and how potential infringements can be efficiently avoided.

C. Development of legal and Regulatory framework for Cloud Computing:

5.21. While the existing laws do cover some legal issues thrown up by cloud computing, they don't contemplate the scope of cloud computing services and the resultant magnification of the issues enlisted in section A. The consequence of this state of affairs is that the current laws may possibly not be able to facilitate cloud computing and there is a need for specific regulation whereby any emergent issues could be dealt with directly and effectively.

5.22. The regulations need to be evolved for cloud computing in India for Regulation of Investigatory Powers, Regulation on Stored Communication, Mandatory guidelines for National Security for cloud operation and Lawful interception and monitoring by Law Enforcement Agencies, State Privacy Laws and Fair Credit Reporting Act etc. A major regulatory parameter will be fostering and developing competitions in the cloud computing market.

5.23. Unduly onerous requirements should be carefully scrutinized from a cost-benefit perspective. A cooperative effort from all the stakeholders including technology industry, users of cloud services, service providers, bandwidth/connectivity providers and government is necessary to determine core cloud practices in order to provide greater

clarity and predictability for individuals, customers and cloud providers.

5.24. **Lawful Interception**: This is an extremely important aspect of any communication or information transfer as Lawful Interception by a Law Enforcement Agency (LEA) is an established and transparent method for letting Governments protects their boundaries, integrity and sovereignty in addition to national security. The Government will have to ensure a strict and vigilant interception system in cloud computing environment so as to meet the above requirements. With more and more happenings in the cloud – the previous methods of Lawful intercept are no longer valid and as such need new thinking as:

- Machines and data are no longer physically in one place or national boundary
- Encryption and security of data are far stronger and of industrial grade
- End companies have to sign deeper and more stringent End User Agreements with customers that previously never covered data (data was local and software manipulated it locally).

5.25. Following measures can be incorporated to channelize the legal framework in cloud computing-

a. *Customised agreements for data* - In the short term, cloud services customers and suppliers could seek to legitimise international transfers on the basis of an adapted version of the new model clauses. Compared to the new model clauses, the tailored data processing agreement should not reduce the contractual safeguards, should incorporate the same descriptions of transfers and detailed security measures. This would give room to customers and suppliers to carefully incorporate various clauses, which are contract specific and help them understand implications of breach by either party.

However, where there are clauses in such agreement that contradict with those mentioned in the Data Privacy Rules, the latter should prevail.

b. *Data Ownership Legal Framework:* The cloud service provider must safeguard the integrity of the data, as well as guarantee the client the ability to easily migrate its data and records to another hosting service, because of unsatisfactory performance. This should be done with complete deletion and destruction of data(data erasure) in the current cloud.

c. *Cross-Border movement legal framework:* Analysts and techno-legal experts have offered a solution that cyberspace must have its own set of jurisdictional rules thus extinguishing geographical borders.

d. *Binding Safe Processor Rules (BSPR)* - In the medium to longer term, suppliers can address their customers' concerns on the basis of BSPR which are a self-regulatory solution for data processors. BSPR are a global code of practice for the data processors' organisation based on EU privacy standards. They set out appropriate adequacy standards and can be tailored to the data protection practices of the cloud supplier. The standards are applied by the cloud supplier/processor to the customer/controller's data and are uniformly applied across the supplier's organisation. BSPR enable customers to easily comply with their data protection obligations and eliminate the need for model contracts.

e. *Multi-Jurisdiction Issue Legal Framework:* To overcome the problem of multiple jurisdictions one of the possibilities may be to mandate the cloud service providers to host the data centres only in India. Another alternative may be to impose restriction on cross border movement of some critical information like tax returns, financial transactions, health records etc.

f. *Adequate Penal Measures*- Where the law stipulates certain precautions to be taken by the ISP, vendor and intermediary with

respect to data storage, transfer and processing, it fails to enumerate any stringent penal action against those who violate these precautions. The punitive measures and especially the fines, defined are too meagre to ensure proper protection of data. Personal and sensitive data has to be maintained with utmost confidentiality; and the trust of the information provider must be safeguarded. Where highly sensitive data is being handled, the law may also suggest an imprisonment term (depending on the gravity of the crime) in addition to the fine prescribed. For repeated contravention, the licenses of service providers may be suspended or cancelled.

5.26. The Government could introduce some form of licensing or operational restrictions on intermediate service providers. Complying with new rules under the amended Information Technology Act, 2000 requires providers of sensitive information to verify the information which can become onerous given that data may be held in fragmented corners of the cloud. For this, the Laws need to be reviewed and new policies should be introduced to effectively and efficiently deal with matters involving confusion with respect to the basic and highly important issue of jurisdiction.

Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

Question 15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud

service providers so as to subject them to the obligations thereunder? Please comment with justification.

Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

Chapter 6

Implementation of Cloud Services in India

6.1. Cloud computing is becoming one of the significant and important areas for investment in India[20]. IT/ITes, Telecommunication, Banking and Financial Services, Manufacturing and Government sector are contributing largely to the Cloud market in India. Increased government expenditure on National Optical Fibre Network (NOFN) and various e-governance portals, coupled with new governmental programmes like Digital India is expected to drive the market for cloud computing. Overall ranked 8th, in the world, India's cloud services market has generated interest among the technology leaders and optimistic predictions for the future.[21]

6.2. Indian government recently launched an innovative initiative called the Smart Cities Mission that enables local development by harnessing technology for creating smart outcomes. Government of India has recognized the importance of cloud-based service-delivery platforms for establishing the foundation of Digital India, as it integrates smart devices and infrastructure and processes data from the large amount of scattered sources in real time.

6.3. On 1st October 2015, Microsoft announced the opening of three data centres in India which would primarily drive adoption of public cloud services by government departments, state-owned agencies, banks and financial institutions. Microsoft now accounts for 30% share in public cloud market in India.

[20]India in the Cloud Computing Arena, Downloaded Cloud Computing, June 16 2011, available at http://goo.gl/4USqy.

[21] A Framework and Roadmap for Cloud Computing Innovation in India, white paper 2.0, December 2014 by IEEE India-Cloud Computing Innovation Council of India

6.4. Cloud accounted for nearly 30 per cent of the overall spending[22] on IT infrastructure in the January-March 2015 period, up from 26.4 per cent a year ago. Sales for public cloud grew from $ 0.2 in 2011 to $0.9 in 2015 (figure 6.1) and $0.7 to $3.6 over same period for private cloud deployments.Cloud services revenue is projected to have a five-year projected CAGR of 33.2 percent from 2012 to 2017 across all segments of the cloud computing market. Segments such as software as a service (SaaS) and infrastructure as a service (IaaS) have even higher projected CAGR growth rates of 34.4 per cent and 39.8%.More such information regarding current year statistics of cloud computing as well as market predictions pertaining to Cloud computing adoption in India is detailed in para 2.2 in chapter 2.

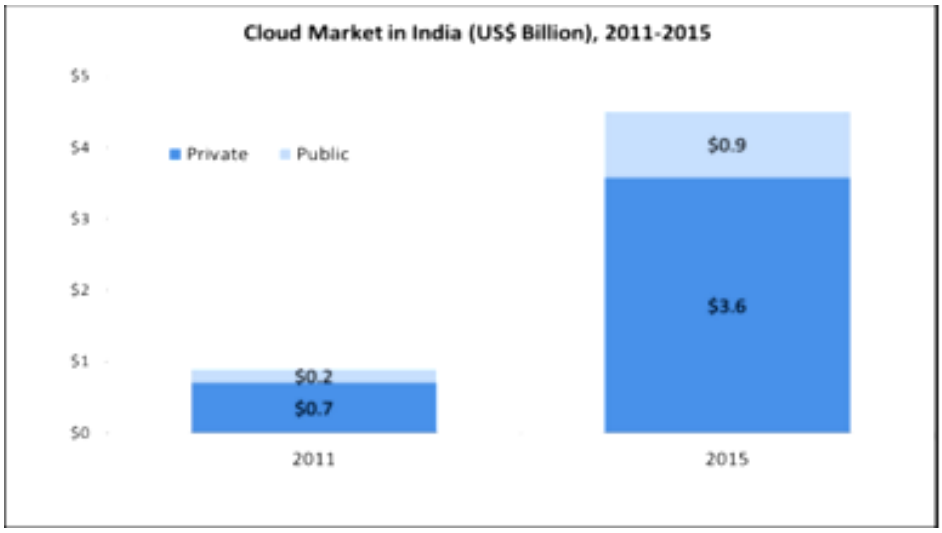

Figure 6.1: Public and Private Cloud Market in India[23]

6.5. As clear from the above statistics, a full-fledged use of public cloud needs to be developed reaping the advantages that public cloud deployment offers. Well defined regulations can ensure the objectivity required for certifications to handle data security, privacy and sovereignty.

[22]Research firm IDC

[23] A Framework and Roadmap for Cloud Computing Innovation in India, white paper 2.0, December 2014 by IEEE India-Cloud Computing Innovation Council of India

A. Barriers for adoption of Cloud Computing in India

6.6. While Indian firms and organisations are well poised for notable successes in adopting cloud computing, there are factors that pose long-term challenges to India's competitiveness in cloud services provision, and IT services more broadly.

6.7. One of the biggest challenges that cloud computing in India is facing is the lack of dependable infrastructure for data centres. For Cloud computing to be successful in India, the basic data centre grade physical infrastructure i.e. Connectivity, Power and Cooling should be consistent.

6.8. The World Economic Forum ranked India as 111th out of 148 countries for the availability of international Internet bandwidth, a measure of the amount of Internet traffic that can be exchanged between countries.[24] Various other rankings and indicators focused on Internet penetration, cloud readiness, and other factors confirm a sub-optimal state of affairs which, combined with ongoing shortfalls in the steady electricity supply needed for data centre operations, are likely to continue to put some limits on cloud growth in India.

6.9. The main problem India faces in this field are broadly classified as follows[25]:

1. *Unreliable power supply*: A stable power supply is the basic need of Cloud computing, a single power cut may mean a huge system crash. The main challenge is to secure affordable and reliable sources of energy. The data centres which store and process data for cloud

[24] http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf

[25] The challenges and offerings of Cloud Computing with the needs of Indian Economic System by Prem Parashar, Pratiksha Haldar, Shradha Salaria and Survey conducted by NASSCOM "India as a hub for delivering and adopting Cloud Services"

activities use great amounts of energy, but electricity is expensive, scarce and unreliable. While firms have often relied on private sources of power such as generators to ensure that their needs are met, the growth of data centres could ultimately be constrained by the weak electricity infrastructure.

2. *Bandwidth availability and network stability*: The companies need sufficient bandwidth to deliver intensive and complex data over the network. There is a lack of reliable connectivity in B and C category Indian cities so they have variable broadband and low penetration degrees. 'A' category cities have a better network infrastructure but the prices for bandwidth are high.
3. *Scepticism on company's side*: regarding market competition as well as security, standards and regulations: The costs of hosting cloud services for a CSP in India are way more than hosting them abroad. But the idea of keeping confidential national information in data centres located abroad raises security concerns.
4. *Service Delivery and Billing*: It is hard to assess the costs involved due to the on-demand nature of the services. Budgeting and assessing the cost will be very difficult unless the provider has some good and comparable benchmarks to offer.
5. *Interoperability and portability*: Organization should have the leverage of migrating in and out of the cloud switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.
6. *Road Infrastructure*: Although the aim is to build a cloud setup that mainly includes computer hardware and network connectivity, to build such a structure, the basic infrastructure like good roads connectivity and communication line coverage is an essential.

6.10. Citing the need to monitor domestic Internet traffic for national security reasons, concerns over foreign surveillance, and a desire to ensure that data is subject to local laws, the Indian government has for years supported the idea of foreign firms storing data within the country. One clear example of the push for data localization is found in the Department of Telecommunications' "National Telecom M2M Roadmap" (referring to machine-to-machine data transmission of the sort expected to increase substantially as Internet connected devices become more common), in January 2015.[26] The guidelines call for "all M2M gateways and application servers" used in providing services to individuals in India to be physically located within the country, based on national security concerns. Although cloud vendors would not be the explicit focus of this provision, its inclusion points to the acceptance of data localization policies among some in the Indian government.

6.11. Some of the other prime concerns associated with adoption of cloud services in India[27]:-

- *Energy Resource Management:* The lack of indigenous manufacturing base increases the fixed carbon footprint of IT equipment deployed in our data centres on account of the increased logistics footprint. In addition, limited availability of cross-platform monitoring tools leads to a higher proportion of underutilized resources.Significant saving in the energy consumptions of a cloud data centre without sacrificing SLA can make a significant contribution to greater environmental sustainability. It has been estimated that the cost of powering and cooling accounts for 53% of the total operational expenditure of

[26]http://www.dot.gov.in/sites/default/files/Draft%20National%20Telecom%20M2M%20Roadmap.pdf

[27]Cloud Computing: Security Issues and Research Challenges, Rabi Prasad Padhyet. Al., IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 1, No. 2, December 2011

data centres. The goal is not only to cut down energy cost in data centres, but also to meet government regulations and environmental standards. Designing energy efficient data centres has recently received considerable attention in India. Energy efficient hardware architecture that enables slowing down CPU speeds and turning off partial hardware components has become commonplace. Energy aware job scheduling and server consolidation are two other ways widely used in the country to reduce power consumption by turning off unused machines.

- *Server consolidation:* Server consolidation is an effective approach to maximize resource utilization while minimizing energy consumption in a cloud computing environment. Live VM migration technology is often used to consolidate VMs residing on multiple underutilized servers onto a single server, so that the remaining servers can be set to an energy-saving state. However, server consolidation activities should not hurt application performance. The resource usage (also known as the footprint) of individual VMs may vary over time. For server resources that are shared among VMs, such as bandwidth, memory cache and disk I/O, maximally consolidating a server may result in resource congestion when a VM changes its footprint on the server. Hence, it is sometimes important to observe the fluctuations of VM footprints and use this information for effective server consolidation. Finally, the system must quickly react to resource congestions when they occur.
- *Platform Management:* This includes challenges in delivering middleware capabilities for building, deploying, integrating and managing applications in a multi-tenant, elastic and scalable environments. One of the most important aspects of cloud platforms is to provide capabilities to developers to write applications that run in the cloud, or use services provided from the cloud, or both. Different names are used for this kind of platform today, including on-demand platform and platform as a

service (PaaS). This new way of supporting applications has great potential but semantics and interface portability becomes serious concern.

B. Building infrastructure, capabilities, strategies and initiatives

6.12. Government of India has two prominent roles of promoting cloud computing and cloud based services in the country as well as leverage the advantages offered by cloud services as a user to implement Government programmes and services.

6.13. The Government has introduced policies and regulatory measures for renewable energy development, such as financial incentives, capital subsidy and lower customs duties. The Government has imposed preferential tariff for renewable power in strategic areas. Further, government efforts include generation-based incentive scheme for wind power, which prescribes incentive for electricity fed into the grid. Such measures would lead to ensuring stable power supplies to cloud computing data centres which are essentially indispensable.

6.14. Despite low adoption levels as compared to US, Europe or Japan, there is significant interest among agencies of India and the Department of Information Technology to promote cloud computing across the country. Department of Telecommunications, Government of India has issued National Telecom Policy-2012 with Cloud Computing adoption as one of its key strategies. The Telecom Engineering Centre (TEC) has also framed a Generic Requirements (GR) document for Cloud infrastructure in October, 2012. This increasing traction is expected to result in increasing adoption in the near future, as governments/agencies look to adopt private cloud to reduce ICT spending and increasing efficiency.

6.15. There is an accelerated requirement to incubate innovation in the cloud infrastructure space in order to make India the next generation international powerhouse destination in the cloud services including e-Health, e-Education and e-Governance. The Government can apply the Cloud through Government-to-Government (G2G), Government-to-Business (G2B), Government-to-Citizen (G2C) and Government-to-Employee (G2E) models as shown in figure 6.2 below:

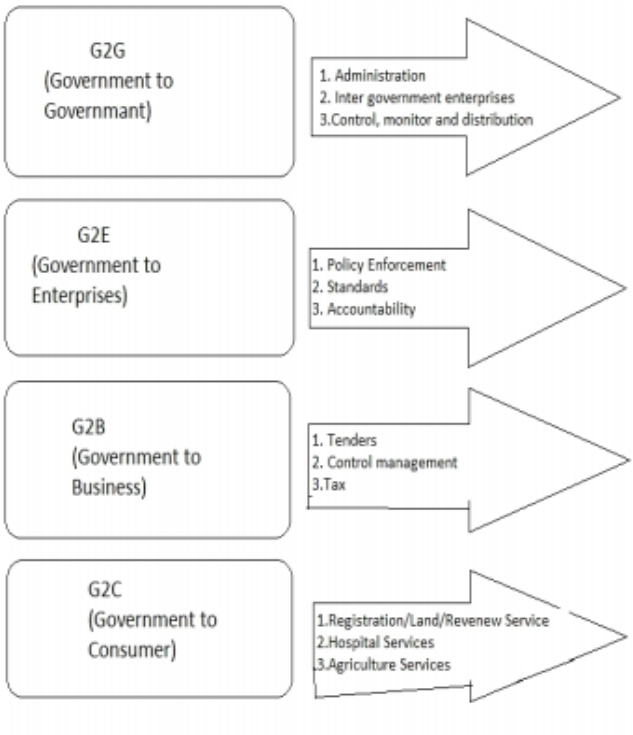

Figure 6.2: Types of e-Governance

6.16. By adopting Cloud computing, government agencies can create a central pool of shared resources including software and infrastructure. The value proposition for Cloud Computing in the public sector is shown in the figure 6.3 given below:

Reduction in ICT Spending	By adopting cloud computing, government agencies can create a central pool of shared resources – software and infrastructure. The consolidation of resources and the fact that cloud computing is more cost effective, leads to reduction in ICT spending.
Agility	Governments operate in a strict hierarchical manner and the process for approvals and purchase orders is a time consuming activity. Cloud computing provides the capability to eliminate these time consuming activities and provision resources on the fly.
Access to Most Updated Technology	Cloud computing offers the government the ability to constantly have access to the most updated software and hardware. The onus of upgrading technology is on the service provider in this delivery model who ensures access to the most up-to-date solutions.
Elimination of Procurement & Maintenance	Another key advantage is the elimination for the need to procure, monitor, and maintain IT resources. This too is the responsibility of the service provider under the delivery model. Apart from reducing the workload, this reduces the need for IT staff and allows the government/agencies to focus on their core areas of work.
Universal Resource Access	Cloud computing is delivered through the Internet enabling universal access to resources. Furthermore, it helps the government in establishing a common platform for all its eGovenance initiatives, one that is easily accessible by the citizens as well.

Figure 6.3: Value proposition of Cloud computing in the public sector[28]

6.17. The several initiatives of Government of India in the Cloud Computing sector are placed at **Annexure-V**

C. Investments for boosting Cloud Services in India

6.18. Government is playing a key role in making cloud service globally competitive and make India an attractive destination for foreign investments in the area. Indian service providers are investing in creating new service offerings in all the areas of cloud, infrastructure, people, partners and data warehouses to support their cloud services and also building on its strengths. India is well positioned to leverage the current investments of market participants because of the large presence of Multi-National Companies (MNCs) and a strong network infrastructure to establish a dominant position in the global cloud computing market. However, a proper structured framework is required to be devised and put in place for promoting cloud computing and to take advantage of India's leveraged position. A proper legal and regulatory framework and favourable tax structure is also required to support and facilitate cloud computing deployment.

[28]Frost & Sullivan-2011

6.19. Recognizing the potential of Cloud Computing, the Indian Government may ensure that researchers and firms contribute to the framework of the cloud. The government may invest heavily in the development of cloud standards and there should be a focus on developing indigenous hardware and software to enable the cloud. Further, investments in research and data centres may be made by State Governments and corporations.

D. Taxation Issues of Cloud Services and Incentives for Growth

6.20. A major challenge in the taxation of cloud offerings is in the tax classification of cloud services themselves. It is to be considered as to what tax regime should be employed for cloud service providers in India and whether tax benefits shall be given to them, for promoting adoption of cloud services in the country.

6.21. Some countries are incentivising to promote cloud services. In Singapore through the inclusion of related costs under the Productivity and Innovation Credit (PIC) scheme, cloud service providers are able to obtain significant tax benefits for cloud computing. Singaporean businesses, including small- and medium-sized enterprises, can claim for their cloud computing expenditure, within certain categories such as the acquisition or leasing of technological equipment, training expenditure, the acquisition and registration of intellectual property rights, actual costs of research and development, and costs incurred in the creation of new products and industrial designs. The Info-communications Development Authority (IDA) of Singapore has been offering subsidies in the range of 50 to 100 percent to boost industry participation in Cloud.

6.22. In some other countries, cloud services are often provided via a network of local data centres, where they offer constantly changing special tax and other cash incentives. Some countries offer abatements or holidays for sales tax or Value Added Tax (VAT) or even

reduced rates of overall income taxation based on profits derived from such cloud computing activities.

6.23. In India, such various incentives exist for specific industries such as power, ports, highways, electronics and software or incentives for units in less-developed regions or incentives for units producing exports or in export processing zones and SEZs. Such Incentives include: Weighted deductions at 200%[29] for in-house research and development (R&D) expenses, including capital outlays (other than those for land) in the year incurred. Software companies are currently granted a tax holiday on income generated, under Sections 10A and 10B of Indian tax laws, out of Software Technology Park of India (STPIs) — a concession that brings down the effective tax rates to 12-15 per cent, compared with the peak effective corporate tax of 33 per cent.Similar incentives could also be extended to the cloud service providers to enhance these services.

6.24. The cloud enablement framework in India therefore needs to strike a fair balance in several areas[30]:

- *Public versus private sector:* In the interest of the public the government may find a need for formulating strict privacy laws defining vendor liabilities and sovereign reach irrespective of server location; however, seeing vendor as a mere carrier of services may dilute the law.
- *Innovation and growth versus standardization:* Cloud Computing is enabling innovation in new business models in dramatically new and faster ways. But facilitating interoperability through

[29]https://www2.deloitte.com/content/dam/Deloitte/in/Documents/tax/in-tax-india-guide-2015-noexp.pdf

[30] A Framework and Roadmap for Cloud Computing Innovation in India, white paper 2.0, December 2014 by IEEE India-Cloud Computing Innovation Council of India

standardization is also crucial to the overall growth and evolution of the cloud ecosystem.

- *Experimentation versus stability*: A range of new cloud offerings have made their foray and have been subject to change from time to time. The freedom to experiment with technologies is necessary for fostering innovation. But standardized offerings may be helpful in addressing interoperability concerns and stability of applications. Interoperability Framework for E-Governance (IFEG) in India addresses three aspects of Interoperability such as Organizational Interoperability, Semantic Interoperability, and Technical Interoperability. Each aspect of interoperability has detailed standards for each applicable area.
- *Formal versus informal:* For instance, in terms of adopting a set of standards, there can be a general consensual approach among the cloud players for standards to be set according to a given industry that is being catered to. On the other hand, an independent body may be involved in setting the standards with involvement of multiple stakeholders.
- *Political inclusion versus technical competence:* While including stakeholders, a clear conflict will be in terms of whether technical competence or political inclusion should be the criteria and who gets to influence more. Striking a balance or finding the golden mean in terms of addressing the concerns of multiple stakeholders of cloud ecosystem is going to be a challenge.
- *Restrictive versus permissive rules:* Often regulations related to data security and privacy across nations are inconsistent and therefore cause major concerns to users as well as providers. When effective regulations restrict the movement of data across borders or force the data to remain within national borders due to absence of cross jurisdictional alignment, the providers lose out on advantages such as improvements through scale offered by collating data in multiple locations. Restrictions and requirements that are industry-specific

and issued in the pre-Internet times need to be reframed to deal with new challenges posed by ubiquitous mobile technologies.

- *Centralized versus decentralized design and governance approaches:* The traditional hierarchical governance processes may be bypassed due to direct information exchanges in the network of end users enabled by the design of cloud services and products. A multi-stakeholder approach to governance is needed to deal with such newer forms of privacy and security breaches.

6.25. Apart from the above considerations, efforts could be made to set up cloud services in the south Asian region. The South Asian Association for Regional Cooperation (SAARC) countries could foster initiatives to facilitate cloud services in the region. Driven by its potential to bring about substantial cost savings, and increase the flexibility and efficiency of business, cloud computing is generating immense interest among enterprises as one of the most effective tools to boost their bottom line. India is already the world's leading exporter of computer and information services. Indian businesses, primarily those operating in the telecom, Banking & Financial Services (BFSI), insurance, education, and governance sectors are beginning to test the waters around cloud computing that promises them access to convenient, on-demand network by a shared pool of computing resources placed in scalable data centres. Some of the Cloud adoption models by Governments in Asia Pacific are discussed in **Annexure-VI**.

Question 18. What are the steps that can be taken by the government for:

(a) promoting cloud computing in e-governance projects.

(b) promoting establishment of data centres in India.

(c) encouraging business and private organizations utilize cloud services

(d) to boost Digital India and Smart Cities incentive using cloud.

Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

Question 20. What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centres and cloud services platforms in India?

Chapter 7

Issues for consultation

Question 1. What are the paradigms of cost benefit analysis especially in terms of:

a. **accelerating the design and roll out of services**
b. **Promotion of social networking, participative governance and e-commerce.**
c. **Expansion of new services.**
d. **Any other items or technologies. Please support your views with relevant data.**

Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organisation?

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

Question 4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for

different service models? The parameters essential and desirable and their respective benchmarks may be suggested.

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

Question 9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.

Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

Question 11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider(CSP); and (b) End users?

Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

Question 15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud

service providers so as to subject them to the obligations thereunder? Please comment with justification.

Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

Question 18. What are the steps that can be taken by the government for:

(a) promoting cloud computing in e-governance projects.

(b) promoting establishment of data centres in India.

(c) encouraging business and private organizations utilize cloud services

(d) to boost Digital India and Smart Cities incentive using cloud.

Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

Question 20. What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centres and cloud services platforms in India?

Annexure-I

Cloud Computing Reference Architecture

1. Issues to Clarify Before Adopting Cloud Computing

Gartner, Inc., the world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers before adopting[31]:

- *User Access:* Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major companies should demand and enforce their own hiring criteria for personnel that will operate their cloud computing environments.

- Regulatory *Compliance:* Make sure your provider is willing to submit to external audits and security certifications.

- *Data location:* Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those jurisdictions.

- *Data Segregation:* Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.

- *Disaster Recovery Verification:* Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.

- *Disaster Recovery:* Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.

- *Long-term Viability:* Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

[31] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011, " AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING", Anthony Bisong and Syed (Shawon) M. Rahman.

2. Cloud Computing Reference Architecture[32]: Cloud computing, located at a central place can be accessed by a cloud transport network that is connected to any form of access network e.g. 4G long term Evolution (LTE), 3G, wired etc. Access to cloud computing resources can be provided by any kind of device and for any kind of service. As per the Oracle's White paper on CRA, November 2012, the following list contains essential yet non exhaustive set of cloud architecture principles:

- Cloud interfaces and formats must conform to relevant industry standards.
- The system must present only the information (interfaces etc.) necessary to perform each specific function.
- The architecture should provide monitoring of all aspects of resource usage for the various dimensions required by both the Cloud consumer and provider.
- Any Cloud provider's claims of Reliability, Availability, Security, and Performance must be verifiable.
- Availability should not be limited by inevitable hardware failures.
- Robust Identity Domain Separation – consumers of the system have no exposure to the consequences of other consumers' use of the system.
- Transparent Architecture and Control – consumers have visibility into the design and operation of the system.
- Improved Productivity - deliver an order of magnitude improvement over current levels of efficiency and productivity experienced in traditional IT environments.
- Assured Data Protection – consumers are assured of compliance with data privacy standards and regulations, have confidence that removal of data is absolute.

[32] Cloud Computing Reference Architecture (CCRA) 4.0 Overview by IBM

- Automate Operations – consumers' runtime of business process services and platform services involves minimal manual operations.

The cloud computing reference architecture is depicted in figure 1 given below:

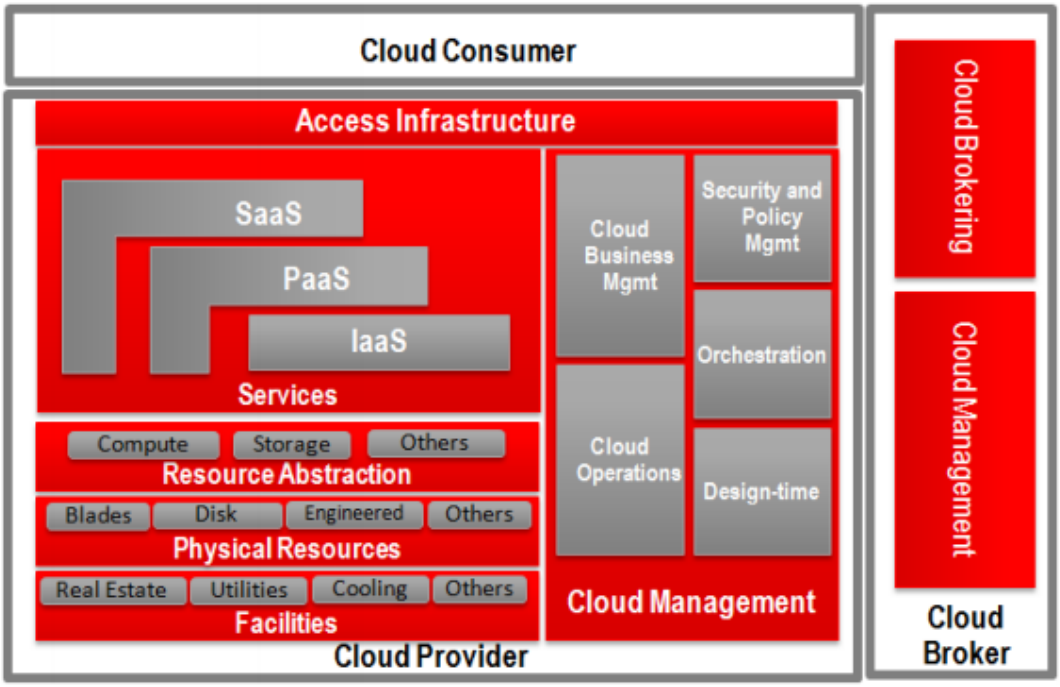

Figure 1: Cloud Architecture[33]

Different parts of the architecture are:

(a) Intra-cloud network*:* This network is to connect local cloud infrastructures, such as data centre LAN used to connect servers, storage arrays and services such as firewalls, load balancers, application acceleration devices, IDS/IPS etc.

(b) Core transport network: This is the network used by customers to access and consume cloud services deployed within the cloud provider's data centre.

(c) Inter cloud network: This network's role is to interconnect cloud infrastructures together. These cloud infrastructures may be owned by the same cloud provider or by different ones.

[33] Cloud Reference Architecture, An Oracle white paper, November 2012

(d) Global Management Centre: This can be used to manage different cloud networks. The communication is to OSS located in each network.

3. Trusted Cloud Initiative (TCI) Architecture: Latest development of architecture was done by CSA that developed TCI reference architecture model. The architecture defines different organization levels by combining frameworks like the SPI model, ISO 27002, COBIT, PCI, SOX and architectures such as SABSA, TOGAF, ITIL and Jericho. A wide range of aspects are then covered: SABSA defines business operation support services, such as compliance, data governance, operational risk management, human resources security, security monitoring services, legal services and internal investigations; TOGAF defines the types of services covered (presentation, application, information and infrastructure; ITIL is used for information technology operation and support, from IT operation to service delivery, support and management of incidents, changes and resources; finally, Jericho covers security and risk management, including information security management, authorization, threat and vulnerability management, policies and standards. The result is a tri-dimensional relationship between cloud delivery, trust and operation that aims to be easily consumed and applied in a security-oriented design.

4. Cloud Computing Architecture Terminologies

A Cloud computing architecture comprising of a quality of service system for supporting market-oriented resource allocation is given in figure 2. Various generic requirements for a QoS system are listed below:

- It should support service differentiation for different categories of consumers.
- It must support the grouping of interactions in sessions.
- Modifications in the system software of the servers shall not be required.
- It should be easy to configure.
- It must be scalable to operate in both a single server and a cluster of servers.

- It should provide protection against overloads and low utilization.
- It should support dynamic negotiation of parameters.

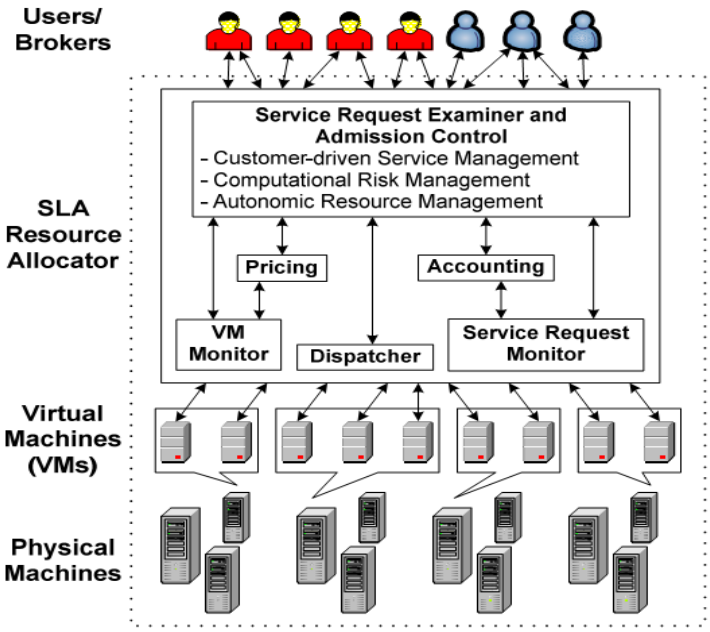

Figure 2: Cloud Computing Architecture[34]

Users/Brokers: They submit their service requests from anywhere in the world to the cloud.

SLA Resource Allocator: It is a kind of Interface between users and cloud service provider which enable the SLA-oriented resource management.

- **Service Request Examiner and Admission Control**: It interprets the submitted request for QoS requirements before determining whether to accept or reject the request based on resource availability in the cloud and other parameters.

- **Pricing**: It is in charge of billing based on the resource utilization and some other factors based on SLA like request time, type etc.

- **Accounting**: It maintains the actual usage of resources by request so that the final cost can be charged to the users. In addition, the

[34]"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", RajkumarBuyyaet. al., Future Generation Computer Systems 25 (2009) 599616, Elsevier Journal

maintained historical usage information can be utilized by the Service Request Examiner and Admission Control mechanism to improve resource allocation decisions.

- **Hypervisor:** In computing, a hypervisor also called as virtual machine manager (VMM) is one of the many hardware virtualization techniques allowing multiple operating systems, termed guests, to run concurrently on a host computer.

- **Dispatcher**: The dispatcher mechanism starts the execution of admitted requests on allocated VMs.

- **Service Request Monitor**: The request monitor mechanism keeps track on execution of request in order to be in tune with SLA.

Virtual Machines (**VMs)**: Multiple VMs can be started and stopped dynamically on a single physical machine to meet accepted service requests, hence providing maximum flexibility to configure various partitions of resources on the same physical machine to different specific requirements of service requests. In addition, multiple VMs can concurrently run applications based on different operating system environments on a single physical machine since every VM is completely isolated from one another on the same physical machine. *System Virtual Machine* provides a complete system platform which supports the execution of a complete operating system while *Process Virtual Machine* is designed to run a single program, which means that it supports a single process.

Physical Machines: The Data Centre comprises multiple computing servers that provide resources to meet service demands. The cloud service provider (CSP) should be able to provide a SLA measuring tool to the client so that the parameter agreed upon between the client and the CSP can be monitored by the client using the SLA tool.

Annexure-II

International cloud standards

1. Approaches for Cloud interoperability

Different approaches are being used by the industry for interoperability in cloud. Some of the prominent approaches are described below.

Approach 1: Unified Cloud Interface or Cloud Broker: Cloud Computing Interoperability Forum (CCIF) is planning to come up with a unified cloud interface (cloud broker) whose features are as follows:

Unification of various cloud APIs and abstract it behind an open and standardized cloud interface. Thus a key driver of the unified cloud interface (UCI) is to create an API about other APIs. It is a singular abstraction/programmatic point of contact that encompasses the entire infrastructure stack as well as emerging cloud centric technologies through a unified interface. UCI model is depicted in figure 1 below

- This model suggests the usage of semantic web and OWL.
- The purpose of cloud broker is to serve as a common interface for the interaction between remote platforms, networks, systems, applications, services, identity and data.

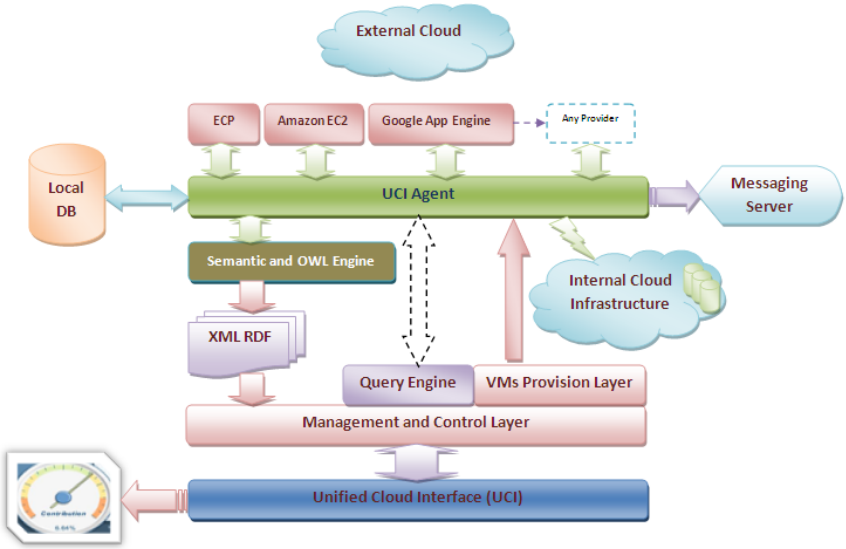

Figure 1: UCI Architecture[35]

[35]Unified Cloud, Available at http://code.google.com/p/unifiedcloud/wiki/UCI_Architecture

- Having a common set of cloud definitions is an important factor that would enable vendors to exchange management information between distant cloud providers.
- The important parts of unified cloud interface (UCI) or cloud broker are a specification and a schema. The actual model descriptions are provided by the schema and the details for integration with other management models are defined by the specification.
- The unified cloud model will address both the platforms as service offerings as well as infrastructure cloud platforms. It will enable a hybrid cloud computing environment that is decentralized, extensible and secure.

Approach 2: Enterprise Cloud Orchestration Platform /Orchestration layer approach: The features of the Orchestration layer approach are explained below:

- Different cloud service providers can register the cloud services that they offer with the orchestration layer. This is similar to vendors who offer web services publishing their web services with the Universal Description, Discovery and Integration (UDDI). The orchestration layer can then dynamically select and bind to services based on criteria/algorithms that determine the best cloud service for a particular job based on factors like highest performance, lowest cost or other requirement as specified by the client.

- Since the orchestration layer interacts with the cloud services offered by different vendors via different APIs, it can use user-computer interface (UCI) for interacting with different Cloud Service Providers (CSP) or have similar functionality built-in to be able to understand and interact with different CSPs via different APIs.

- The client uses only one single API offered by the orchestration layer and thus is insulated from the different APIs offered by different CSPs.

  Figure 2 shows an example of how a client's request for executing a business process (or workflow) is satisfied by the orchestration layer

by invoking a sequence of three different services provided by three different CSPs.

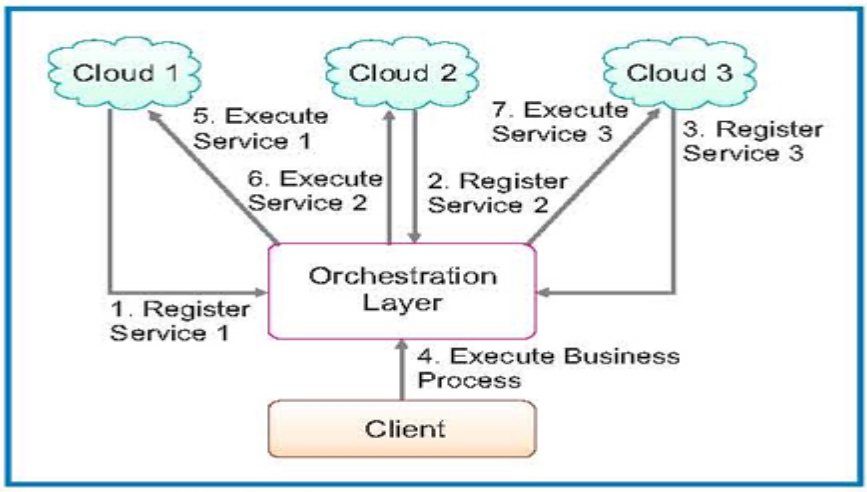

Figure 2: Cloud Orchestration[36]

Approach 3: The Open Cloud Computing Interface (OCCI) by Open Grid Forum (OGF): The OCCI effort is focused mostly on IaaS, creating interoperability bridges between providers.

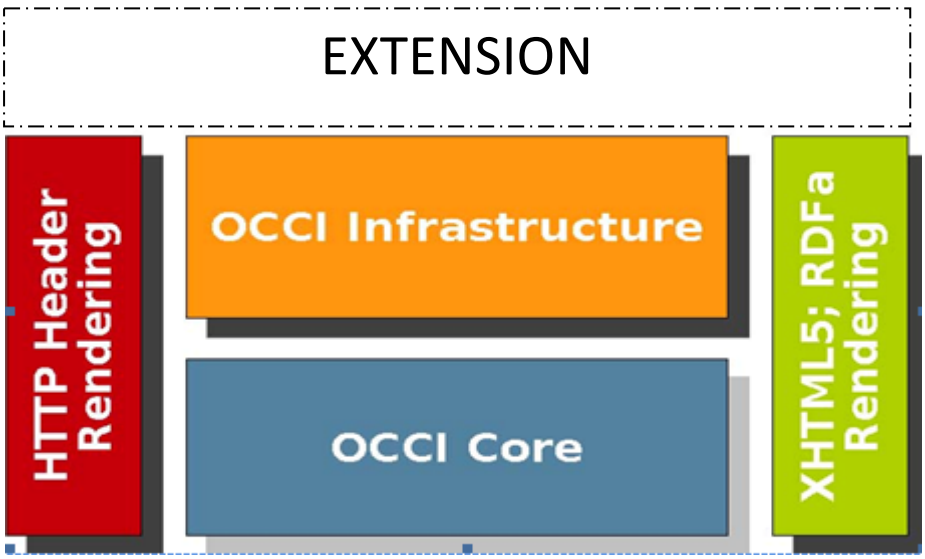

Figure 3: OCCI Model- view

[36]Infosys Research

The OCCI model uses a very flexible API for Service Management (IaaS and more) and consists of 3 parts (i) Core – which defines the OCCI model, (ii) Rendering –which defines rendering using text/plain or text/OCCI and (iii) Infrastructure – which defines IaaS resource parameters of compute, storage and network. It is easily extendible by linking to new or external objects and services and by adding new attributes to existing objects. Figure 3 above depicts the details of OCCI.

2. ITU-T Initiatives for Cloud Interoperability:

The structure of ITU working groups (WG) and work areas for cloud computing are given below:

WG1: Cloud computing benefits & requirements

- WA 1-1 Cloud Definition, Ecosystem & Taxonomy
- WA 1-2 Uses cases Requirements & Architecture
- WA 1-3 Cloud security
- WA 1-4 Infrastructure & Network enabled Cloud
- WA 1-5 Cloud Services & Resource Management, Platforms and Middleware
- WA 1-6 Cloud computing benefits & first Requirements from ICT perspectives

WG 2: Gap Analysis and Roadmap on Cloud Computing Standards development in ITU-T

- WA 2-1 Overview of cloud computing SDOs activities
- WA 2-2 Gap analysis & Action plan for development of relevant ITU-T Cloud Standard

The Focus Group will have seven output documents delivered namely:

- Overview of Standards Development Organizations involved in Cloud Computing
- Introduction to the Cloud Ecosystem
- Benefits of Cloud Computing from Telecom/ICT Perspectives

- Cloud Security, Threat & Requirements
- Functional Requirements and Reference Architecture
- Infrastructure and Network Enabled Cloud
- Cloud Resources Management Gap Analysis

3. Standards for Cloud Computing:

To date, most of the focus for cloud interoperability and portability standards has been at the IaaS layer although activity at the PaaS level is starting to accelerate. In addition, there are several security standards that enable and facilitate cloud computing interoperability even though they are not exclusive to cloud computing. Cloud computing customers should determine the level of support for the following standards by prospective cloud service providers. Lack of support for these standards is likely to result in interoperability and portability challenges down the road.

- Open Virtualization Format (OVF): A packaging standard developed by the Distributed Management Task Force (DMTF) that is designed to address the portability and deployment of virtual machines.
- Cloud Data Management Interface (CDMI): A standard defined by the Storage Networking Industry Association (SNIA) that defines the functional interface that applications will use to create, retrieve, update and delete data elements from the cloud.
- Open Cloud Computing Interface (OCCI): A set of open specifications delivered through the Open Grid Forum that defines a protocol and API for all kinds of cloud computing management tasks.
- Topology and Orchestration Specification for Cloud Applications (TOSCA): A standard developed by OASIS that enables the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behavior of these services (e.g., deploy, patch, shutdown).

- Cloud Application Management for Platforms (CAMP): A standard developed by OASIS that defines an interoperable protocol that cloud implementers can use to package and deploy their applications.
- Cloud Auditing Data Federation (CADF): A standards developed by DMTF that defines open standards for cloud auditing.
- LDAP, OAuth, OpenID Connect and SAML: Standards that enable third party ID and Access Management functionality.
- US FIPS 140-2: Standard that specifies the security requirements to be satisfied by a cryptographic module utilized within a security system protecting sensitive information.

Annexure-III

Common attacks in cloud based services

1. Security attacks in Cloud Computing

The following attacks are of immense concern in today's cloud based services. Few countermeasures were also discussed in Chapter 4.

a) **Theft of Service attack[37]:** The Theft of Service attack utilizes vulnerabilities in the scheduler of some hypervisors. The attack is realized when the hypervisor uses a scheduling mechanism, which fails to detect and account of Central Processing Unit (CPU) usage by poorly behaved virtual machines (VM). This failure may further allow malicious customers to obtain cloud services at the expense of others. This attack is more relevant in the public cloud where customers are charged by the amount of time their VM is running rather than by the amount of CPU time used.

   A countermeasure to this attack can be by modifying the scheduler to prevent the attack without sacrificing efficiency, fairness or I/O responsiveness. Another countermeasure can be to use new instance of cloud-to-user surface in victim machine to monitor the scheduling of parallel instances. Then, the outputs of both the attacker and the legitimate instances are compared. A significant difference in results is reported to the responsible authorities as an attack.

b) **Denial of Service attack:** Most of the serious attacks in cloud computing come from denial of service (DoS), particularly HTTP, XML and Representational State Transfer (REST)-based DoS attacks. The cloud users initiate requests in XML, then send requests over HTTP protocol and usually build their system-interface through REST protocols such as those used in Microsoft Azure and Amazon EC2. Due to vulnerabilities in the system interface, DoS attacks are easier to implement and very difficult for security experts to countermeasure.

[37] Cloud Computing Security: A Survey, Issa M. Khalil et. al., www.mdpi.com/journal/computers

c) **Malware Injection attack:** Cloud malware injection attack refers to a manipulated copy of the victim's service instance, uploaded by attacker to cloud, so that some service requests to the victim's service are processed within that malicious instance. The incidents of this attack include credential information leakage, user private-data leakage and unauthorized access to cloud resources. The challenge does not only lie in the failure to detect the malware injection attack but also in the inability to determine the particular node on which the attacker has uploaded the malicious instance. Retrospective detection (examination of hard-drive and memory) has been a widely used technique to detect the host of malware instances. Some researchers recently developed new retrospective detection approach based on portable executable (PE) format file relationship. This approach has been implemented and validated in HADOOP platform and has proved higher detection rate

d) **Cross VM Side Channel attack:** VM side channel attack is an access-driven attack in which an attacker VM alternates execution with the victim VM and leverages the processor cashes to infer the behaviour of the victim. It requires that the attacker resides on a different VM on the same physical hardware as that of the victim's VM. Instead of directly attacking the software stack (virtualization layer), attackers can indirectly collect sensitive information about the cloud using energy consumption logs. This type of data (energy consumption log) is maintained to monitor the infrastructure status and to provide computer energy efficient workload mapping.

e) **Targeted Shared Memory attack:** In this attack, attackers take advantage of shared memory (cache or main memory) of both physical and virtual machines. It is an initial level attack in cloud computing that can lead up to several different types of attacks such as side channel attacks and malware injection attacks.

f) **Phishing attack:** Phishing is an attempt to access personal information from unsuspecting user through social engineering

techniques. It is commonly achieved by sending links of web pages in emails or through instant messages. These links appear to be correct, leading to a legitimate site such as bank account login or credit card information verification but they practically take users to fake locations. Through this deception, the attacker can obtain sensitive information such as passwords and credit card information. Phishing attacks can be classified into two categories: (1) an abusive behaviour in which an attacker hosts a phishing attack site on cloud by using one of the cloud services and (2) hijack accounts and services in the cloud through traditional social engineering techniques.

g) **Botnet or Stepping Stone attack:** In Stepping Stone, attackers try to achieve their goals (such as spying, DoS, damaging, etc.) while avoiding revealing their identities and locations to minimize the possibility of detection and trace-back. This is achieved by indirectly attacking the targeted victim through a sequence of other hosts (called stepping stones). Stepping stone hosts can be recruited through illegal botnets. A bot-master, through botnet attack, can setup command and control server and stepping-stones into cloud in order to steal sensitive information and to gain unauthorized access to cloud resources in a bid to make it behave abnormally. The countermeasure includes what they call a “pebble” trace scheme to trace-back the bot master. It first identifies the cryptographic keys of the botnet communication in order to configure the botnet operations and then it traces back the bot master. It involves the design and implementation of a new key identification scheme and an approach for tracing-back bot master across stepping-stones beyond multiple cloud.

h) **Audio Steganography attack:** Steganography attack has been regarded as one of the most serious attack to cloud storage systems. Audio Steganography helps users to hide their secret data within regular audio files. The steganography user can transmit secret information through sending media files, which appear to be normal sound files. Hackers utilize this feature to deceive the current security

mechanisms or traditional countermeasures (e.g., steg-analysis) for protecting cloud storage systems by hiding their malicious code in sound files and sending it to victim servers.

i) **VM Rollback attack:** The virtualization environment in cloud computing is the most vulnerable area to attack. The hypervisor can suspend a VM at any time during execution, take a snapshot of current CPU states, disk and memory and resume a snapshot later without guest VM awareness. This feature has been widely used for fault tolerance and VM maintenance; however, it also provides an open window to an attacker to launch VM rollback attacks. In a rollback attack, a user can take advantage of previous snapshots and run it without the user's awareness and then clean the history and again run the same or different snapshot. By cleaning the history, the attacker will not be caught for his suspicious activities. An architecture named "Hyperwall" is used as a countermeasure in order to manage hypervisor vulnerabilities. The solution to prevent VM rollback attack is based on disabling the suspend/resume functionalities of the hypervisor.

2. Privacy Regulations

Policies on the creation of privacy legislation are different in the European Union and the United States. The United States favour a laissez-faire approach where Industry self-regulation is favoured over federal law. It is believed that businesses shape their policies according to consumer preferences, following economic theory. This theory implies that consumer preferences determine market share, and that a higher market share leads to higher profits. Privacy in the United States is dispersed among various different sector specific laws. These sectors include the health care sector for the Health Insurance Portability and Accountability Act (HIPAA) and the financial services sector for the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and the Payment Card Industry Data Security Standards. The Act covers Credit Reporting Agencies (CRAs) and is enforced by the Federal Trade Commission. All these acts basically implement the Fair Information

Principles. The European Union has a different approach concerning legislation and it favours participation among businesses and governments as opposed to the US self-regulation approach. The European Union set privacy regulations up front as opposed to relying on industry self-regulation.

a) **EU Directive 95/46/EC:** Directive 95/46/EC, commonly known as the Data Protection Directive, was implemented in October 1995 (EU Directive, 1995). The main purpose of the directive was to harmonize the privacy laws that existed in the different member states of the European Union and to provide a basic standard on privacy protection. Directive 95/46 /EC address personal data or personally identifiable information. Personal data is defined as any information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Directive 95/46/EC was written with the purpose of safeguarding the privacy of European Union inhabitants and to integrate different privacy legislation of EU member countries. European based organizations should adhere to its principles. Organizations outside the EU may use the Safe Harbour Agreement, Standard Contractual Clauses or Binding Corporate Rules.

b) **The Safe Harbour Agreement:** From a European point of view, the United States do not provide adequate privacy protection. This prevents data transfers between Europe and the United States. To address this problem, the European Commission and the United States Department of Commerce negotiated the Safe Harbour agreement which is only applicable to transfers between the United States and the European Union. Organizations outside the United States that have business operations within the European Union have to rely on different mechanisms to adhere to the Trans-border Transfer principle from Directive 95/46/EC. This principle requires that personal identifiable information can only be transferred to those countries that are

deemed to provide adequate security. A US-based organization in order to comply with the Safe Harbour agreement must follow the Safe Harbour Privacy Principles, disclose their privacy policies, be subject to the statutory powers of the Federal Trade Commission, verify compliance with the Principles through self-or third-party assessment and register with the Department of Commerce. The Department of Commerce maintains a list with organizations adhering to the Safe Harbour agreement.

c) **The FTC Fair Information Practice Principles:** The FTC Fair Information Practice Principles are a set of guidelines concerning fair use of information about individuals. The Federal Trade Commission (FTC) first mentioned its Fair Information Principles in the 1998 report and the last version was published by the FTC on the 25th of June 2007. Organizations are allowed to adhere to the Fair Information Practice Principles but cannot be enforced to comply with the principles. The FTC Fair Information Practice Principles consist of the following five principles: (i) Notice/Awareness, (ii) Choice/Consent, (iii) Access/Participation, (iv) Integrity/Security and (v) Enforcement/Redress.

d) **Other Privacy Regulations:** Some other American privacy regulations are sector specific, they include (i) the Health Insurance Portability and Accountability Act (HIPAA) which is created specifically for the health industry, (ii) The Gramm-Leach-Bliley Act (GLBA) which is specifically designed for the financial services sector and applies to financial institutions and (iii) the Fair Credit Reporting Act (FCRA) applies to consumer reports of United States citizens.

3. International organizations' efforts to address data privacy[38]:

Recognizing the differences in domestic data privacy regimes, there have been a number of international efforts through multilateral organizations to develop a common framework for cloud-related policy. The two most notable of these are the efforts of the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC)

[38] Policy Challenges of Cross-Border Cloud Computing-Renee Berry and Matthew Reisman

forum. Both organizations have focused primarily on developing a shared set of principles for data privacy.

a) The **OECD Guidelines** were adopted in 1980, making them the first multilateral effort to address privacy issues related to cross-border data flows. The Guidelines establish several rights of the individual pertaining to his or her personal data and lay out framework principles that national governments should follow in protecting these rights. The Guidelines also encourage countries to support industry self-regulation where possible. Overall, while the Guidelines established some principles that have guided the direction of countries' data privacy laws, they also preserve a great deal of flexibility, as evidenced by the very different data privacy regimes among OECD countries. The OECD is currently in the process of conducting a review of the guidelines to evaluate whether they need to be revisited or revised.

b) A more recent set of international principles for cross-border data privacy is the 2004 **APEC Privacy Framework**. While the OECD Guidelines address the rights of individuals and the responsibilities of governments, the APEC Framework primarily addresses the responsibilities of companies and organizations that collect personal data. The core principle in the APEC Framework is "accountability", that the entity that collects personal information is responsible for ensuring it is handled in accordance with the privacy guidelines in the Framework, regardless of where that information travels.

c) The most recent effort to develop international data privacy principles is the **Madrid Resolution**, adopted in late 2009 by about 50 countries participating in the annual International Conference of Data Protection and Privacy Commissioners. The principles laid out in the Madrid Resolution are broadly similar to the framework of the EU Directive, but the major difference is that the Madrid Resolution is non-binding.

Annexure-IV

Legal Framework in some countries

1. European Union: The EU is in process of building Cloud Computing strategy as highlighted in their Digital Agenda. This strategy will clarify the legal conditions for the take-up of cloud computing in Europe, stimulate the development of a competitive European cloud industry and market and facilitate the roll-out of innovative cloud computing services for citizens and businesses. The strategy comprises three main aspects –

- The legal framework: This covers data protection, privacy (including the international dimension), laws and other rules having a bearing on the deployment of cloud computing and user rights insofar as provided for by law.
- Technical and commercial fundamentals: The strategy would seek to extend EU research support for cloud computing and focus on issues such as security and availability of cloud services. Also addressed would be the technical standardization of APIs, data formats and templates for contracts and service level agreements.
- The market: Pilot projects will be supported aiming at cloud deployment. The Commission will work on common approaches to cloud computing.

2. United States: In the US, there is no dedicated legislation on cloud computing. However, cloud computing has not escaped the attention of the federal government with the term being formally defined by National Institute of Standards and Technology, US Department of Commerce (NIST).The Cloud Computing Act of 2012[39], which seeks to set specific security and privacy measures, definitions, and transparency mandates that would apply only to a cloud environment and not to other forms of

[39]http://www.govtrack.us/congress/bills/112/s3569/text

computing is proposed. The Act encourages the federal government to negotiate with other countries to establish consistent laws related to online security and cloud computing. It also aims to form new civil and criminal enforcement tools to investigate and prosecute hackers, and would require all federal agencies to create a "cloud-computing plan" and monitor progress toward more secure policies. It also provides for patent and copyright protections. It also sets a pecuniary penalty floor for violations. The Act is presently referred to a committee.

In 2002, the US put in place a streamlined process called the Safe Harbor Privacy Principles by way of which US companies can comply with the EU data protection laws. There are also different laws governing state and federal access to private information.

There is a perceived threat to the US cloud market, due to worries about government surveillance. According to a survey in 2014, 82% of US-based IT companies said privacy laws are a top concern for them when choosing where to store data. Meanwhile, US government policy mandates have called federal CIOs and other IT executives to adopt cloud technologies, beginning with the launch of Federal Cloud Computing Initiative (FCCI).

3. International laws: The Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" enumerating seven principles for protecting personal data. However, these guidelines are non-binding. With more and more sensitive commercial and personal data being stored on the cloud, regulators and authorities around the world have responded to concerns about the security of cloud computing by introducing new laws, regulations and compliance requirements which attempt to mitigate the perceived security and data privacy risks associated with the use of cloud computing. The stringency of some of these requirements has led to some organizations shunning the adoption of cloud computing solutions, citing the web of legal

and regulatory requirements and the costs associated with ensuring compliance as a prohibitive factor. Major international developments are:

- Cloud Industry Forum ('CIF'), UK has formulated a Code of Practice for Cloud Service Providers for organizations offering remotely hosted IT services of any type.
- New Zealand Computer Society (NZCS)has developed a Cloud Computing Code of Practice which applies to businesses who offer remotely hosted IT services of any type, either to New Zealand or within New Zealand, that meet the definition of Cloud Computing defined by them.
- The Data Protection Acts (Section 2C (3)) place responsibility for data security squarely on the data controller who is accountable to the individual data subject for the safeguarding of their personal information. A data controller must therefore be satisfied that personal data will be secure if it is outsourced to a cloud provider.
- The Singapore government has passed the Personal Data Protection Act, 2012 (PDPA) which is consistent with international standards for data protection. The PDPA will be implemented in a phased approach after coming into force in January 2013.

Annexure-V

Government Initiatives in Cloud Computing sector

1. Government of India (GoI) is keen to explore a cloud based application and data access model to revolutionize its e-governance initiative. The focus of e-governance is to reduce corruption and ensure the government schemes are reaching people living in rural areas of the country. Further, e-governance services ensure quicker service delivery and eliminate the involvement of middlemen who tend to capitalize on loopholes for quick money by means of exploiting people. To build the backbone of national e-governance plan, the Department of Information Technology intends to establish a national cloud-based network which would link all the data centres of the 29states and 7 Union Territories (UTs) of the country. Not only would this enable the states and UTs to get their own private cloud, this plan would also assist in the timely implementation and delivery of different government to citizen and government to business services via the cloud. Once implemented, the infrastructure would help the government to share critical information across departments via common IT resources.

2. Another example[40] which shows the renewed focus of the government on e-governance projects is the Unique Identification Authority of India's **Unique Identification (UID) project** which is the most ambitious example of how Government can harness cloud computing to help change the lives of people at the bottom of the economic pyramid. The UID aims to provide a real-time service for verifying the identity of any Indian resident through biometrics and demographic information and can be used by a variety of national, state and local government agencies, as well as private businesses. So far, the Unique

[40] http://theinstitute.ieee.org/ieee-roundup/opinions/ieee-roundup/an-indian-perspective-on-cloud-computing

Identification Authority of India has collected biometric and demographic information from over 100 crores people and various government agencies are beginning to use the system. The government has already taken a decision to move the critical information infrastructure on the cloud, and DIT has taken steps towards a national cloud based network that connects all state data centres. Once this is done, the NeGP (National e-Governance Plan is likely to get a boost in delivering most government services more efficiently and with complete data back-up.

3. Further, Government of India (GoI) has approved the setting up of National Optical Fibre Network (NOFN) on 25th October, 2011 to provide connectivity to 2,50,000 Gram Panchayats of the country which would ensure broadband connectivity with adequate bandwidth. This is to be achieved utilizing the existing optical fibre and extending it to the Gram Panchayats. For this purpose, GoI has set up **Bharat Broadband Network Limited (BBNL)** on 25th February, 2012 as a Public Sector Undertaking for the establishment, management and Operation of National Optical Fibre Network (NOFN) now upgraded to a full-fledged project *BharatNet*. Services like G2C, B2B, P2P, B2C etc. covering e-education, remote health monitoring, e-governance, weather, agriculture etc. can be accessed by common man through NOFN. TRAI recently released "Recommendations on Delivering Broadband quickly" for effective deployment of BBNL in such areas.[41]Such services may be built on top of the cloud infrastructure.

4. The Indian Government in on the advent of leveraging the advantage of Cloud Computing more effectively in collaboration with all the State governments. All e-governance platforms across the country could be migrated into cloud architecture with an option of a public cloud and a private cloud. The private cloud will associate with all inter

[41]http://www.trai.gov.in/WriteReadData/Recommendation/Documents/Broadband=17.04.2015.pdf

departmental communications while the public cloud will interface with the consumers. The data centres for such applications could be centrally located strategically at number of places in the country. This model will substantially lower the capital cost and the operational cost in each of these states. The burden of maintaining such complex IT systems, up gradation of the same at regular intervals, imparting effective training for the users will also be substantially reduced.

5. Some examples of cloud adoption in various states across India are as follows:

   - The **Jammu & Kashmir** state government has adopted cloud computing for its e-Governance services by using Microsoft's solution. It is the first state of India to adopt cloud computing for e-governance like issuing birth or death certificates etc. The data centers of these services are located in Madhya Pradesh
   - The governments of **Himachal Pradesh and Uttarakhand** are also in discussions with Microsoft to roll out e-Government services based on the cloud platform. Uttarakhand government has already deployed **State Wide Area Network (SWAN)** and in process of putting State Data Centres (SDCs) in place to fully deploy the e-government services on cloud platforms. These SDCs are to be used for hosting the State Service delivery gateway (SSDG) and state portal and forms the main engine of e-Forms. Once the infrastructure is in place, state governments would be loading applications on the Uttarakhand SWAN, which can accessed through the SSDG, These gateways will provide a single window access to the information and services of the state government at all levels. By simply filling in specific forms with the required information at nearby service centres, all citizens, including those in remote rural areas, will be able to access data and apply for certificates etc with the click of a mouse.

- The **Tamil Nadu** state government launched the cloud computing services of Microsoft from state secretariat through the company's hyper scale data centre set up in the state in September 2015.
- **Maharashtra** state government has implemented the cloud based platform known as MahaGov as shown in figure 1 below, in partnership with companies such as VMware Inc. and Microsoft India Pvt. Ltd. It is the first state to incorporate IPv6 protocol. The initiative is successful in reducing the cost drastically while increasing the IT capacity with maximum flexibility.

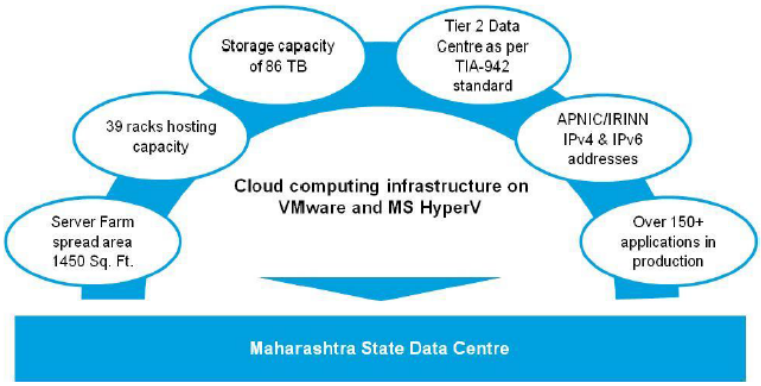

Figure 1: Salient features of MahaGov

Apart from these government initiatives, software giants are also showing increasing interests in India. Global software major Microsoft also announced its partnering with Federation of **Karnataka** Chambers of Commerce and Industry (FKCCI) to help about 200,000 small and medium businesses (SMBs) across the state use cloud computing to spur their revenue growth.

6. At present the SWANs in 30 states (Andhra Pradesh, Chandigarh, Chhattisgarh, Delhi, Gujarat, Goa, Haryana, Himachal Pradesh, Jharkhand, Kerala, Karnataka, Lakshadweep, Maharashtra, Orissa, Punjab, Puducherry, Sikkim, Tamil Nadu, Tripura, Uttar Pradesh, West Bengal, Assam, Bihar, Madhya Pradesh, Uttarakhand, Manipur, Arunachal Pradesh, Meghalaya, Nagaland and Mizoram) are operational. The SWAN in **Rajasthan** is in advance stage of

implementation. Such initiative form the backbone for boosting the adoption of cloud services application in public sector.

7. The current National e-Governance Plan (NeGP) has its own strengths as the first well organized plan of the Govt. of India for both Central and State level e-Governance projects. Twenty-seven mission mode projects (MMPs) of NeGP had seen their partial successes. However, many additions such as stakeholders needs analysis, project planning and management, process reforms and reengineering could be identified, especially in the context of technology developments such as the ubiquitous mobile phone penetration calling for mobile applications, new technologies such as Service-Oriented Architecture (SOA), grid, cloud, big data analytics, and enterprise architecture techniques for deployment in e-Governance.

8. *Cloud Adoption in Banking Sector:* Reserve Bank of India (RBI) is working on financial inclusion of the technology and they are keen on incorporating Cloud based solutions particularly for Cooperative banks to extend the banking services across the country through core banking solutions. Government e-Payment Gateway will facilitate direct credit of dues from the government into the account of beneficiaries using digitally signal electronic advice (e-advice). The systems, covering all central government departments and ministries are accepted to eliminate almost 20 million cheques.[42]Indian Banking Community Cloud (IBCC) is the first Community Cloud initiative for banking industry in the country. The theme has been to "Optimize costs while maintaining desired levels of efficiencies and security". Institute for Development and Research in Banking Technology (IDRBT) is working with public sector and private sector banks to provide Infrastructure as a Service for non-customer facing and less critical applications. The banks would benefit from the following:

[42]Proceedings of International Conference on Cloud Computing and e-governance, K.KokulaKrishanHariet al.

- Reduced timelines
- Moving the cost from CapEx to OpEx
- Focus on core banking business

9. *Cloud adoption in manufacturing sector*: With **Make In India initiative** in full swing, Indian manufacturing sector since 2010, CIOs in Indian manufacturing have started adopting cloud models and this is highlighted in many research studies and industry circles. Some of the most notable application areas in manufacturing suited for cloud are CRM and supply chain applications which provide better connectivity to external stakeholders and customers. The area of business intelligence (BI) and business analytics (BA) is highly important for manufacturing sector because of large amounts of data generated in manufacturing which is a challenge for CIOs. For instance analytics will help the organization to better forecast products range and provide analysis for future investments in different business areas. BI helps to understand customer demands and provide inputs for demand shaping. Human machine interface (HMI) is another area where companies such as Jindal Steel have adopted cloud model for their HMI applications to quickly recover their ROI. HMI refers to interfacing IT systems like ERP with manufacturing executing systems (MES) and plant automation. In addition to the above applications, the other areas where cloud enhances manufacturing effectiveness are in data warehousing, information security, green IT, and many others.

10. *Cloud Adoption in Telecom Sector:* The Operation Support System (OSS)[43]and Business Support System (BSS) in Indian telecom industry are now widely keen on deploying SaaS (Software-as-a-Service) to reduce their CapEx and OpEx.

[43]www.tele.net.in Volume no. 16, Issue no. 12, December 2015

(a) Deploying OSS/BSS solutions over cloud platforms is a highly effective method of addressing several business and technical challenges, including management of software upgrades (with near zero downtimes) and the on-demand scaling up of operations using virtual machines on the same hardware.

(b) Cloud-based infrastructure offers an efficient way to enable resource sharing, automation and monitoring. It provides elasticity in handling burst traffic scenarios without having to make upfront investments as well as the ability to automate server configurations.

Big data solutions and analytics for OSS/BSS in Indian telecom companies are easily complemented by cloud owing to its scalability.

11. *Cloud Adoption in Start-up and SMEs:* One of the key benefits of cloud computing is the low capital investment and quick time to market the new ideas. This particularly encourages entrepreneurship in the country, enabling start-ups and small medium businesses to start small and expand their business based on demand. Cloud undoubtedly accentuates self-employability. The entrepreneur can be a simple software developer who uses the PaaS cloud to develop new cloud services without investing towards application development. Once the service is live, customers of the new business can be managed by SaaS platforms with support cloud services such as CRM-as-a service. Cloud which provide services to the customers which require less load balancing like those of SMEs are able to overcome the bandwidth requirements and facilitate faster deployment of cloud in the country. Indian SMEs are expected to increase cloud adoption at a CAGR of 20 % between 2012 and 2016.[44]

[44]http://www.business-standard.com/article/economy-policy/smes-may-increase-cloud-adoption-at-20-by-2016-ey-assocham-114050100538_1.html

12. *Cloud Adoption in Indian Railways:* Railways are utilizing the mobile technology in a big way for freight management and passenger reservation system. Protection of data and implementation aspects are very crucial and guidelines for Industry interaction on such matters are essentially worked out by Government of India. Strategies have been rolled out to use cloud for GIS management in railways, for e-ticket bookings and for automated surveillances of railway premises and storage of video logs in cloud data centres.

13. *Cloud Adoption in Education Sector:* Megh-Sikshak is a cloud-based learning management system, which is evolved from the objective of converting the traditional model of e-Learning system (eSikshak) to a SaaS model. Megh-Sikshak offers multi-lingual e-Learning services leveraged by cloud computing capabilities and demonstrates the new model of a SaaS based e-Learning system. This SaaS-based Learning Management System (LMS) currently conforms to SaaS maturity level 3, which allows the system to support multiple tenants of multiple organizations. The cloud-based eSikshak delivers e-Learning as a service rather than as a product, which helps the institutions/organizations/individuals in alleviating the burden of installation, maintenance, and management of the e-Learning application on-premise. Apart from this, IIT Delhi, IGNOU and other universities have deployed their own cloud environments.

14. *Cloud Adoption in Health Sector:* Cloud Computing Innovation council of India has proposed a layout for systematic adoption of cloud services in Indian health sector, known as **e-Health** vision. e-Health vision aims to incorporate **Health Information Exchange (HIE)** mechanisms to successful deployment of cloud. An electronic health information exchange (HIE) allows stakeholders associated with health data to appropriately access and securely share a patient's vital medical information electronically.HIE Proposal for India include the following **types of HIE:**

- *Directed Exchange:* Directed Exchange enables healthcare providers to easily and securely send confidential patient information (such as laboratory orders and results, patient referrals, and discharge summaries) to another health care professional. This information is sent over the Internet in an encrypted, secure, and reliable way among health care professionals. This information is packaged further in encrypted, secured, and reliable form and sent over the Internet among health care professionals. The format of data exchange is XDR and XDM for messaging.
- *Query-Based Exchange:* Query-based exchange enables providers to search and discover accessible clinical sources regarding a patient. These exchanges deal with transport and structure of data. The format of data exchange is HL7 CDA and messaging.
- *Consumer-Mediated Exchange:* Consumer-mediated exchange provides benefits to patients such as management and control of health care through online mode. Patients can provide access to their health records on a need basis. This concept is called health recording banking.

Usage of cloud for e-healthcare analytics is also upcoming at a fast pace in Indian health industry. National Health Registry is being planned. NIC Hyderabad is working on a pilot in which aggregate data like number of births, number of vaccinations, etc. is available in real time.

15. *Cloud adoption in RTI:* Government initiative to digitize its database and make more and more information available to the public domain calls for an indispensable need of adoption of cloud services in the domain of Right To Information for efficient performances.

16. *Meghraj:* Department of Electronics and IT (DeitY) of Government of India has initiated an extensive project termed as 'GI Cloud'. The 'GI Cloud' *Meghraj* is the Government of India's cloud computing environment that will be used by government departments and agencies at the centre and statesfollowing a set of common protocols, guidelines and standards issued by the Government of India. Figure 2 shows architecture of *Meghraj.*

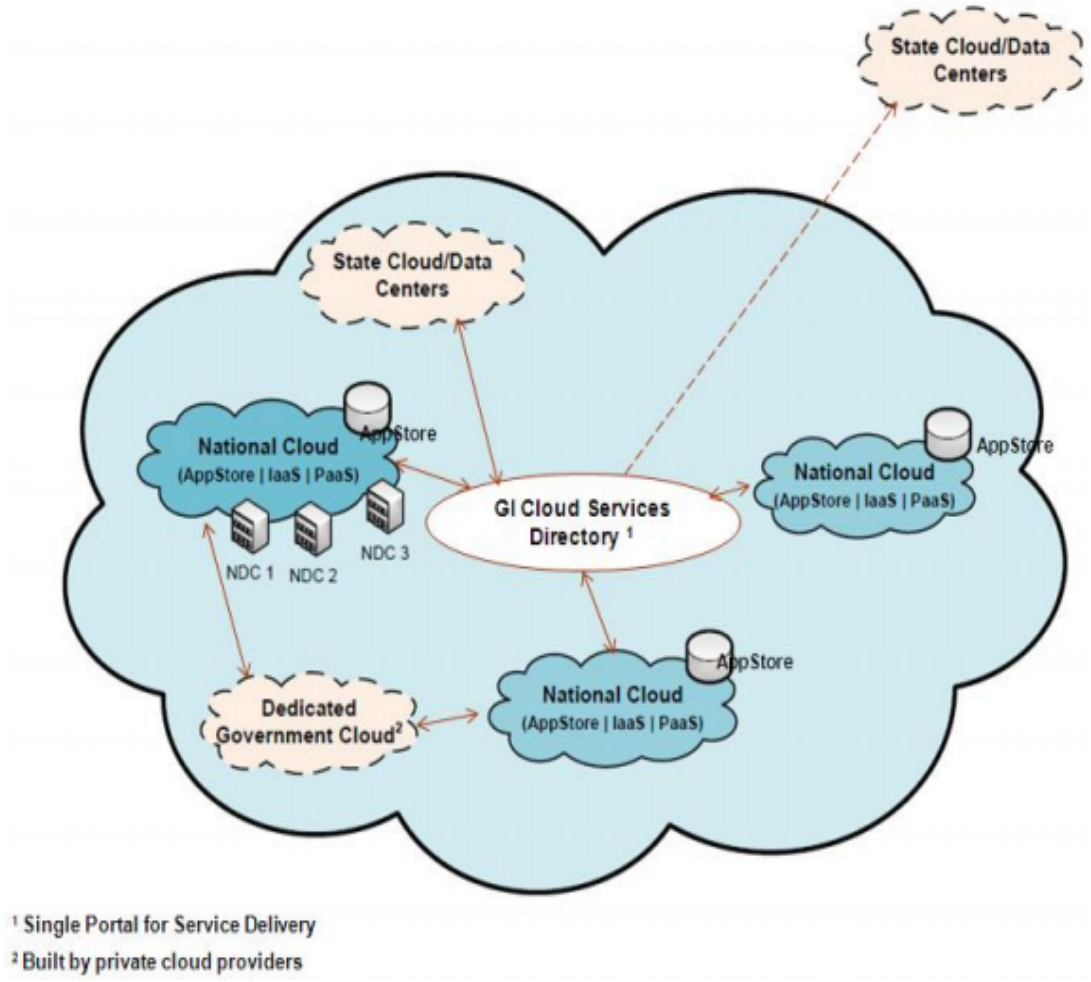

Figure 2: GI Cloud *Meghraj* Architecture[45]

[45]GI Cloud (Meghraj) Adoption and implementation Roadmap, April 2013, Department of EIT, GOI

17. There shall be separate National and State Data centres with the provision of integration as per the need of a state. It will enable the government to leverage cloud computing for effective delivery of e-services. Keeping this in mind, National Data Centre at Shastri Park, Delhi is at an advanced stage of virtualisation and is the largest government data centre. Initially, one National Cloud will be set up and after assessing the demand, application sensitivity and data classification. Services provided by National Cloud could include infrastructure (compute, storage and network), platform, backup and recovery, infrastructure scaling of the State Cloud, application development, migration, hosting etc. The institutional set-up of GI Cloud is described in Figure 3.

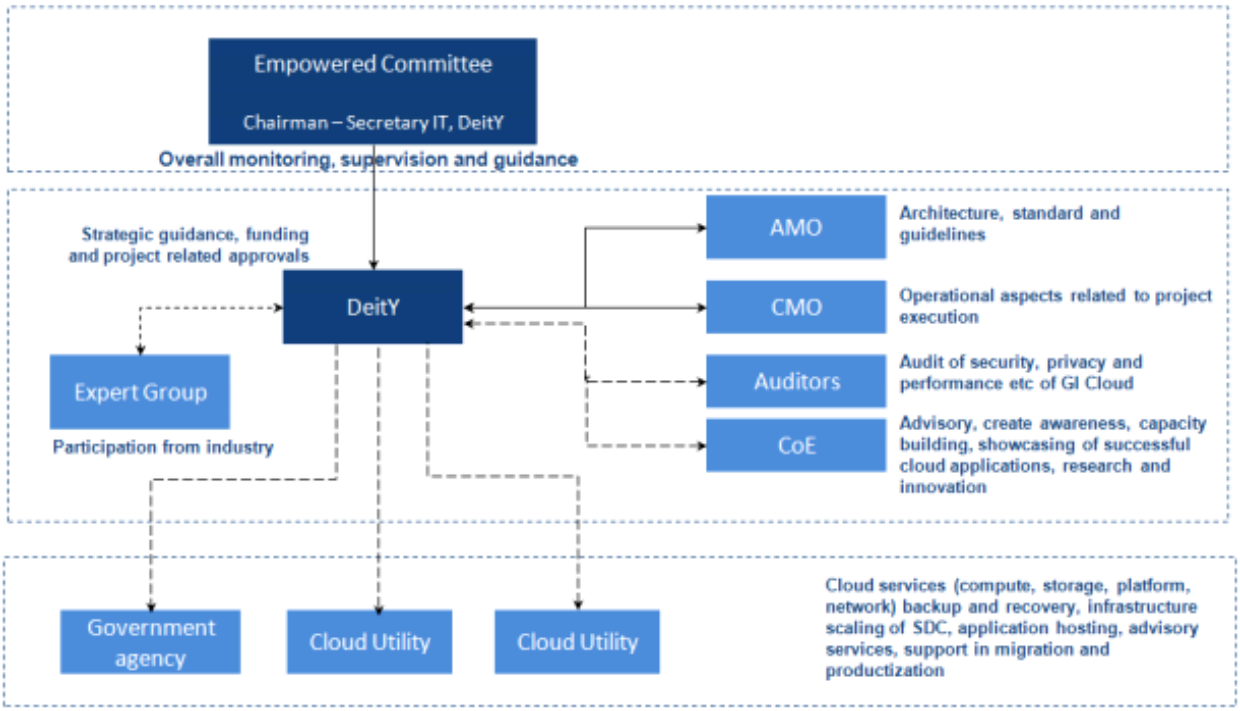

Figure 3: GI Cloud Institutional Set-up

18. It is also pertinent to clarify that the cloud services envisaged for GI Cloud are different from the end-user services like services delivered through various MMPs like e-District, Passport, eSeva Project, MCA21 and Income Tax, and other national or state projects like UIDAI.

19. *National eGov App Store:* The eGov App Store will include the setting up of a common platform to host and run applications (developed by government agencies or private players) at National Cloud, which are easily customisable and configurable for reuse by various government agencies or departments at the central and state levels without investing effort in the development of such applications. The eGov App Store hosted on the National Cloud will be termed as the 'National eGov App Store'. More than one application store can exist in the GI Cloud ecosystem. However, there will be a single window or portal or service catalogue – the GI Cloud Services Directory – displaying the various applications and services of each of the eGov App Stores.[46]

20. A Task Force was constituted by Department DeiTY with a focus to bring out the strategic direction and implementation roadmap of GI Cloud leveraging the existing or new infrastructure. Based on various discussions , inputs and industry consultations, the following two reports have been prepared by DeitY Task Force:

- GI Cloud Strategic Direction Paper
- GI Cloud Adoption and Implementation Roadmap

These reports have been approved by the Hon'ble Minister of Communications and Information Technology.

21. The DeiTY also formed an inter-ministerial working group including experts from various organizations including NASSCOM, FICCI, CDAC, RBI, DSCI, IDRBT to examine all various issues. The working group had series of meetings and detailed discussions in 2015 with experts from these organizations in the context of security, infrastructure and legal challenges associated with cloud computing. The recommendations of the committee are also expected.

[46]https://negp.gov.in/pdfs/cloud_adoption.pdf

22. The DeiTY also conducted a survey towards the close of 2015 from various organizations using cloud computing services about their expectations from the government and their experience while running their business from cloud. As per the survey and feedback, the organizations enlisted have, the following expectations from Indian government:

- Need to create a Cloud First Policy to incentivize the cloud adoption by government departments.
- Promote creation of state level data centres and sharing of resources between states
- Provide access to certain government databases to private sector to build services
- Incentivizing the creation of data centres within India by private sector for the government's cloud adoption
- Incentivizing the creation of cloud services by private sector.

23. *NIC Cloud Computing:* NIC's cloud computing approach provides government partners with an opportunity to effectively manage technology resources that accelerate speed to market and deliver resources on a scalable as-needed basis. The NIC private cloud offers federal, state, and local government partners a state-of-the-art, high performing, and fully secure hosting operation that support secure transaction processing worth several billion dollars per year. NIC's private cloud is backed by a team of technicians with more than 200 years of combined IT management experience.

Annexure-VI

Cloud adoption models by Governments in Asia Pacific Region

1. Cloud adoption in Asian Economies[47]

The Asia Cloud Computing Association has issued third Cloud Readiness Index (CRI) in May, 2015in Singapore to track the development of the necessary infrastructure and enabling environment for cloud computing across leading Asian economies. The index has been measured based on ten different parameters. The country wise status is given in figure 1 below:

SME Cloud Computing Market Attractiveness Index 2015

Overall Ranking

RANK / ECONOMY		Addressable Market	Early Adoption	Demand Drivers	Affordability	Support	OVERALL SCORE
1.	Japan	101.4	57.7	71.0	64.7	56.6	70.2
2.	Singapore	25.7	78.0	68.7	73.0	73.8	63.8
2.	Hong Kong	29.3	75.7	66.7	75.3	72.3	63.8
4.	South Korea	40.3	67.7	78.0	70.7	58.8	63.1
5.	China	141.9	37.3	36.3	29.3	59.0	60.8
6.	Taiwan	27.6	73.3	62.7	66.7	73.0	60.6
7.	Australia	44.3	56.7	72.0	80.3	46.0	59.9
8.	New Zealand	28.3	72.3	71.3	77.7	48.8	59.7
9.	Philippines	17.8	66.0	52.7	54.3	52.8	48.7
10.	Indonesia	76.8	39.7	39.3	31.3	52.0	47.8
11.	Malaysia	20.6	57.3	41.0	53.0	60.8	46.5
12.	Thailand	22.4	50.0	47.0	48.7	56.8	45.0
13.	India	39.3	39.3	24.3	43.7	42.0	37.7
14.	Vietnam	6.2	41.0	26.0	34.7	35.5	28.7

Source: Asia Cloud Computing Association 2015 http://www.asiacloudcomputing.org/research/smecloud2015

Figure 1: Cloud Readiness Index

On a country-by-country basis, Cloud Readiness Index (CRI 2015) shows the region breaking down into three groups of countries: ever-ready leaders such as Japan, China, Singapore, Hong Kong and South Korea; the dedicated improvers such as Taiwan, Australia, New Zealand, China

[47]http://asiacloud.org

and the Philippines, and the steady developing countries including Thailand, Indonesia, India and Vietnam.

2. Cloud Adoption by Governments in Asia Pacific

The figure 2 below depicts the adoption of cloud by different Asia Pacific governments.

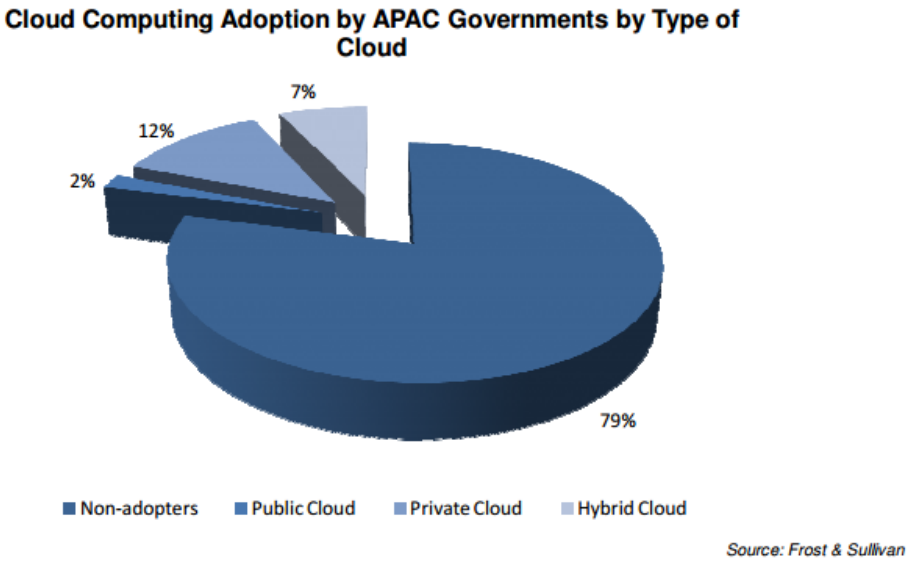

Figure 2: Cloud Adoption by APAC Governments

Japan: Japanese businesses are adopting cloud computing at the highest rate in the Asia-Pacific region. In a survey of more than 3,500 organizations in Japan, Springboard Research found that 13% had adopted some form of cloud computing or software as a service (SaaS). Take-up is strongest (36%) among companies with 10,000 employees or more. The Japanese government, for its part, is encouraging companies to use cloud services, as it believes that more effective use of IT will make the economy more competitive. As per the Japan's Ministry of Internal Affairs and Communications, the cloud initiative, Kasumigaseki Cloud, aims to establish a large cloud computing infrastructure to meet the increasing requirements of the Government's IT systems and bring in greater efficiencies though a shared pool of resources, thereby eliminating the need to maintain separate IT systems for different ministries. The Kasumigaseki Cloud is now in completion phase. The cloud supports all government ICT systems and has been key in growing Japan's cloud market. This cloud has

enabled public and private sector collaboration on processing of government documents and included increased online applications to encourage public use of mobile devices in accessing government functions. Moreover, Japan's government has committed to ensuring all households have "very high speed" fibre broadband connections by the end of 2015, bringing the potential benefits of cloud services to every household in the country. By 2016 Japanese regulators will require the electronic submission of data from any scientific or health care clinical trials, a key market for U.S. cloud providers like Medidata and one offering opportunities for other vendors.

Singapore[48]: A major example where Government is showing strong confidence in Cloud Computing and adopting various measures for its promotion is Singapore Government. Singapore Government recognises Cloud Computing as an "important next paradigm" in information technology with advantages of "low cost virtualization, long-term cost effectiveness, and new possibilities in applications involving massive data". The interest in cloud computing is very high in Singapore, and this was best exemplified by the amount of support that the government gave to CloudAsia 2014 event which got underway on November 2014.Current cloud offerings are seen to be commercially accessible with common SaaS packages running at between 0.42-5.21% of SME IT spend, and common PaaS access running at between 1.63-13.63% of SME IT spend.[49] The Republic is indeed considered to be the largest and fastest-growing cloud and data centre event in Asia. Programmes of particular note include the Productivity and Innovation Credit (PIC) scheme, which grants businesses 400% tax deductions for each of five years against the acquisition of cloud computing services and IT equipment, and SPRING Singapore's Capability Development Grant (CDG), which can defray up to 70% of SME project costs as they relate to ten key capabilities including cloud computing. The government has formulated and in process of implementing an eGov2015

[48]Thien-Huong, thienhuong.do@gmail.com. Apr 2012

[49]http://www.asiacloudcomputing.org/images/research/ACCA_SMECloudComputing2015_Index_FINAL.pdf

master plan for Singapore about building an interactive environment where the Government, the private sector and the people work together seamlessly, through the enabling power of infocomm technologies.

Australia[50]: The Australian Government has been quite circumspect in its approach in adopting cloud computing, primarily due to their uncertainty over storing data in offshore data centres. Australian Taxation Office, Australian Bureau of Statistics, Treasury/ ATO, Department of Immigration and Citizenship (IMMI) and Australian Maritime Safety Authority are some of the agencies that have implemented cloud computing technology in the country.

The Australian Government's Phased Cloud Implementation Strategy is given in figure 3 below:

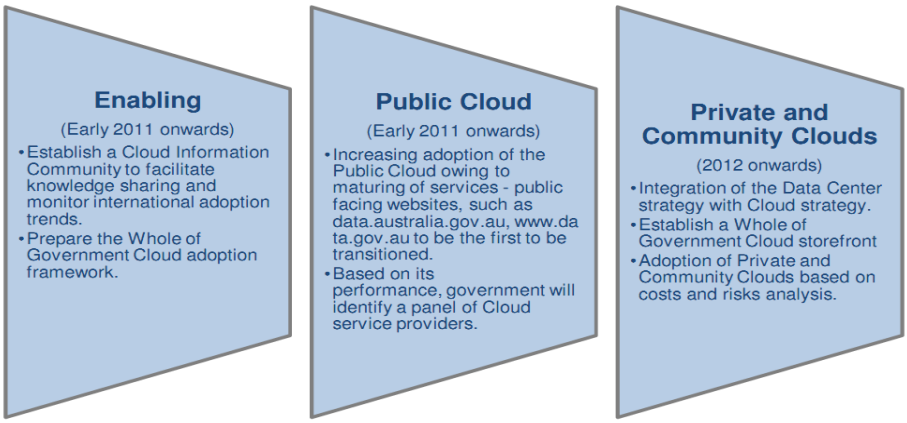

Figure 3: (Source: Cloud Computing Strategic Direction Paper, Department of Finance and Deregulation, Australian Government)

New Zealand: In 2013, only 10% of New Zealand SMEs were using cloud computing services; but, by 2014 this was up to 32%. Sixty percent of New Zealand businesses reported that they use, or intend to use in the near future, at least one type of cloud computing technology. In August 2012, the New Zealand Government adopted a "cloud-first" policy towards its own IT

[50]Frost & Sullivan

developments and has a highly developed policy and roadmap for a transition to cloud computing. In addition, the government has made Universal Fast Broadband rollout a flagship policy and created a NZD1.5 billion revolving fund to subsidise its construction. These measures, combined with the industry's development of a Cloud Computing Code of Practice, make the country a leader in cloud computing policy and infrastructure.

China: Cloud has come into the trial and implementation phase from the initial recognition phase in China. Some metropolitan cities in PRC are trying to build up cloud data centres and enrich various service types on the cloud platform to improve their own investment environment from the government side. Under such circumstances, public cloud was triggered and is entering into another era with more rapid growth. Government is expected to adopt more aggressive measures to introduce more enterprises to leverage the infrastructure. Gartner projects the public cloud market to reach $20.7 billion by 2018, with an annual growth rate of 31.5 percent (while IDC notes sustained annual growth of over 40 percent in the Chinese public cloud market). Cloud adoption in the public sector in China is being driven at a local level in cities such as Dongying and Wuxi. The Yellow River Delta Cloud Computing Centre, being built by IBM, will provide cloud-based platform for the petroleum industry to develop more innovative application services. Furthermore, the centre will provide software development and test resources, through the Internet, to start ups and other companies that establish their presence in the city. In addition, this cloud will be expanded to also be an e-Government Services Platform for the economic development zone. As part of future phases, there are plans to implement a solution that will enable "Smart Roads" and a "Smart Airport" based on data analytics. This will be followed by the addition of healthcare services to the cloud as part of the plan to centralize patients' records and make them available to doctors online. In the city of Wuxi, the Government has developed a Cloud Services Factory to provide adequate computing resources to the enterprises located in the Software Park. These enterprises, primarily start-ups, did not

have the financial bandwidth to acquire the required IT assets to compete effectively. Programmes such as these can be taken up after detailed analysis on their viability. In January 2015, China's State Council published Guiding Opinions for Promoting the Innovation and Development of Cloud Computing to Cultivate New Types of Information Industry Services, which lays the basis for further policies and regulations. During the National People's Congress in March 2015, Lee Keqiang announced a new concept of "Internet Plus" for China's 2015 Government Work Report, which involves the holistic integration of citizen life, with new technologies like big data and cloud computing, e-commerce, etc.