THE INDIAN CLOUD REVOLUTION
CII believes that Cloud Computing as a disruptive technology and business model offers an accelerator approach for economic growth as it connects people to data, information and computing resources anywhere and anytime.

Globally, the adoption of cloud has increased over the years, and growing at a rapid pace. India, as a nation of more than a billion, understands the importance and challenge of connecting the ‘Bottom of the Pyramid’. Cloud can drive the inclusive growth agenda by providing platform to scale the reach of education, healthcare, financial services, entrepreneurship and governance among other areas.

Indian Government has started using Cloud to benefit masses and launched massive projects like Aadhar, National Population Register, National Rural Heath Mission, M-NREGA. While more technology is being adopted by businesses and Government, there is a huge potential to harness the potential of the Cloud for percolating the benefits of scale, efficiency and low cost to all communities and sections of society.

This whitepaper evaluates the opportunities and challenges that is faced in India’s roadmap for cloud adoption. Through this, we seek more clarity in policies on data-sharing and security to expedite the move to cloud in the interest of all.

Government, as one of the biggest users of the cloud is expected to play the role of catalyst for the emergence of the technology. It is not about rallying for India to be a prominent cloud user but also to be one of the leading players of cloud in terms of services offered. We seek indigenous capacity building and creating an ecosystem for cloud computing that will spur a new wave of job creation and economic prosperity.
Internet had increased productivity manifold, created new businesses and also created new business models. All these happened in the 2nd half of the 20th century. There is a need to continue developing and adopting new innovations that give boost to the proliferation of communication and networks to reach and rectify the challenges the world faces today. As we realize the need for an inter-disciplinary approach to solve real-world problems in the areas of healthcare, sustainability, education and poverty, Cloud computing comes across as a unique platform for developing and harnessing most cost-efficient solutions having far-reaching implications on technologies, business environment and people themselves.

Services to citizens such as banking, insurance, healthcare, education and governance are increasingly moving to the cloud, mainly because it is cheaper, had infinite storage capacities and ensures mobility. But the main challenge is to come out with the right policies enabling cloud computing in India, with a regulatory framework to be able to offer citizen services. The National Telecom Policy 2012 is one such step in right direction.

Indian IT industry had established a global model that was viable and offered better services to IT companies across the world but Indian companies are yet to take to cloud computing in a big way. The whitepaper examines the role of Government as a user and enabler and facilitates the Government to come out and review the right policies to build the confidence of small and large entrepreneurs, private or public to adopt cloud. This will also require bringing clarity on issues like data ownership and security that are core for adoption of cloud.

This whitepaper is an effort to understand the implications of this disruptive technology and harness it for the good of the nation which can push growth and revolutionize the reach of opportunities and services to the Indian citizen.
The Indian Cloud Revolution
Contents

1 The Indian Cloud Revolution 01
2 Institutional challenges 05
3 Law enforcement and investigative aids 11
4 Data Security and Privacy 15
5 Migration to the Cloud - Government and Industry 19
6 Cloud Ecosystem 25
7 Developmental opportunities presented by the Cloud 33
8 Conceptual Framework for a Cloud Policy in India 43
9 Conclusion 51
The Indian Cloud Revolution
The India Vision 2020 document by the Planning Commission of India mandates that our vision of India’s future should be both comprehensive and harmonious; it envisages that:

“By 2020, the people of India will be more numerous, better educated, healthier and more prosperous than any time in our long history”

The document also acknowledges that “A powerful set of catalytic forces is accelerating the speed of social change throughout the world. They include a rapid rise in levels of education, high rates of technological innovation and application, ever faster and cheaper communication that dissolves physical and social barriers both within countries and internationally, greater availability and easier access to information, and the further opening up of global markets … Technology, organization, information, education and productive skills will, therefore, play a critically decisive role in governing the future course of development.”

If there is one technological change which can have an all encompassing effect on all the above mentioned factors – it is the Cloud. Enabled by Information Technologies and riding on the back of telecommunications network, the Cloud can herald a myriad of solutions ranging from enabling tele-medicine, setting up remote-classrooms, creating national citizen health and skills databases and creating a new Cloud based services industry for generating employment.

Specifically, Cloud based services can be leveraged by the Government to launch new e-Governance initiatives quicker and with lower overhead costs. A common Cloud platform will also enable local Governments and other public agencies to adopt e-Governance for better citizen services, without requiring the setting up of significant IT infrastructure.

The Cloud also presents an opportunity for India’s Information Technology (IT) & IT Enabled Services (ITES) sector by opening up a new avenue of providing Cloud based services to global organizations ranging from Software as a Service (SaaS) based application services, providing remote testing and prototyping services in addition to remote application hosting services such as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

However, on one hand where Cloud promises to change the way Indian businesses and Government leverage technology to their benefit, on the other hand it also presents significant challenges relating to security and privacy of information.

A comprehensive policy for adoption of Cloud in India is thus the need of the hour. It is important for all stakeholders in India to understand the implications of this disruptive technology and harness it for the good of the nation.

The National Telecom Policy 2012 (NTP-2012) also acknowledges this and aims 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.”

In this whitepaper, we first seek to understand the importance of Cloud to India. We thereafter try to assess the impact of the Cloud on two critical developmental areas for India, Healthcare and Education. Finally, we examine the role the Government should play in enabling a Cloud revolution both as a user and as an enabler of the Cloud and the regulatory framework on which a Cloud policy in India should be based.

---

Characteristics of the Cloud

In order to understand the components and ecosystem which are termed as Cloud, it is important to understand Cloud. In simple terms Cloud refers to:

In order for any offering to be termed as a Cloud it should have the following characteristics:

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>On-Demand Self-Service</th>
<th>Internet Accessibility</th>
<th>Pooled Resources</th>
<th>Elastic Capacity</th>
<th>Usage-Based Billing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: KPMG India Cloud Publication: Changing the ecosystem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cloud computing is characterized by its fundamentally flexible nature, which stands in stark contrast to the rigidity of systems tied to on-site, physical IT infrastructure. This flexibility is the source of many of the potential strengths and weaknesses of Cloud computing, and as such it merits a fuller discussion. From the perspective of the Cloud’s architecture, flexibility can be seen in three main areas: the potentially dispersed and far-flung geo-location of data servers and storage enabled by virtualization and remote access; the rapid elasticity and scalability enabled by the on-demand nature of Cloud computing resources; and the broad resource pooling in large-scale data centers, which allows for greater economies of scale and more efficient targeting of resources.

So while the technological basis for Cloud computing is not new, the capability of the technology is. The features of Cloud computing are new dimensions and opportunities of an existing technology.

Geo-location

The fundamental economics of Cloud computing depends on the ability of cloud service provider (CSP) to operate large and efficient data centers in order to service a large customer base. In order to maximize on the economic efficiency, many cloud vendors have created a geographically distributed data center strategy.

Data centers are typically located strategically across the world to service a global customer base. The location of data center is dependent on many factors such as geographic proximity to customer base, operational cost structures, legal and regulatory environment, political and safety concerns, among others. These data centers are typically connected over a network to move data between data centers for backup, load balancing and disaster recovery purposes, among others. Cloud service providers can also routinely transfer requisite data to international third party sub-processors for functions such as technical support, etc.

Cloud computing in its modern form developed out of efforts by large web-based companies to capitalize on the use of their large-scale data center capacities for public as well as internal storage and processing. As such, the initial centers were largely concentrated in the United States—particularly Texas, California, Oregon, Washington, and Virginia—in areas where land, electricity, taxes and other overhead costs made...
operating the centers relatively cheap. Most Cloud-specific data centers continue to be concentrated in North America and Europe, with some recent expansion into East Asia (especially Singapore).

This geographical concentration does not, however, technologically stymie international expansion. Because servers and processes are virtualized (meaning that the function performed is logically separated from the physical infrastructure) and based on network access, a server in a state in the United States can (and does) serve clients all over the world. In fact, because server resources are dynamically reassigned to users based on demand, the user often has no control or knowledge about the actual geo-location of the physical infrastructure providing or supporting the service. In part because it has not been necessary, and in part out of proprietary concerns, large Cloud service providers (CSPs) have been notoriously tight-lipped about the location and characteristics of their data centers.

Nonetheless, there has been a slow but growing push towards offering location specific services, which allow customers to choose where their data is stored and how it is delivered. One such CSP, for example, uses content delivery network nodes in over 17 countries worldwide, which facilitates data transfer to end users to end users on a more localized scale. This push has been driven in part by technology, and in part by the security, privacy, and compliance concerns of both private users and government regulators of the Cloud, discussed in more detail in a later section.3

Still, the technological underpinnings of the Cloud allow an IT team to decouple the traditional ‘stack’ of resources so that the infrastructure, platform or software offered is separate from the physical architecture. This allows customers flexibility in choosing service providers and (in theory) the location of data storage and processing, in addition to the logistical benefits of scalability and resource pooling outlined below.

Rapid elasticity and scalability

One of the difficulties associated with traditional IT architecture is that the combination of physical server requirements and uneven demand levels leads to inevitable waste of resources. This can happen either due to over-utilization—where servers cannot meet the needs of spikes in demand, resulting in slow response times and an inability to process all requests—or under-utilization—where servers purchased to accommodate spikes in demand sit dormant and unused during long stretches of normal user activity.

By contrast, the pay-as-you-go, on-demand functionality of the Cloud allows users to match their usage (and therefore costs) to demand. This is possible again because of the technological opportunities provided by virtualization. The technology involves services spread out over a vast physical architecture, sometimes even encompassing more than one data center. Virtual machines increase the available storage size, and because they are abstracted from the physical architecture, the lag time between order and deployment is a matter of minutes (compared with the weeks required for delivery and installation of new physical servers).

Again, because of the vast resources provided by large data centers and virtualized services, there are relatively few limits on the extent to which users can scale their usage. With advances in the ability to accurately and precisely model demand, this capability allows users to finely calibrate their usage requirements to meet the normal spikes and dips in demand throughout the day. The result is that even with a premium for Cloud services which is higher than the amortized purchase price of a physical server, the scalability of Cloud architecture still offers the possibility for significant savings due to the reduction and near-elimination of wasted IT resources.

Broad resource pooling

Closely linked with the scalable capacity of Cloud services is the potential for broad resource pooling. This again is linked to the way that services are decoupled from and run out of large data centers. The virtualization of IT processes allows multiple clients to operate on the same physical network on a ‘multi-tenancy’ basis. Because certain processes use some IT resources (such as CPU, memory, etc.) more heavily than others, virtualization allows the physical infrastructure to be utilized in a way that optimizes its technological capacity. Again, this feature presents an opportunity for significant savings under the pay-as-you-go cost structure.

The vast scale of modern data centers also allows for economies of scale in terms of research, development, and reinvestment. Whereas companies with in-house IT technologies were hampered by the costs and delays associated with constant upgrades and reinstallations, the large data centers can afford to stay on the cutting edge of technological developments.

Finally, the uniformity provided by large data centers means that certain functions can be centralized and harmonized across multiple institutional users. This is true for data security (although centralization has its associated risks as well), where the increased capacity of the data center allows for more sophisticated and resource-heavy protection against attacks. Institutional units spread across a large geographic area can also use the same Cloud architecture to harmonize access controls, share data and resources, and utilize uniform applications and services. This too represents a potentially fundamental break from the traditional, silo-based (i.e. isolated) approach to data and IT resources.

3 http://www.cdnfinder.com/find_cdn?types%5B%5D=Pay-As-You-Go+CDN+Providers&types%5B%5D=CDN+Providers
Despite the many potential advantages offered by the Cloud, this does not lead to the inexorable conclusion of its superiority as an IT model for businesses and governments. As the Federal Risk and Authorization Management Program (FedRAMP) in the United States notes:1 “The decision to embrace Cloud computing technology is a risk-based decision, not a technology-based decision.” In addition to the data security and privacy risks inherent in Cloud technology, its characteristics and features also elicit a number of institutional challenges and considerations that must be taken into account. These include questions regarding data sovereignty and jurisdiction, the licensing and registration requirements imposed on CSPs and data centers, the effect of corporate business strategy on the relative utility of Cloud computing, the loss of governance resulting from outsourcing IT functions to the Cloud, and supply chain guarantees necessitated by the multiplicity of actors in the Cloud model.

To this extent, this report does not represent a novel effort. The U.S. government has launched a ‘Cloud First’ policy, the Australian government has already developed a Cloud computing strategy, the EU is engaging with stakeholders to develop its own Cloud policy.2 The rubrics below aim to guide the Indian government’s policy on Cloud computing.

### Data subject and jurisdiction

The question of sovereignty and jurisdiction over data in the Cloud has been a source of frequent and persistent tension between providers and regulators throughout the world. Generally speaking, the norm has been for the local law of the place of data storage to apply. However, governments may exert pressure via licensing restrictions or operational restrictions on intermediate service providers. Furthermore, compliance with the local laws of the place of operation or storage, such as the PATRIOT Act in the United States, may conflict with obligations imposed on the Cloud user or data provider in their home jurisdiction, such as the EU privacy laws. Similarly, compliance with the new rules under the Information Technology Act, 2000, as amended (the IT Act), that enables providers of sensitive information to verify their information, may become onerous given that data maybe held in fragmented corners of the Cloud.2

These issues are still largely unresolved, but some progress has been made. One area of growth has been the development of bi- and multi-lateral privacy frameworks, such as the Safe Harbor Framework developed by the EU and the United States to govern the transfer and storage of data between those two entities in order to comply with the EU Directive on the protection of personal data. The Framework has become a major compliance standard for company privacy policies in the United States and elsewhere.

The problems associated with jurisdictional conflicts and the global nature of Cloud architecture has also led to calls for an international regulatory body or a treaty aimed at harmonizing regulations across countries. The OECD is working on developing international standards for security and privacy which could provide the basis for a more harmonized regulation across the globe. However, calls in the UN for an international regulatory body in the wake of the Wikileaks scandal have so far been rejected by Australia, other western governments, and business leaders, who say that the current Internet Governance Forum (IGF)— whose recommendations are nonbinding—allows for more input from civil society.2

---

1 [http://www.gsa.gov/portal/category/102371](http://www.gsa.gov/portal/category/102371)
2 Amarchand Mangaldas analysis
The jurisdictional problems associated with a lack of harmonized regulations are compounded by the global, physically unfettered nature of Cloud computing. Data storage and processing tend to be fragmented and may even be spread across multiple Clouds in different locations. This creates serious difficulties in terms of tracing problems as well as determining which regulations govern that data, as noted in a recent Brookings Institution forum on Cloud computing. Furthermore, the dynamic nature of Cloud computing means that data is more often in transit, both within and away from the Cloud provider, resulting in multiple jurisdictional claims on the same information.

The response of some countries has been to exploit the advantages posed by data storage, or, lacking those benefits, to attempt to force network traffic or storage within their countries. The PATRIOT Act in the United States allows federal security agencies to directly utilize Cloud provider’s infrastructure for wiretapping and surveillance purposes. In an attempt to strengthen government control over the internet, Cambodia is implementing a government-controlled, national exchange point through which all internet service providers (ISP) must go in order to access the national market. This allows it to centralize and regulate internet traffic and content, and could be extended to Cloud services as well. However, control over the physical data still largely depends on the locus of storage, which has led to recent efforts to force companies to open data centers within the jurisdiction of their operation. The IGF notes, however, that such attempts may ultimately hamper data flows in and out of the country (as well as the innovation that they spur), highlighting the trade-off between the benefits and risks posed by the Cloud.

The location of the data center does not always necessarily determine the applicable laws; there could be additional factors such as the principal place of business.

**Location, Licensing and Registration**

Despite the obvious jurisdictional benefits created by a Cloud provider’s decision to process and store data within the country it operates, India hosts a far smaller number of data centers than its size and technological human capital might suggest. One industry website lists 36 privately-owned data centers available in India, which puts it on par with Italy (33) and Switzerland (36) but far behind other developed countries such as the U.K. (144), Germany (127) and France (96). The United States is the clear industry leader with well over 1,000 servers listed. A similar trend emerges for Cloud-specific servers, with the vast majority in the United States and the rest concentrated in Europe, with only an isolated few in the developing world. Despite this current distribution, aforementioned concerns about security, jurisdiction, and content delivery are driving a push toward a more globalized Cloud infrastructure. Furthermore, the cost drivers of large data centers drivers and new emphasis on greener, energy-efficient technologies indicate that the developing market can still be a leader. The question, then, is what the proper regulatory environment is and should be for service providers and data center operators who consider India as a location.

The newly created Data Centre Risk Index lists a number of risk factors, including ease of doing business and corporation tax, that potentially affect data center operations, and ranks countries according to this metric. The United States, Canada and Germany scored highest, while both India and China scored poorly despite their size, natural resources and economic strength. The major obstacle to a better rating, according to one author of the index, is regulation: “Despite their status as engines of global growth, China and India score poorly as a result of strict foreign ownership regulations and other barriers to investments.” Also related to the issue of data center risks are factors associated with operational costs, including environmental regulations, the quality and availability of energy and utilities infrastructure (including water for cooling), and inflation.

As mentioned previously, one primary motivation behind companies’ unwillingness to disclose details about their data centers is a concern for their proprietary information and a desire to keep innovations and developments within the country. In the context of Cloud-related FDI, this concern naturally relates to a hesitation about transfer of technology and other side-effects of transnational investment, providing a further barrier to growth. There are also regulatory compliance requirements such as under the EU data protection directive that restricts the transfer of data to third countries that ensure an adequate level of protection for the transferred data. Similarly, the new rules under the IT Act on data security and privacy require that transfer of sensitive information may only occur when the transferee provides the same level of protection as the transferor. The institutional challenge then is to determine when such data on Clouds will constitute a transfer under extant laws and how the transferee’s jurisdiction will be determined. International agreements in this regard, such as the Safe Harbor Framework will also have to be taken into account in this determination. These laws and the ultimate conclusion on ‘transfer’ of data to Clouds will be instrumental in determining location.

With regards to licensing for operations in the country, companies are likely to be sensitive to the interplay between compliance requirements within India and their other obligations to customers and regulatory authorities in their own jurisdictions. The decision of how to classify and define liability for CSPs (e.g. as intermediaries under the IT Act) also has an impact, and will likely depend on the type of service being offered.
**Effect of corporate business strategy**

While Cloud computing represents an area of potential growth, it can also be disruptive of an organization’s strategy and infrastructure. Corporations’ decisions in terms of acceptable levels of risk, the relative importance of transparency, cost efficiency, and security are all interdependent determinants in transition to the Cloud.

Moreover, transitioning to the Cloud also necessitates involving the IT department in corporate strategy discussions to a far greater extent than in the traditional model, in which the IT department responded to the needs of predetermined applications instead of helping to shape a holistic strategy on how to conduct business. The strategy must be holistic because the same technological flexibility that lends Cloud computing its valuable economies of scale also means that different departments are more interconnected and vulnerable to each other. A more connected business environment needs governance, risk and compliance solutions that can protect all elements of the enterprise. Other aspects of larger corporate strategy, such as responding to clients’ transparency demands or lessening the organization’s environmental impact, are also directly impacted by migration to the Cloud.

Furthermore, Cloud computing has the potential to be disruptive in terms of industry as well as intra-organizational dynamics. Software industry observers note that the previously dominant corporate giants are under increasing pressure from a much broader range of competitors including from global outsourcing companies. This newly competitive environment—particularly following the global recession—necessarily affects strategy calculations and has already resulted in renewed emphasis on transparency, flexible provisioning, and cost-effectiveness.

These considerations not only affect whether or not an organization will transition at all, but also which services and deployment model it will employ, as each carries different opportunities and challenges. For example, SMEs with fewer existing investments may find that a wholesale transition to rented IT resources in the Cloud are worthwhile even in the short term, while larger organizations with more extensive infrastructure may require a hybrid internal/external system, utilizing the Cloud to provide extra computing resources to meet spikes in demand. Weighing the trade-offs between outsourcing and growing the Cloud internally are a key area in which strategy dictates an organization’s approach to the Cloud.

In addition, Cloud computing will affect an entity’s manner of conducting its business. Use of the Cloud will mean an entirely new way of doing business resulting in new back to back contracts with CSPs, clients etc; new supply chain arrangements which have been discussed later and new guarantees to ensure control over their operations on the Cloud. So Cloud computing presents not just the task of rethinking internal corporate policies but also industry-wide operational policies. This of course will have far reaching implications on the wider economy as well. Some estimates suggest that Cloud computing will create 100,000 jobs in India as against 10,000 as of now.⁴

---

⁴ Amarchand Mangaldas analysis
Financial intermediaries’ interplay

Banks, credit card companies, and other financial intermediaries represent an area of relatively slow growth in Cloud computing, primarily because the security risks of Cloud-based transactions are particularly unacceptable to such institutions. Most banks are still not using any form of Cloud, and those that are, tend to do so in controlled test environments using nonessential data. From a security standpoint, the dispersed nature of public and hybrid Clouds means that financial institutions are unable to gain a clear picture of the storage location and transit routes of their data. This lack of certainty is enough to keep financial institutions from migrating to the Cloud, regardless of the actual security controls that CSPs have in place. As one executive explained: “An infrastructure that you know something about is inherently less risky than one you don’t know anything about…But that doesn’t mean a public Cloud is less secure than a private data center environment. It just means that you’ll always have less information about that environment from which to make decisions about security”.

Moreover, the regulatory and liability framework facing banks has often led them to shy away from any steps to outsourcing any control over their information. Cloud providers’ Service Level Agreements (SLAs) often provide inadequate protection in terms of liability, and even if they did, banks—not service providers—would be ultimately liable for loss suffered by their customers. The uncertainty of the regulatory framework provides a further obstacle. While banks and other financial institutions are heavily regulated, CSP are not—at least so far—and this uncertainty leads risk-averse financial players to shy away from outsourcing decisions that could lead them into conflict with regulations that were not written with Cloud computing technology in mind.

Cloud-based credit card transactions are similarly stymied by the global regulatory environment. The Payment Card Industry’s (PCI) Data Security Standard—used by the five largest credit card companies as the basis for their security policies—requires that secure transactions take place on logically separated computing infrastructure. The latest version of the standard, released at the beginning of 2011, makes no mention of Cloud computing or virtualization technologies, indicating a wait-and-see approach to allow for further progress in security. So far the qualified security assessors have been unwilling to interpret the rules to allow Cloud-based transactions. Until that happens, web-based financial transactions will necessarily remain tethered to the more transparent, secure physical hardware utilized by credit card companies and vendors.

There is, however, some evidence that other financial institutions are willing to transition some operations to the Cloud, even if they do not support a full-scale migration as intermediaries. The new emphasis on efficiency and

---

5 Amarchand Mangaldas analysis
transparency in corporate treasury departments has created a new, albeit largely untapped, market for banks to provide holistic, Cloud-based business solutions. Additionally, certain stock exchanges abroad have approved the use of a private Cloud to host broking and trading software, which run and store some of the most sensitive transactions and information on the exchange. This represents a significant step forward in the trust placed on virtualized technology and computing, although analysts agree that a move to a public Cloud remains a long way off.

**Loss of governance**

The relative ease and low barriers to entry of Cloud computing is a double-edged sword in terms of governance. Whereas companies with in-house infrastructure could previously control each aspect of the IT stack, from physical security of the server or hard disk to the access and authentication controls on individual devices on the network, outsourcing services to CSPs necessarily involves a loss of some of this direct oversight.

This problem is compounded by the fact that in-house firewalls and authentication systems tend to be configured to perform on the structures for which they were created, making them ill-suited to the dynamic and fluid nature of resources on the Cloud. This necessitates a retooling of internal security mechanisms and access controls so that they match and are compatible with the new infrastructure. Furthermore, new controls and measures may be necessary depending on the type of Cloud delivery mechanism chosen. For example, multi-tenant situations in larger data center facilities can make users vulnerable to unauthorized access by their co-tenants. Co-tenants’ misdeeds and subsequent investigations may also result in reputational damage and availability outages caused by police seizure of physical hardware. It should be noted, however, that other Cloud delivery options, such as a private Cloud, allow users to mitigate some of the governance issues. This carries its own drawbacks in terms of increased costs and foregone economies of scale.

Ceding control to the Cloud provider also matters in terms of liability and responsibility for various aspects of security. Current SLA are often from contracts developed by service providers and are tilted heavily in their favor. Auditing Cloud provider performance to ensure that contractual security and privacy standards are met is also difficult due to the fragmented nature of data storage.  

The lack of transparency combined with unfavorable allocation of risk creates the potential for significant difficulties for organizations migrating essential services or sensitive information to the Cloud.

A report from the European Network and Information Security Agency (ENISA) also notes that, in the current state of Cloud computing technology, organizations can become dependent on a single Cloud provider—particularly if the data is not portable or interoperable between different systems—and lose the knowledge and expertise associated with IT management. This problem of data or vendor lock-in is one of the chief obstacles for larger enterprises and governmental agencies’ transition.

However, these difficulties are an area of constant innovation. Developments such as industry standards for application programming interfaces, negotiation of SLAs with CSPs, and Cloud-appropriate auditing practices and procedures offer a chance to mitigate the issues raised in this section, although much more work remains to be done. In the short term, governance-related risks continue to play a large role in the decision to migrate to the Cloud, particularly where sensitive data is concerned.

**Supply chain guarantees**

The difficulties associated with auditing and a fragmented storage system also have an effect on the chain of suppliers of Cloud services. Virtualized IT processes can interact such that multiple intermediary companies provide Cloud-based services to each other—whether infrastructure, platforms or software as a service—as well as the end-user. However, the flexibility offered by this virtualized chain of supply opens the system to vulnerabilities at multiple stages. Depending on the placement of the service purchased by the end user in the stack, their provider may be more or less dependent on a contractor’s underlying infrastructure. For example, the relationship between client and provider of IaaS controls many links in the chain than a subscriber to SaaS, which in turn might be dependent on multiple third party suppliers.

This technological separation is also reflected in the lack of contractual relationship between the end user and infrastructure provider. This is significant because the current relative lack of regulation means that guarantees regarding data security, privacy, authentication standards, etc. are left to the terms of the contractual relationship. The user must therefore ensure that both the Cloud provider and its suppliers maintain the requisite levels of controls. Enforcement of these provisions, however, is complicated by the fact that the interconnectedness of Cloud operations makes apportioning blame for subsequent failures difficult. Moreover, as the ENISA report points out, providers often change their contractors frequently, so a list of specific, real-time third party contributors is hard to produce. Instead, ENISA suggests that CSPs be forced to disclose which functions they outsource and which they perform in-house.

---

6 Amarchand Mangaldas analysis
Law enforcement agencies’ ability to collect and analyze personal and electronic data has previously been relatively limited to traditional wiretapping of telecommunications lines or efforts to bug or confiscate personal computers or business network servers. However, the simultaneous centralization and fragmentation of data represented by Cloud computing represents a new set of opportunities and challenges for law enforcement. On the one hand, Cloud-based communications technology allowed the FBI to install software onto mafia members’ phones that turned on the microphone and essentially converted the phone into a ‘roving bug’ even when it appeared to be turned off. Some Cloud communications providers have also allegedly given the U.S. National Security Administration (NSA) permanent access to their backbone infrastructure, which allows the NSA to make internal decisions about when and whom to wiretap without seeking the providers’ specific consent or cooperation. On the other hand, jurisdictional difficulties, recalcitrance on the part of some CSPs, and other logistical or forensic difficulties comprise continuing obstacles to investigative and regulatory efforts.

**Locus and enforcement**

The geo-location of data storage and processing has important implications for end-user security as well as data sovereignty and jurisdiction, and the same is true for law enforcement efforts. Although efforts have been made to impose disclosure requirements on CSPs, lack of control over physical information stored outside the jurisdiction has illustrated the limits of the coercive authority the state is able to wield over foreign service providers. This has resulted in a push to require providers to operate out of local data centers, to which the domestic police force would have physical access. Certainly, some countries have been able to obtain concessions: Saudi Arabia notably induced a company to build data centers in the country so that local authorities could intercept messages at will, while other companies have agreed to comply with Chinese censoring requirements in order to operate in that country. Still, the benefits offered by local data storage are aptly illustrated by the advantages the United States security apparatus enjoys due to the presence of so many data centers and the broad powers conferred on the federal government by the PATRIOT Act.

It should be noted, however, that access to a given physical server does not necessarily lead to usable information for law enforcement, and confiscation also has spillover and chilling effects on co-tenants. First, the fragmented nature of data storage means that information may be physically spread out and must be reassembled at a different level of abstraction in the Cloud before it can be usable. This therefore requires the cooperation of the Cloud provider in the reassembly and delivery of the usable data. Second, data may be encrypted, which can require the consent of the encryption key holder (often the information provider) or further cooperation with the Cloud provider in order to crack the key and gain access. Finally, confiscation and analysis of physical hardware also harms innocent co-tenants whose information is stored on the network. In response to these issues, Cloud computing expert Prof. Michael Nelson has emphasized that, for the sake of certainty for providers and users, governments should be transparent about their policies, regulations and self-imposed limitations with regard to security and privacy.

---

1 Amarchand Mangaldas analysis
Ownership of data

Questions regarding the ownership of data are, in the absence of comprehensive regulations, largely left to contractual provisions in SLAs. Apart from large, sophisticated parties who can negotiate more favorable terms, the current state of affairs is problematic for several reasons. Most SLAs continue to be from contracts, many of which contain provisions about the right of service providers to disclose and use information and impose limitations on users’ ability to bring proprietary-based claims against the Cloud provider. The standards attached to ownership also depend in part on the type of information being handled. Agreements often do not differentiate or sufficiently define non-personal, personal, sensitive, and proprietary information, although ownership standards could and should apply differently to these different types.

In the United States, the legal implications of Cloud computing for data ownership are dominated by the third party principle, which excludes information transferred to third parties from Fourth Amendment protections against illegal search and seizure. This, in turn, has important implications for the level of official action necessary to induce third party service providers to disclose information. Instead of an official, judge-approved warrant, a simple subpoena often suffices. This has led to a push to reinterpret or rewrite data ownership and privacy laws to reflect the new realities of modern computing, but so far data in the Cloud remains relatively detached from the protections normally offered to ‘owners’ of information.

The uncertainties surrounding ownership highlight the need for government leadership in terms of regulation in the medium and long term, and for vigilant scrutiny and crafting of standard contractual provisions for the industry in the short term.

Data retention

Particularly for companies and users moving sensitive information to the Cloud, data ownership and security concerns during the life of the contract with the Cloud provider are only part of the issue. This issue is compounded with the peculiarities of the nature of activities undertaken by an enterprise. Typically, data retention obligations of an enterprise are based on the nature of activity undertaken by it. Thus, it may not always be a feasible approach to make regulations around data retention applicable on cloud providers. For eg, data retention obligations of a bank are very different from retention obligations of a courier agency. Also, customers may want to be and indeed be reassured that their information is completely erased from the provider’s servers. In fact, EU privacy laws mandate this ‘right to be forgotten’. In response to pressure from privacy advocates, some service providers now enforce an 18 month data retention policy, after which data is anonymized (i.e. wiped of indicators that could lead to the identification of the individual). However, the technologies underlying Cloud computing make this difficult to prove, much in the same way that they frustrate traditional auditing and forensic techniques. Also it may not be a judicious approach to shift the burden of retention on to CSPs. It may be a more efficient outcome to mandate a data retention policy as part of sectoral regulations as opposed to having a standardized retention regulation for all data residing on Cloud computing infrastructure.

Conversely, the frequency with which data is overwritten also creates a forensics issue for internal responses to security breaches as well as external probes by law enforcement and regulators. This characteristic may make it difficult for providers to comply with regulations or court orders mandating that providers store certain types of information for a certain length of time (as was the case in a recent investigation of copyright violators who used peer-to-peer software).

In other respects, however, Cloud computing allows users to capitalize on the greater storage capacity by providing more robust, built-in redundancies in the architecture. This insulates the data and services from mechanical failure, seizure, or other problems associated with a single piece of physical hardware. This redundancy can even be built into the design of entire data center locations, such as a pair of Cisco facilities in Texas which serve as “active-active” mirrors of each other, automatically updating a given server in one whenever its pair in the other facility changes.

Information requests

In terms of the efficacy information requests, much depends on the location of providers and the breadth of authority and bargaining power enjoyed by local law enforcement. Most major CSPs now have full-time legal compliance departments to deal with requests for information by law enforcement. Depending on the type of service and the contractual provisions the provider has with its users, it may be more or less willing to share that information with inquisitive governments. This cooperation can be crucial when the information needs reassembling or decryption before being useful. While this process has tended to be shrouded in secrecy, there are emerging transparency measures such as published reports in which it lists the number of requests and rates of compliance by country over a six-month period. While it still does not list the details of the requests or the reasons for its refusal or acquiescence, the report does offer a glimpse into the general global trend of requests as well as which tend to be more or less successful.

All this relates to data in storage from different providers. However, Cloud computing also involves frequent transmission of data, allowing law enforcement agencies (as well as hackers) an additional opportunity to intercept or put pressure on intermediaries who transfer the said information.

2 Amarchand Mangaldas analysis
Content for many applications providing platforms for public sharing of documents and social networking sites, remains largely unencrypted and available for immediate inspection. However, other sources of raw data may not be useful due to the widespread use of encryption technologies for certain types of services. These controls are mandated in certain sectors, such as banking and e-commerce, and are becoming more common in others. Governments have undertaken two main responses to this problem. The first is to obtain the encryption key, which is sometimes held by the Cloud provider as well as the user as per the terms of service. This can also be done with the key holder’s consent or—in the case of criminal operations—with more traditional methods aimed at extracting the information from the suspect’s keystrokes or hard drive logs.

The second possible response is to force CSPs to build in vulnerability in their programming code (known as a ‘back door’) that allows government authorities to access the information—regardless of encryption—on demand. In theory, this would then be utilized only after obtaining proper legal authority, although privacy advocates criticize the policy’s potential for abuse by government agencies and vulnerability to exploitation by hackers. Despite these concerns, the U.S. proposed a law which would have required communications services to maintain a way to unscramble encrypted messages, ensured that foreign based providers keep an office in the United States capable of performing intercepts, and forced peer-to-peer software developers to redesign their service to allow interception.

While this law has not been passed (and likely will not in the near future), the PATRIOT Act does enable U.S. law enforcement agencies to compel the production of information via National Security Letters issued to carriers including CSPs. In addition to providing invasive access to data stored on company servers, the Letters are accompanied by a ‘gag rule’, meaning that the companies are barred from informing their customers that the wiretap or disclosure has taken place. Though the access to the information by the US law enforcement agencies under the PATRIOT Act works within the framework of the 4th Amendment in the US and also under appropriate oversight, it still poses a risk especially for the sensitive data.3

### Content regulation

All governments, albeit to varying degrees, attempt to regulate the content of the internet to some extent and hold violators of those regulations liable. In the context of Cloud computing, several challenges emerge in terms of regulating and blocking the content itself as well as holding individuals and companies liable for the offending material. To begin with, content regulation is warranted only for those medium carrying mass communication, such as the internet. Cloud computing infrastructure on the other hand is not meant to be an instrument for mass communication, it is a tool that may be used for internal operations of an organization. Therefore, content regulation, strictly speaking should be administered on any specific enterprise depending upon the nature of activity undertaken by it and not by the mere fact that it uses cloud computing infrastructure.

In light of this, it is noteworthy that traditional content blocking has channeled through regulating ISPs, and this is unlikely to change. In fact, in recent years countries such as Cambodia and Australia have instituted comprehensive measures to combat material deemed to be harmful by those governments—an ISP exchange point in Cambodia and a national filter in Australia. These efforts are used to clamp down on a variety of content, from pornography to dissidence.3 However, the challenge posed by the Cloud relates to the dispersion of data and the possibility that a regulator may take the view that content regulation may be applicable to Cloud-hosted VPN clients, which can hide the location of the computer and make enforcement more difficult.

With respect to liability, the question is the extent to which the Cloud provider, client and end user are individually responsible for data transferred to and from the Cloud. As a corollary, deciding how to classify Cloud service providers is also important. Last year, for example, an Italian court found executives of a leading service provider liable for a video uploaded to their website based on a decision to classify them as content providers, rather than simple service providers—despite the fact that the company in question removed the video once alerted. While the case is on appeal, it nonetheless highlights the importance of clear and consistent regulations of content and all the key players in the Cloud.3 This effort is made more difficult when CSPs do not conduct significant business operations within the country, making jurisdictional claims more difficult.

---

3 Amarchand Mangaldas analysis
Data Security and Privacy

Perhaps the most consistent concerns raised by private and public sectors alike with respect to the Cloud are the risks it poses for security and privacy. However, its proponents argue that there are also gains to be had—even in security and privacy—from migrating to the Cloud, which may offset the risks for some users. In both areas, the challenges posed by the Cloud arise out of the same characteristics that make it an attractive option for many organizations.

Encryption and data security

One of the most fundamental problems facing organizations who want to migrate to the Cloud is how to protect their data from theft and unauthorized access in an environment in which it is frequently in transit and—in the case of multi-tenant environments—stored on physical hardware that is shared with other users. Encryption is one of the key tools used by organizations to protect this information. Moreover, new technologies strengthen the controls around data even while it is in use: reverse proxies, for example, can allow authenticated, individual access to data on a Cloud server while maintaining its encrypted status to the rest of the world.

Despite the gains in encryption security, vulnerabilities still exist. One is the presence of government-mandated back doors, discussed in the previous section. While they can serve a lawful purpose, their presence does represent a vulnerability that may be exploited by hackers searching for a weak link in the encryption code. More commonly, however, encryption is overcome by more traditional means, namely by obtaining the encryption key. This is the case because despite all the advances made in encryption technology, keys still generally rest in the hands of individuals and are open to theft by vulnerabilities in web browsers, personal computers, etc.

This example also highlights the general vulnerabilities of the Cloud. While reliance on a network allows for greater flexibility and scalability, it also creates a single point of attack for hackers wishing to gain access to data. Moreover, the flexibility offered to end users allows them to access Cloud services from personal devices as well, which may have weaker security controls. If this potential vulnerability is not addressed, the entire network may be open to attack.

Finally, the nature of data storage and transfer in the Cloud simply offers more opportunities for hackers and other cyber criminals to attempt to gain access. A summary of Cloud computing challenges by ENISA notes that multi-tenant storage in hybrid or public Cloud creates a risk of unauthorized access by co-tenants. The report also notes that the increased rate of data transit—both between the Cloud provider and the user and within the Cloud itself—opens data to the risk of interception. Finally, the report cautions that (at least with the current state of technology) users often end up dependent on a single Cloud provider (known as lock-in). This not only makes users particularly vulnerable to attacks on that provider, but it also increases the risk and potential damage done by an inside job, i.e., unauthorized access or theft by a disgruntled or dishonest Cloud provider employee.

Addressing vulnerabilities

The challenges posed above necessitate a coordinated response from both users and providers. Indeed, this is one of the greatest challenges posed by Cloud computing: by outsourcing some services, users necessarily outsource some security as well. The response to the vulnerabilities inherent in Cloud computing therefore encompasses purely security-focused controls as well as transparency, management and coordination efforts with CSPs to ensure that security controls remain adequate.

Central to any attempt to address vulnerabilities in the Cloud are the new technologies and innovations in security controls. In this respect, the Cloud can be an asset as well as a liability. Many technologies now use the greater, scalable computing potential offered by the Cloud to offer more powerful filtration services and protections against attacks. Many web content blocking systems use Cloud-based filtration technologies. One such use of the Cloud, for example, allows it to do real-time analysis of unknown websites to determine whether they pass the filtration settings. The result is that organizations can finely calibrate network access to the internet, decreasing the risk of attacks from malicious websites.

The 2009 Association for Computing Machinery Workshop on Cloud Computing presciently noted another danger for which the Cloud poses both a unique problem and a solution:

“Availability also needs to be considered in the context of an adversary whose goals are simply to sabotage activities. Increasingly, such adversaries are becoming realistic as political conflict is taken onto the web, and as the recent cyber attacks on Lithuania confirm. The damages are not only related to the losses of productivity, but extend to losses due to the degraded trust in the infrastructure, and potentially costly backup measures. The Cloud computing model encourages single points of failure. It is therefore important to develop methods for sustained availability (in the context of attack), and for recovery from attack. The latter could operate on the basis of minimization of losses, required service levels, or similar measures.”

The most common threat of this nature is a distributed denial of service (DDoS) attack, which operates to disrupt services by overflowing servers with requests. While CSPs are just as open to these attacks as more traditional networks, the scalability provided by Cloud architecture provides an opportunity—especially for larger providers—to dynamically absorb DDoS attacks without a loss of service.

The risk of DDoS attacks underscores the importance of security in the Cloud as well as within the organization. Experts frequently note the importance of coordinating the security policies of users and providers in order to ensure that user security controls (such as identity verification and authentication) are compatible with the Cloud and that the Cloud’s own policies meet the user’s standards. International standards such as the ISO 27000 series and Information Technology Infrastructure Library (ITIL) service management infrastructure best practices can be helpful in this regard. Their usefulness—and ongoing efforts to adapt them to the realities of Cloud computing—indicate an area in which both private industry organizations and government agencies can be a source of leadership.

Currently the primary mechanism for ensuring this cooperation and standard-sharing is through the contract negotiation process. ENISA has developed a model list of questions and areas of importance for use by organizations while evaluating CSPs. Likewise, NIST guidelines note that negotiated agreements can address traditional as well as technological security policies such as employee vetting, isolation of tenant applications, data encryption and segregation, and the use of validated products that meet government standards and regulations. Some commentators have called for the imposition of liability on CSPs for losses caused by breaches in security, noting that this could provide an additional incentive for security and also more accurately reflect the relative control and responsibility exercised by providers and users. This would nonetheless be difficult due to the often sprawling chain of supply, interdependency of many operations, and general forensics issues noted above. In response to the difficulties surrounding contracts, there have been calls in the U.S. for a national IT security oversight board to develop standards and respond to larger breaches.

Another issue is simple transparency. As more services migrate to the network, record keeping and clear and consistent authentication and access controls become of paramount importance. A cohesive system of record-keeping with regard to authentication, authorization and accounting helps in-house and providers track and respond to security incidents. Innovations such as immutable audits also allow this logging process to be individualized and automatic, allowing each user to view his/her access and usage history. Transparency not only allows organizations to track and respond to internal threats, but also to strengthen compliance and enforcement of internal security policies and procedures. This is crucial to overcoming the risks posed by employees who may carelessly introduce vulnerabilities into the network by failing to take proper precautions on devices they own for personal as well as business use. For organizations starting from scratch, these controls should be planned and built into the IT architecture from the very beginning. For organizations transferring to the Cloud from a more traditional IT set-up, however, properly re-calibrating their systems remains a significant challenge and a barrier to migration.

While the response to security concerns remains part of the larger strategic decision taken by organizations considering the Cloud, government leadership can also provide a more stable environment in which to consider the risks. Auditing standards, transparency and reporting requirements, and imposition of liability on CSPs and subcontractors for breaches are all potentially useful means of balancing stability and growth.

2 http://dl.acm.org/citation.cfm?id=1655008&picked=prox&CFID=92339077&CFTOKEN=14623505
http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494
Data privacy

The issue of data privacy is closely linked to the problems of data security, data ownership, and law enforcement access discussed in previous sections. On the one hand, vulnerabilities in and the essential fluidity of the Cloud’s IT architecture open users’ data up to the risk of access by third parties, whether hackers, co-tenants in data centers, or trespassing employees. On the other hand, provider-dominated SLAs often contain provisions that weaken or outright eliminate users’ exclusive control over their sensitive information in certain circumstances. These issues are compounded by mismatches in the privacy laws of different countries the potential for access by government authorities, both of which loom large due to the potentially dispersed locations of Cloud services.

Customers (particularly individual end users) often tend to be ignorant of these issues and are simply unaware of the privacy risks inherent in Cloud-based services. Even for those who are aware, CSPs are often reluctant to disclose details about their policies and the routes data take, meaning that customers simply may not know when their data is stored or transferred through a jurisdiction that poses a higher risk of interception or interference. Furthermore, the history of privacy policies for larger Cloud-based companies indicate that companies whose revenue is based largely on the data mining and aggregation necessary for targeted advertising may not have sufficient incentive to unilaterally protect users’ information, particularly in the face of relative ignorance and/or apathy in the consumer market.

It is worth noting that the prevalence of form contracts (and the concomitant privacy concerns) in the Cloud computing world takes on special significance in the Indian context due to the language of the IT Act and subsequent Rules regarding personal and sensitive information. Section 43A imposes liability for a failure to maintain reasonable security practices and procedures, but the wording of the explanation of that section indicates that “an agreement between the parties” might take precedence over the current Rules, which take effect “in the absence of such agreement or law.” Similarly, the provisions of the Rules relating to collection, transfer and disclosure frequently refer to the purposes for which the information was collected and the prior consent of the information provider. These areas are often governed by contracts with CSPs, who tend to play a dominant (if not exclusive) role in shaping their terms.

Some have argued that this situation represents a market failure, requiring government intervention to spur providers to adequately protect users’ privacy.

Remedial measures and recourse

A predicate consideration to the different ways to combat privacy concerns in the Cloud is to carefully analyze and plan the migration itself. Some organizations—particularly those dealing with highly sensitive data, simply find that the benefits outweigh the risks. It is also important to note that the risks and benefits differ according to which Cloud service is being utilized. IaaS, for example, offers more control and potentially more transparency in terms of information storage than SaaS, which often leaves the user in the dark concerning the precise way their data is being handled. Similarly, alternatives to public Cloud deployment, such as a private Cloud or simple virtualization of internal processes, provide greater privacy controls, albeit at the cost of limiting some of the characteristics and economies of scale that make Cloud computing so beneficial.

As with security, coordination between the user and Cloud provider is of paramount importance. For those who can, careful contract drafting and negotiation can help determine issues such as data ownership and disclosure rights and set standards to deal with problems before they arise. Contracts should also ensure the proper identification, allocation and management of risk and liability between the Cloud provider and the client. This is particularly important given the frequent use of subcontractors in the provision of Cloud-based services, since they add to the privacy risks.

Despite the incentives of major service providers to collect user data and their resultant reluctance to enact strong privacy policies, civil society groups have had some success in effecting change. A few service providers now enforce an 18 month data retention policy, after which data is anonymized (i.e. wiped of indicators that could lead to the identification of the individual). While some argue this does not go far enough, in theory this process allows companies to continue to aggregate, analyze, and share data without posing a danger to individuals’ privacy rights. Other options from a governmental perspective include regulations of the storage, transfer, and disclosure of information.
The Indian Cloud Revolution
Migration to the Cloud - Government and Industry

In its guidelines for U.S. government agencies considering migration to the Cloud, the U.S. FedRAMP emphasized that the decision should be based on an assessment of risk rather than a pure evaluation of the technological and cost-saving advantages to be gained.¹ This sentiment has been echoed in multiple guidelines for the adoption of Cloud computing, all of which call for a careful assessment of the risks and benefits of Cloud computing before making the shift. For example, the process could begin with planning, then a migration and testing phase, then a full launch followed by continual monitoring of performance with a clear division of responsibilities between the different administrative units of the agency. Similarly, IT security industry leaders recommend virtualizing the agencies’ internal operations before moving to a private Cloud and ultimately considering hybrid or public Cloud deployment options for some services. The best practices models provided by ITIL and the ISO 27000 series also provides a useful, more general framework for structuring the transition.

With regard to the crucial planning stage, the process should take into account business factors, such as existing IT investments, costs, data security, regulations, and scalability requirements, as well as technical factors, such as existing infrastructure requiring retooling, security architecture, the complexity of the current system, availability needs and guarantees, local access and storage requiring transition, the IT skill base of the staff and Cloud-specific training needs, and the sufficiency of SLAs. NIST in the United States has drawn up a helpful list of intermediate steps in this planning process, including specifying requirements (security, business, etc.), assessing security and risks, assessing individual Cloud provider competency, and finally negotiating the contract and establishing the respective obligations of providers and government users.²

Government and the Cloud

The challenges facing governance in India are well-suited in many respects to solutions offered by Cloud-based services. This is particularly true with regard to e-governance initiatives aimed at engaging the public—both receiving input and administering regulations—and the delivery of social welfare programs.

One of the strategies of NTP 2012 is “To promote synergies between roll-out of broadband and various Government programs viz e-governance, e-panchayat, MNREGA, NKN, AADHAR, AAKASH tablet etc.”³

It further emphasizes 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.”⁴

Many of these e-Governance initiatives or plans require a large amount of information about population etc. Due to limited centralization and/or interconnected IT systems, this information and the exercise of collecting such information is often duplicated. Government bodies across India including central and state Government, SPV’s, local Governments, usually operate with moderate to low level of IT involvement – many departments having undertaken computerization in the past decade. These difficulties can be overcome by the opportunities provided by virtualized processes and network-dependent services. Responsiveness, information sharing and coordination between different areas and levels of government can also be augmented by the potential for scalable and shared resources in the Cloud. Not only will this result in a significant reduction in capital expenditure, it will also enable building transparent systems and robust reporting and information records systems which will ultimately help in improved governance and bring efficiency to citizen services.

¹ http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf
The India Vision 2020 document\(^5\) states that “India’s economic and technological transition will be accompanied by a multifaceted political transformation that will have profound impact on the functioning of Government. This transformation will foster decentralization and devolution of power to local bodies, including financial devolution and financial responsibility; increasing direct participation of people in setting grass root priorities for distribution of resources, and building and managing local projects; and greater efficiency, transparency, and accountability in Government agencies at all levels. E-governance has the potential, if fully harnessed and rightly utilized, to radically improve the speed, convenience, quality and transparency of public administrative services, while enhancing the ability of individual citizens to express and exercise their democratic rights.”

The NTP-2012 also supports the above by stating, “Strengthen the institutional, legal, and regulatory framework and re-engineer processes to bring in more efficiency, timely decision making and transparency.”

The Cloud provides public agencies with distinct advantages to meet new ‘open’ Government requirements. Cloud services make available an environment that provides Government agencies with access to a shared pool of easily usable computing resources (such as hardware and software). As these benefits directly impact the effectiveness of governance, by allowing Governments to quickly deploy IT resources for new eGovernment initiatives.

Governments across India including central and state Government, SPV’s, local Governments, currently operate with moderate to low level of IT involvement – many departments having undertaken computerization in the past decade. The Cloud promises to be a panacea for the challenges being faced by the Government in the IT space. It presents an opportunity for Government bodies to leapfrog the IT enablement which developed countries underwent and set up infrastructure for the next wave of eGovernance in India. The Cloud can help fulfill the above promise by migrating and adopting appropriate Cloud infrastructure for widespread implementation of e-Governance services by Government agencies. The Cloud promises to be a panacea for the challenges being faced by the Government in the IT space and presents an opportunity for leapfrogging and set up infrastructure for the next wave of e-Governance in India.

The Cloud presents the following advantages to Government:

- The flexibility provided by the Cloud infrastructure will be leveraged by the Government to provide e-Governance services in a more time-efficient manner.
- One of the tenets of the Cloud is ubiquitous access – wherein services offered through the Cloud can be accessed by general public from remote locations.
- Cloud should also be used to enable centralized storage of data across Government bodies. Many current governance related requirements revolve around sharing of information among Governments; Efficiency levels will increase when Cloud will be used for this sharing.

Various Government agencies across the globe are adopting Cloud. Presented below are some select case studies or examples of Cloud adoption by Governments:

**Case Example 01: AWS GovCloud (US)**

AWS GovCloud is designed to allow US Government agencies and contractors to move more sensitive workloads into the Cloud. It offers the same high level of security as other AWS Regions. The AWS GovCloud also supports the existing AWS security controls and standard industry certifications such as FISMA, SAS-70, ISO 27001, FIPS 140-2 compliant end points and PCI DSS. AWS also provides an environment that enables agencies to comply with HIPAA regulations.

**Case Example 02: Army Experience Center, Department of Defense (U.S. Army)**

The U.S. Army Experience Center needed a flexible, extendable and customizable recruitment tracking platform to track prospective recruits. They moved to a Cloud environment that permits a 360 degree community outreach and relationship management approach.

The projected results of adopting the Cloud for this requirement are:

- Costs down to 8M for full licensing from USD 83M
- 33 percent productivity gain
- 30 times higher response rates
- Social media (Twitter/ Facebook) integration to help in better outreach to younger recruits
- Geo-location and contact data in the field available via iPhone and Blackberry
- Enablement of visitor and user surveys for instant information
- Massive email campaign capabilities

While it is expected that the Cloud will ultimately transform IT in the Government there are also some concerns with respect to Cloud adoption by the Government which have been discussed earlier and will be discussed in the context of developing an appropriate Cloud policy in India.

While in the long run, almost all the applications may be Cloud-ready, it is important to note that not all the application enabled services will be ripe for Public Cloud deployment. Government needs to identify applications that can be migrated to cloud in the short-term, medium term and long term. For example, sensitive applications relating to defense services may not be the moved to the Cloud whereas the public facing municipal applications may be moved to the Cloud immediately, and other municipal applications can be moved in the medium term.

---

5 http://planningcommission.nic.in/reports/genrep/pl_vsn2020.pdf
6 http://www.dot.gov.in/ntp/NTP-06.06.2012-final.pdf
7 http://aws.amazon.com/govcloud-us/
Industry

The Cloud can lead to significant change in the way IT services are provisioned and used. It makes a promising business case on both technical and commercial fronts. The key proposition of the Cloud is to transform the current IT infrastructure model from CAPEX (Capital Expenditure) based into a ‘Pay-as-you-go’ or OPEX (Operational Expenditure) based. This together with the benefits of flexibility, scalability and ease of implementation makes it an attractive prospective for not only startups, small & medium enterprises (SMEs), and but also large enterprises.

According to the Gartner 2011 CIO Agenda survey, ‘Indian companies expect to adopt new Cloud services in 2011 much faster than anticipated, with two-thirds of CIOs expecting the majority of IT to be running in the Cloud within the next four years. The large shift towards Cloud adoption corresponds to the overall positive effect of Cloud with efficient allocation of resources, resource pooling, and increase in distributed accessibility which empowers organizations to focus on core competencies.’

As per the India Vision 2020 document—“The largest number of new jobs will be created by SMEs.” However, the high cost and complexity of implementing software packages in the traditional IT environment had kept SMEs away from technological adoption. The Cloud provides easy to deploy and affordable pay by usage model. This enables SMEs to deploy cutting edge technology which was earlier the privilege of only large corporations.

With growing population, growth of entrepreneurship and the SME sector is a key to generate employment. The Cloud with its ability to provide quick and easy provisioning of IT resources will only help accelerate the growth in the SME segment and setting up of new businesses.

Education

As per the India Vision 2020 document “Literacy must be considered the minimum right and requirement of every Indian citizen. Presently, the country has about 300 million illiterate adults. The Government’s goal is to achieve 75 per cent literacy within the next five years.”

The key challenges facing the educational sector today are quality of education and reach of educational services to remote corners of the country. As per the India Vision 2020 document, “the current enrolment rate for primary education is around 77 per cent and for secondary education about 60 per cent.” Further, “increasing enrolment to cover the entire school-age population needs to be combined with efforts to increase the quality and relevance of school curriculum to equip students with not only academic knowledge, but also values and life-knowledge … Concentrated efforts are needed to tap the potentials of alternative methods of knowledge delivery for both school going and non-school going children and adults, including television, computerised self-learning and Internet-based courses.” The NTP-2012 envisages that, “Thrust of this policy is to underscore the imperative that sustained adoption of technology would offer viable options in overcoming developmental challenges in education, health, employment generation, financial inclusion and much else.”

The Cloud offers to address both reach as well as quality issues marring the education sector by low cost implementation of IT tools leading to qualitative improvement in educational content and delivery and by enabling remote education.

Since, the Cloud eliminates the costs of procuring and maintaining IT infrastructure, the educational sector can now embrace software tools for smoother operations and improving the quality of educational content. Educational institutions are also in a position to take advantage of certain SaaS based software which has been made available for free or subsidized cost to this sector alone by certain CSPs.

The other important application of the Cloud for educational sector is in remote education. Remote classrooms will help run simultaneous classrooms by a smaller number of teachers – thus helping overcome the challenge of lack of qualified teachers. At the same time, it will help in standardizing the content and delivery methods of education.

Higher education is another area where the Cloud can make a difference. According to the India Vision 2020 document there are a “huge number of young students that will quest for all levels of higher education and a severe shortage of qualified instructors” The document further highlights that “the country should embark on a massive program to convert progressively the higher educational curriculum into a multi-media, web-based format and to establish accredited standards for recognition of courses taught under distance education programs.” There have been some initiatives to harness the internet in the area of higher education; for example NPTEL – a joint initiative by IITs and IISc – which broadcasts regular classroom lectures in engineering, science and humanities streams on the web. Such initiatives are precursors and can be extended further by providing dedicated remote classroom sessions using the Cloud.

We discuss the developmental opportunity presented by cloud for the educational sector in detail on page 34
Healthcare

The Indian healthcare sector is one of the largest sectors in India in terms of revenue and employment. Quality and qualified medical information is not available across the country. With the increase in population and expanding middle-class segment and potential for growing private sector funding, India which is yet to develop a national electronic health record management system should utilize the Cloud to set up a common Cloud based database for health records for the Healthcare sector to utilize. This would allow the sector to skip the creation of federated heath record databases as has happened in developed countries.

The Cloud shall also enable services such as telemedicine which will address the challenges of providing specialized healthcare services to remote areas of the country with fewer resources. Another area of application is technologies such as artificial intelligence, which require high computing power, being made available as Cloud based services to enable medical practitioners to correlate disparate pieces of patient data for a more comprehensive and reliable diagnosis.

The developmental opportunities in the healthcare sector are explained in detail on page 37

The NTP-2012 also points out national benefits of the Cloud by stating that “The advent of technologies like cloud computing present a historic opportunity to catapult India’s vaunted service delivery capabilities to a new level domestically as well globally.”

Given the benefits of the Cloud, many organizations have, in principle, decided to migrate to the Cloud. However, due to the rapidly evolving Cloud market and dynamic technical information, most organizations are unsure on how to proceed with the migration into the Cloud. One of the biggest challenges organizations contemplating Cloud adoption face is where to start and what to focus on. Further, depending on the type of enterprise e.g. SMEs, government or large corporations, the Challenges and migration process would vary.

There are both business and technical factors to consider while evaluating the suitability of an application and infrastructure for Cloud migration. In the migration phase, the applications selected will be ported to the Cloud and tested in a structured manner. Simple applications like e-Mail would just need testing prior to migration in terms of functionality and performance. However bespoke and/or complex applications would need the creation of a development and test environment.
Real-world examples of migration to Cloud

For a leading ISV, Cognizant migrated I/O-intensive Web conferencing onto the cloud. The new cloud-based solution supports 30,000 concurrent meetings, all with screen sharing, camera, voice, telephony and recording features.

A large media and cable services provider engaged Cognizant to transition 46 unstructured, over-provisioned applications onto a flexible cloud environment. The resulting utilization gains generated a 35 percent cost savings.

City of Orlando migrated their email application onto the Google Cloud. Within a year, they started realizing USD 200,000 annual cost savings, increasing email storage 100-fold and mobile phone access.\(^{10}\)

The General Services Administration (GSA) became the first US federal agency to completely migrate its email system on Cloud. The agency has migrated more than 17,000 employees to Google Apps for Government for cloud-based email and collaboration. The migration was completed in flat 6 months and agency sees a 50 percent cost savings over a period of 5 years.\(^{11}\)

Real-world examples of migration to Cloud

There are many resources available in India including Indian Cloud service providers and industry bodies to enable organizations to migrate to the Cloud.

### Catalogue of services offered by Indian Cloud Service Providers (CSPs)

<table>
<thead>
<tr>
<th>Service</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Cloud Enablement            | Cloud related services such as:  
  • Migration  
  • Deployment  
  • Planning  
  • Consulting                                                   |
| IaaS                         | On-Demand Virtual Servers  
  • 99.995 percent uptime  
  • Tier 4 datacenters                                          |
| PaaS                         | Providing a cloud-based development platform for building business applications and deploying them on public or a private cloud          |
| SaaS                         | A wide range of software delivered as a service via Cloud ranging from Email, Productivity applications, Business applications, Collaboration applications, ERP, CRM, Core banking etc.  
  These CSPs cater to a wide variety of customers ranging from SMEs to large enterprises. |
| Private Cloud                | Catering to Indian enterprise sector with a dedicated pool of computing resources.                                                          |
| Cloud Telephony PaaS        | India-based telephony platform in the cloud. It is the simplest and easiest way to build telecom applications, IVRs, office PBX and outbound campaigns and deploy them on the Cloud. |
| iTaaS – Cloud based IT as a Service | Covers the entire spectrum of business processes for SMBs. Domains included are:  
  • Manufacturing  
  • Wellness  
  • Retail  
  • Education                                                  |

Thus we see that the Cloud presents a unique opportunity to India to be able to leapfrog the IT enablement revolution by directly adopting Cloud based services, similar to the telecom revolution in India wherein we skipped the wireline network growth and leapfrogged directly to large scale adoption of mobile phone based network.

\(^{10}\) [http://planningcommission.nic.in/reports/genrep/pl_vsn2020.pdf](http://planningcommission.nic.in/reports/genrep/pl_vsn2020.pdf)  
The Cloud unlike previous technology shifts is not a mere collection of technologies but a transformational concept which requires the ecosystem to be developed. The Cloud ecosystem consists of the components as shown below:

- **Demand side:** Fundamental factors required to enable the use of Cloud services by Indian businesses and citizens to enable creation of a sustainable demand for Cloud services in India.
- **Supply side:** Prerequisites for CSPs to set up Cloud operations in India.

Source: KPMG in India Analysis
The following section will discuss the different infrastructure and regulatory framework requirements along with possible ways to overcome challenges in ensuring the availability of each infrastructure component:

**Power**

Power is the common denominator in terms of both supply and demand side for adoption of Cloud in India.

**Demand Side**

The use of Cloud services by businesses and citizens will require them to operate end-user computing devices such as PC’s, network devices and mobile computing devices. Operation of all these devices also requires a reliable supply of power to end consumers.

As per ‘Powering India – The Road to 2017’, a report by McKinsey&Company India’s electricity demand is likely to cross 300GW in the next 10 years earlier than most estimates. As per the India Vision 2020 document the “total demand for power is expected to increase by another 3.5 times or more in the next two decades, which will necessitate a tripling of installed generation capacity from 101,000 to 292,000 MW by 2020”

The Cloud will contribute a small component of the total demand for power, but ensuring reliable supply of power to Cloud services will determine the availability of various services supported by it.

The NTP-2012 highlights the fact that “Introduction of new technologies has posed fresh challenges in network security, communication security and communication assistance to law enforcement agencies. NTP-2012 provides a clear strategy for squarely addressing these concerns.”

It is also important to define policy measures such as allowing captive power plants for ensuring a reliable power supply to Cloud data centers or grant of preferred status to such facilities.

**Supply side**

CSPs will need to set up large data centers which shall not only require power for powering computing hardware but also for cooling and other support facilities.

In order to ensure sufficient and reliable electricity to service providers the Government should allow creation of captive power plants. Further, to encourage reduction in technological waste and carbon footprint, tax holidays should be offered to the CSPs who endeavor to set up green data centers which produce their own electricity by utilizing renewable sources of energy such as wind or solar farms.

In this regard the NTP-2012 encourages “To promote the use of energy efficient equipment including low power wireless devices in telecom networks and adopt measures for the reduction of carbon footprint in the telecom sector.”

In addition local and state Governments should support setting up of Cloud data centers in their states and regions by offering electricity at subsidized rates to venturing CSPs.

**Connectivity and Bandwidth**

The other common denominator between demand and supply side for Cloud adoption is internet connectivity in terms of available bandwidth and uptime. Vision 2020 also conceives of India evolving into an information society and knowledge economy built on the edifice of information and communication technology (ICT), of which telecommunications is the springboard.

**Demand Side**

India’s Internet penetration trails behind China, New Zealand, Australia and other emerging economies. India has relatively few Internet users: just 7 percent of its population is connected to the Web, compared with 32 percent in China and 77 percent in the United States. India is also said to be the most expensive in the world in terms of cost of bandwidth ahead of even USA, Korea and Japan.¹

Recognizing this gap, the NTP-2012 also aspires “To provide secure, affordable and high quality telecommunication services to all citizens.”

It presents the vision of ‘Broadband on Demand’ and envisages leveraging telecom infrastructure to enable all citizens and businesses, both in rural and urban landscape, to participate in the Internet and web economy thereby ensuring equitable and inclusive development across the nation.

With the entire operations of the organization shifting to the Cloud, the single point of failure can hamper the business-as-usual of an entity using the Cloud service.

There are various initiatives to bring the availability and reliability of connectivity at par with other countries. One example is the National Knowledge Network, a pan-India network which helps in providing unified high speed connectivity across the country. With implementation of 3G services and the 4G revolution on the brink of implementation in the country, India can soon bridge the gap.

The Government needs to further encourage investments in growth and penetration by promoting both ISPs and telecom providers. At the same time CSPs should be allowed to provision dedicated bandwidth from ISPs.

The NTP-2012 promotes “ubiquitous network connectivity of mobile technology, broadband Internet, fiber penetration in all villages, high-technology low-cost affordable devices and software solutions which enable electronic access to service including m-payment.

Provide affordable and reliable broadband on demand by the year 2015 and to achieve 175 million broadband connections by the year 2017 and 600 million by the year 2020 at minimum 2 Mbps download speed and making available higher speeds of at least 100 Mbps on demand.”

¹ http://planningcommission.nic.in/reports/genrep/pl_vsn2020.pdf
Supply Side

Cloud data centers require connectivity not just to be able to reach consumers in India, but also to provide reliable services to their global clientele. This requires not only normal internet access but more specifically reliable and unhindered access to international internet traffic gateways. The bandwidth requirements of Cloud data centers may require them to provision for dedicated fiber optic leased lines especially where such data centers are located in remote locations without regular connectivity.

The Government should encourage investments in growth and penetration of internet access by ISPs and telecom providers. The NTP-2012 also points in a similar direction viz. “To move at the earliest towards liberalisation of spectrum to enable use of spectrum in any band to provide any service in any technology as well as to permit spectrum pooling, sharing and later, trading to enable optimal utilisation of spectrum through appropriate regulatory framework.”

Given the continued predominant role of wireless technologies in delivery of services in ICT sector, NTP-2012 incorporates framework for increasing the availability of spectrum for telecom services.”

In addition to the above strategic initiatives, tactical provisions such as allowing CSPs to provision dedicated bandwidth from ISPs are also required to tackle short term requirements arising from Cloud adoption.

Land and Real Estate

While not critical from a demand side, real estate is critical from a supply side perspective as Cloud data centers shall require large warehousing space to set up. Cost of real estate in suitable locations (those with a combination of sufficient power and internet bandwidth) at a low cost is an enabler in setting up of the datacenter.

A strong demand from BFSI and the IT/ITeS coupled with a very limited supply of quality office space has led to a sharp increase in lease rentals for commercial office space in most micro-markets, with an average increase of 108 percent between 2005 and early 2008, according to CRISIL Research.2

In addition to financial aspects, there are logistical challenges such as:

• physical security of Cloud data centers (which shall house critical data of Indian as well as international clients)
• availability of affordable housing and amenities near data centers for personnel managing them (in order to attract high quality talent) and
• managing the environmental and social impacts of such projects.

Policy level incentives are needed to ensure that availability of real estate in suitable locations does not become an impediment to setting up CSP operations in India. The NTP-2012 also highlights the need to “Emphasize the active role of both private sector and Government including the State Governments and Local bodies to enable the growth of telecom infrastructure necessary for meeting the telecommunication demand of the country and leveraging Universal Service Obligation Fund wherever appropriate.”

One of the ways to overcome the challenges is the creation of Special Economic Zones (SEZ’s) for setting up of Cloud Parks similar to Software Technology Parks set up by the Government in the 90s. Such SEZs can be set up near sources of power while planning for development of other utilities such as housing and consumer services. This approach shall also helps in overall development of a region by attracting other associated players to the region such as:

• Power and utilities companies
• Consumer services companies such as retail, hospitality and housing
• Educational institutions and Hospitals
• Transport and Logistics

Cloud and related IT industries are fundamentally green industries. However, further focus on environment can be brought about by extending subsidies to players who invest in SEZs using green technologies such as of captive solar or wind power farms; environment friendly building design; rainwater harvesting and environment friendly waste disposal.

Technology Enablers

Proliferation of Cloud services among industry and citizens will require availability of a new class of end-user devices such as mobile viewers, tablet PCs, and specialized devices. For the Cloud to grow, such devices will have to be ubiquitous and affordable – which will require them to be produced in large quantities and with locally available resources.

This presents an opportunity for growth of the consumer electronics sector, and also paves way for innovation by Indian entrepreneurs in the application of Cloud based services. The NTP-2012 also looks forward to3 “reposition[ing] the mobile phone from a mere communication device to an instrument of empowerment that combines communication with proof of identity, fully secure financial and other transaction capability, multi-lingual services and a whole range of other capabilities that ride on them and transcend the literacy barrier.

The NTP-2012 plans to3 “create a corpus to promote indigenous R&D, IPR creation, entrepreneurship, manufacturing, commercializing and deployment of state-of-the-art telecom products and services during the 12th five year plan period.” It also plans “to promote synergy of academia, R&D centers, manufacturers, service providers, and other stakeholders for achieving collaboration and reorientation of their efforts for creation of IPRs, development and deployment of new products and services suited to Indian environment.”

A common ingredient in enabling Cloud services as well as the growth of the local electronics industry is the availability of personnel equipped with the requisite IT skills. India is in a fortunate situation in terms of availability of such skills which can act as a major driver to enable Cloud a revolution in India.

One of the missions of the NTP-2012 also is to “make India a global hub for telecom equipment manufacturing and provisioning of converged communication services.”4

However, policy level thrust in terms of tax incentives will be needed to ensure that required resources are invested to ensure a sustained and swift growth of the sector.

For India to become a hub for Cloud data centers, government shall need to offer conducive environment and incentives to attract investments from Cloud Service Providers to set up such data centers. Currently, there are significant challenges for India to become a hub for large Cloud data centers due to, inter alia, the quality and reach of the data networks, broadband and power grid capabilities. In order to enable India to harness the latest Cloud technologies at reasonable costs, technology and location neutrality should be the cornerstones of policy.

Awareness and Local language support

With a literacy rate of 61 percent and challenging statistics in terms of school attendance, the general awareness regarding new technologies in India is a big challenge. This is complicated by the diversity of local languages present in India. According to the last census of 2001, 29 ‘languages’ have more than a million native speakers, 60 have more than 100,000 and 122 have more than 10,000 native speakers.5

As a result adoption of new technologies in India is often impeded by the lack of awareness and unavailability of local language interfaces. This challenge has reduced to a certain extent in the past few years due to the Mobile phone revolution in India which has aided both – increase in general awareness regarding technology and the adoption of local language interfaces.

Currently, most Cloud services are provided by CSP’s outside India and hence do not provide interfaces in Indian languages. Regulations and policy level incentives are needed to encourage creation of local language interfaces for Cloud services.

As is stated in the NTP-2012 also, further thrust is needed “To stimulate the demand of broadband applications and services, work closely with Department of IT in the promotion of local content creation in regional languages which would enhance the investment in All-Internet Protocol (IP) networks including NGN.”

4 http://www.dot.gov.in/ntp/ntp-06.06.2012-final.pdf
5 http://en.wikipedia.org/wiki/Languages_of_India
Regulatory Framework - Government in Action

Single window clearance for data centers

The unique mix of challenges and opportunities posed by Cloud computing necessitates India’s involvement in the physical infrastructure of the Cloud. One needs to only look at the United States to see what the presence of data centers within one’s borders can offer in terms of security benefits, regulatory and jurisdictional claims, and technological innovation and growth. Despite these advantages, India lags behind in both the number and sophistication of data centers it hosts. A recent index of risks associated with data centers ranked India and China poorly based largely on the presence of political risks from regulations and controls on investment and other aspects of data center installation.

Creation of a single window clearance process for data centers could go a long way in mitigating these perceived disadvantages. India has the natural resources and skilled IT workforce necessary to make it a leader in data center technology, particularly given the new emphasis on servers and data centers uniquely configured to operate for the Cloud. Energy costs are on the rise, so green, energy-efficient data center technology is already becoming an area of significant growth. A stable, streamlined regulatory framework could remove uncertainty and allow for an increased influx of technology transfers that can allow India to seize the market in this respect.

Multilateral framework for enablement and sustenance of Cloud architecture

International governance in the Cloud is currently a hodgepodge of governmental and industry research groups (e.g. the IGF in the U.N., ITIL in the IT industry), bilateral standards (such as the Safe Harbor Framework between the EU and Switzerland), and agreements between private MNCs and sovereign governments.

In the wake of the Wikileaks scandal and the new focus on data security, Brazil led an effort to establish an international regulatory body responsible for data security and common standards which would address the new developments and challenges represented by Cloud computing. However, this proposal was unsuccessful due to opposition from business leaders and countries such as Australia, who wanted to keep the current non-binding, civil-society-oriented IGF model.\(^6\)

Given the wide disparity in regulatory schemes and competing national interests between major players, an international treaty on Cloud governance is unlikely in the short term—as acknowledged by the IGF.\(^7\) Nevertheless, the international community can and should take steps to develop a framework to solve some of the most pressing issues facing the future of Cloud computing, particularly sovereignty and jurisdiction over regulatory violations and crimes. Given that emerging markets are an area of relative growth—even when compared to booming markets in the developed West—countries such as India and Brazil can take the lead in determining the shape of these discussions.

In the absence of a treaty, one solution is to follow the model of the EU and the United States, whose Safe Harbor Framework allows data flows to continue despite differences in privacy regulation that may have otherwise hampered business and trade. While taking a hard line on data sovereignty may serve important national goals, if not offset by these sorts of agreements it could have the effect of hampering data flows and ultimately cutting the country off from innovation and growth. Another option suggested by the 2010 IGF conference is the possibility of private-public memoranda of understanding between large data center operators and national governments. This could allow the frequent sources of conflict such as data ownership, disclosure requirements, and law enforcement access to be resolved ahead of time by quasi-contractual agreements. Governments could even set up liaison offices to coordinate operations with the centers. Such an approach would require participation from a critical mass of major international players to be effective, but it represents an alternative to the traditional state-state approach.

Ultimately Cloud computing operates in a vacuum when it comes to multilateral governance, leading to the heavy reliance on contractual provisions seen throughout this Note. This represents an opportunity for leadership in the field, from questions of jurisdiction and sovereignty to environmental and corporate regulation.

---


Amarchand Mangaldas analysis
Rationalizing policies relating to the movement and storage of data

With respect to policies governing data in the Cloud, the current state of affairs in the international arena is one of relative fluidity. Governments from the United States to Australia are still grappling with the regulatory implications of Cloud computing and the flexibility, geographic dispersion, and loss of governance it entails. Major issues needing resolution include: the question of data ownership, the respective obligations and liabilities of Cloud service providers, clients, and end users, the use of background versus mandatory rules with respect to regulations and contractual obligations, and the transparency and disclosure requirements imposed on providers.

One point of caution for government regulators, however, is the difficulty of balancing the need to regulate in the public interest with the freedom necessary for technological innovation and economic growth. To this end, commentators have suggested drafting technology-neutral standards for issues such as security and privacy, which can be flexible and allow government regulators to control the effects of technology without its implementation, leaving businesses with the challenge to innovate within that framework.

Despite the lack of certainty, both OECD and the United States (among others) have already begun efforts to develop uniform standards applicable to Cloud computing. FedRAMP in the United States, for example, is responsible for developing model security controls that would be applicable to CSPs used by government agencies. Other efforts are aimed at developing the jurisprudence on data privacy and ownership to more accurately reflect the state of modern computing and the expectations of the public. In all these efforts, outreach to industry players as well as civil society groups (privacy NGOs, libertarian think tanks, etc.) has been important in ensuring input from a variety of interests in society.

In the Indian context, two major areas of focus would be privacy and the obligations imposed on CSPs. The former is all the more important because of the public’s relative unfamiliarity with the mechanics of Cloud computing, which in turn makes them less sensitive to its risks. The latter will necessitate a review of existing laws and regulations to determine if the current categories of service providers and information reflect the realities of Cloud computing. To the extent that they do not, regulations can either attempt to force providers to shift their services or practices (similar to mandating back doors in encryption) or change or develop new categories to accommodate the unique characteristics of Cloud providers and services.

These considerations could lead to an emphasis on the application of the IT Act and accompanying Rules governing ‘reasonable security practices and procedures’ and ‘sensitive information’ to CSPs. While the Rules mandate internationally accepted standards and audits, even these are in a state of flux with respect to some aspects of Cloud computing. Similarly, proposals for additional privacy legislation can take into account the essential flexibility of Cloud architecture while still providing protection for individuals. A harmonized system must balance the needs of the State and its citizens with the reality of Cloud computing as a global force subject to multiple overlapping jurisdictions. Requiring data to largely remain within the country may help alleviate conflicts with other jurisdictions, but this may come at the cost of international inflows and outflows of data. Most importantly, these rules and regulations should be considered from a holistic standpoint in order to provide an environment that properly balances the needs of the State, providers, and users.

7 http://www.gsa.gov/portal/category/102371
Summary

As evident from the above description of the Cloud ecosystem, India is currently challenged in availability of several ecosystem components excepting IT skills. While we have the required IT skills, we lack the other essential components of power, connectivity, real estate, the enabling regulatory framework and other adoption enablers.

In this regard, the NTP 2012 plans to “Encourage recognition and creation of synergistic alliance of public sector and other organizations of Department of Telecommunications (DoT) through appropriate policy interventions and support for optimum utilization of their resources and strengths in building a robust and secure telecom and information infrastructure of the country.”

While the Government is one of the primary pillars to help overcome these challenges, involvement of the private sector is also equally important for swift and effective enablement. Hence, the Public-Private-Partnership (PPP) model is one of the best mechanisms for setting up entities which shall help overcome the above challenges.

An example of the PPP implementation is setting up of joint SEZs wherein the Government will assist in land acquisition and channelizing utilities such as power and security, while the private sector would bring in the required investment and knowhow for setting up of the required infrastructure.

Another area of opportunity for PPP is setting up of a national health records database by the Government for healthcare services. The Government would provide for the investment in setting up the national Cloud infrastructure for such a database while the private sector agencies would provide services for upkeep of the records.

In addition, special financial provisions should be made available by the Indian Government for the private players who wish to build infrastructure for cloud computing.

Cloud Infrastructure - Private Cloud players should be allowed to procure raw infrastructure such as servers, firewalls etc at a subsidized rate for setting up the Cloud infrastructure.

Loans - Government should incentivize Banks to extend loans at concessional rates to entrepreneurs planning to set up Cloud services.

Tax incentives - CSPs should be granted exemption from paying regular taxes for a limited period of time from the time of setting up the Cloud operations.

Land - State governments should be directed to provide land at subsidized rates for setting up Cloud Datacenters.
Developmental opportunities presented by the Cloud

The NTP-2012 envisages “support to platform neutral services in e-governance and m-governance in key social sectors such as health, education and agriculture that are at present limited to a few organizations in isolated pockets. This will expand the footprint of these services and thus foster an atmosphere of participative democracy delivery model that is truly citizen-centric.”

The following sections specifically examine development opportunities presented by the Cloud for the education and healthcare sectors.

**Education**

The Educational sector is one of the cornerstones of socio-economic development. It is widely accepted that education contributes to poverty reduction and increased economic growth, which in turn leads to an improved standard of living. It also enables the individual to participate in wealth generating activities, leads to the creation of employment, and the overall development of society.

Growth of the Indian economy in the recent past is putting pressure on the educational sector to enhance the quality of discourse, expand the curriculum to include new subjects, make education affordable and improve its reach. While technology can play a significant role in accelerating the expansion of the Education sector in India, the digital divide hinders its reach.

While, both the Indian Government and private players are currently investing in the Education sector, these efforts are currently limited to adopting and enhancing traditional methods of imparting education. Private players are primarily catering to the needs of the urban segment of the Education sector, the Government has taken several initiatives to upgrade the reach and quality of education in rural and semi-urban areas. However, radical thinking is needed to exploit Cloud for the educational sector so that the challenges facing the sector can be tackled.
Challenges to Educational Sector

As has been outlined earlier in the whitepaper, the primary challenges associated with the educational sector in India are:

- Poor quality of education
- Reach of education to remote corners of the country
- Increasing cost of education
- Low engagement of students

As per the India Vision 2020 document\(^1\) – “With the development of modern media that brings sound and video images into every household, and with the advent of the Internet that enables us to reach out to sources of knowledge around the world, education offers both unprecedented richness of content and the capacity to deliver it. If only we could break free from the limitations of out-dated curriculum and outmoded delivery systems, we could utilize the opportunity to close the education gap that separates the world’s most prosperous communities from their poorer cousins”. The Educational sector transformed by Cloud adoption will be a true manifestation of the above vision.

Advantages of Cloud adoption to the Education Sector

The Cloud can transform the Educational sector by providing tools such as Learning Management Systems, Online portals, Virtual remote classrooms and Computer based tests as shown in the illustration below. Notably, adoption of these tools could be done at reasonable costs using the Cloud.

---

\(^1\) http://planningcommission.nic.in/reports/genrep/pl_vsn2020.pdf
The benefits of using these technologies in the Educational sector are:

**Standardized Content:** Educational content delivered through Cloud based services will be standardized thus ensuring that the quality of content available to students across the country is the same. Such tools will also ensure that teachers and instructors maintain a common delivery standard.

**Environment of collaboration:** Globalization has highlighted the advantages of collaboration between people across geographies. Schools are increasingly in favor of using collaborative tools to prepare students for a future where common goals are achieved through interactions between people sitting across geographies. Cloud services will allow such collaboration across schools and regions exposing students to a larger cross section of peers and fostering greater social camaraderie.

**New modes for providing education:** Dependence on the brick-and-mortar infrastructure and traditional teaching methods has inhibited the reach of education. New modes of providing education such as virtual learning environment, tele-education and online education programs enable providers of education to cut across geographical boundaries. This has the potential to help Governments boost literacy rates especially in rural areas.

**Administrative efficiency:** New age education systems, regulations and guidelines of governing bodies require educational institutes to function in a more professional manner. Cloud services can provide tools such as Learning Management System and Student Information System to enable better administration of schools and universities.

**Universal access to educational information:** For a country like India, where access to textbooks and educational information is limited by lack of public libraries and public schooling infrastructure, the Cloud can deliver the promise of delivering educational content on mobile phones and other devices which with the growing proliferation of ICT tools and the internet will help in making educational content ubiquitous.

**Recommendations**

The educational sector can be transformed into an inclusive, collaborative and efficient ecosystem by using Cloud based services. The Cloud can not only help in short term tactical solutions to reach a large population, but also pave way for transformation of the learning process into a futuristic model which will result in an overall improvement in the quality of learning.

In order to encourage the adoption of the Cloud and creating a suitable technical and regulatory environment for implementation of the Cloud in India, the following is recommended:

- Encourage set up of education content databases with universal access
- Provide incentives to education Cloud providers to develop content in Indian languages. Textbooks in various languages should be made available online at low costs.
- Create a policy with guidelines for usage of Cloud in education.
- Provide incentives to telecom providers to rollout high speed broadband access to educational institutions.
Healthcare

Seventy percent of the Indian population lives in rural India and most of them lack access to hospitals, physicians, trained medical personnels, critical medicine supply and medical equipments. India has only an elementary network of public hospitals and clinics (around 25,000 primary health centers). Public hospitals are also scarce outside large cities, and their service standard varies and lack even basic healthcare records management systems.

On the other hand, unlike the healthcare sector in developed economies, the Indian healthcare ecosystem is at a nascent stage of adopting technology. Currently, the Indian healthcare industry is evaluating technology deployment models for digitization of health records like EMRs and remote patient monitoring; futuristic trends such as centralized healthcare record management are not even thought of.

This presents us with an opportunity to leapfrog technology adoption in the healthcare industry. In developed economies, the governments are struggling to centralize the currently federated digital healthcare records. In addition, the legacy of IT applications are no longer scalable to handle large data volumes.

India can skip all these challenges by directly moving on to Cloud based centralized healthcare records management, Cloud based healthcare applications and harness the potential of telemedicine.
As highlighted earlier in this whitepaper, challenges in the Indian healthcare sector can be summarized as:

**Quality of Healthcare services in India**

The Indian Healthcare industry has traditionally been a cost sensitive market. As a result, the quality of services has remained rudimentary. Key issues for the healthcare industry, as far as IT adoption is concerned are Upfront IT investment costs, non-availability of trained manpower, and high cost of Transition from legacy to new systems. On the other hand, technological change and growing consumer awareness is resulting in mounting pressure on healthcare providers to improve the quality of services.

**Reach and affordability challenges in the healthcare sector**

Strong economic growth in India has resulted in demand for better healthcare facilities from rural and urban areas. However, the penetration of public healthcare centers remains moderate at best. Poor proliferation also makes healthcare more expensive for citizens because there is high pressure on limited resources resulting in rising costs. This trend is expected to further worsen as our population ages and aspirations grow.

**Lack of digitization of medical records and citizen data**

Lack of IT implementation in the healthcare industry also has repercussions on health record management. Healthcare data in most elementary healthcare centers is not digitized as smaller providers cannot afford to invest in technology. In larger hospitals, while the data is digitized, it is still not linked across other hospitals. This often makes it difficult to pull together patient data and medical history for efficient diagnosis.

This also creates complexity in handling of healthcare expenses by insurance companies. Insurance is a key component in making healthcare affordable for masses in India.

**Advantages of Cloud Adoption to the Healthcare Sector**

The Cloud can help overcome most of the challenges faced by the healthcare industry; following are specific advantages to each segment of the industry which will drive the adoption of the Cloud in this industry.

**Hospitals:** Using third party SaaS applications housed in the Cloud, patients can be provided access to their health history and information so that hospitals can streamline the admissions, care and discharge processes. Hospitals can connect to their own web portals and access patient data stored in the Cloud. Standard based services can also be used to build value added web-applications for patients so that their healthcare can extend beyond the boundaries of the hospital covering their entire lifecycle.

**Physicians:** With the Cloud, people can provide their health history and information to their physicians anywhere, anytime, including data uploaded from health and fitness devices, to help physicians make more informed decisions.

**Pharmacies:** People can administer or manage their prescriptions and associated information such as dosage, amount and frequency, and provide this information to their healthcare provider.

**Laboratories and imaging centers:** Patient’s diagnostic results can be transferred via suitable Apps onto Cloud based platforms, e.g. Google Health or Microsoft Healthvault. This eliminates the need for in-house storage and helps retain historic information in a systematic manner. Healthcare providers can access these results with the patient’s permission, to help them make more informed health decisions.

**Pharmaceuticals/Drug manufacturers:** The IaaS model could provide a drug manufacturer with On-Demand computing resources to perform drug research analysis, eliminating the need to retain high power computing capabilities and related IT expertise in-house.

**Application Providers:** Health and wellness companies can design and deliver health and wellness solutions compatible with Cloud platforms to offer a rich user experience and ease of managing the user’s sensitive personal health information.

**Device manufacturers:** Health and fitness devices can be designed to work with Cloud platforms and Apps, so users can upload device data and share it with their doctors and families.

**Insurance Companies:** Insurance providers through transparent access to medical records can provide better services to their customers. They can also offer customers with innovative tools which giving members’ access to richer wellness information thereby increasing effectiveness of care management programs which can help reduce claims costs. Insurance companies can also incentivize customers to keep their health records updated.
Concerns resulting from Cloud adoption by the Healthcare sector

Though the Cloud in healthcare provides several benefits for all the stakeholders of the industry, it has its own set of challenges as highlighted below:

- **Patient information security and privacy protection**
  The primary reason the Healthcare sector would offer resistance to making a move to the Cloud would be patient information security and privacy protection. Patient information across countries has been under the purview of legal frameworks. The patients themselves would be concerned about the security of their personal data.

- **Interoperability and standardization**
  In order to ensure efficiency and optimum utilization of resources it would be ideal if there is a high degree of interoperability and standardization between healthcare solutions for the Cloud.

- **Absence of legal framework for healthcare related data**
  There is no legal mandate / framework in place for centralized storage, maintenance and retrieval of healthcare information. Further there are no standards or metrics for features and security provisions in software to be used by Healthcare service providers. Finally, there is the lack of a regulator and regulatory guidelines for entities entitled to access healthcare records (hospitals, wellness clinics, insurance providers, online healthcare services etc.) and mechanism for sharing of healthcare records.

**Recommendations**

Cloud adoption will provide one of the most promising opportunities to reduce technology and treatment costs within health care. The Government should consider the following recommendations to enable Cloud in Healthcare:

- Set up a national authority for health record management
- Lay down rules for maintenance of health records across agencies
- Define guidelines for IT adoption by public hospitals
- Implement legislation for protection of patient data
- Provide incentives for laying of Cloud infrastructure dedicated to the needs of the healthcare sector

**Policing**

Policing is fundamental to having a civil society. Maintenance of law and order, investigation of crimes and intelligence collection are vital functions of police in the country. Police play a pivotal role in ensuring peace in society, by preventing instances which could threaten harmony within society, by disrupting activities which are anti-social in nature. They also investigate variety of crimes, where victims could be individuals, groups, community or the nation at large, and play role in prosecuting & deterring their recurrence. Because of their ground-level contacts, police officials also help in collecting important intelligence on activities which could be inimical to the State.

However, with increasing social strain, law and order has taken a priority for day-to-day operations of police force, thereby relegating crime investigation & intelligence collection on a lower priority. Police forces in the country continue to be hamstrung by lack of infrastructure like proper buildings for police stations, facilities for interrogation & recording of evidence, vehicles, stationary and computers; lack of arms required for a modern police force and an overall atmosphere of huge demands from all sides without adequate resources and a crippling low morale.

The Government of India has recognized the need to modernize the police in the country and has launched several initiatives. For instance, the Scheme for Modernization of State Police Forces (MPF) has been running from 1969-70. Another scheme which has been launched in 2009 is Crime and Criminal Tracking Network and Systems (CCTNS).

The Cloud can serve as an excellent delivery model for many of the above outlined schemes. Systems such as CCTNS if moved to a the Cloud can be easily accessed by several law enforcement/intelligence agencies irrespective of their jurisdiction or organizational boundaries. Further, such access will come through without any requiring additional investment from the local agencies or police force.

**Brief information about CCTNS²**

Crime and Criminal Tracking Network and Systems is a plan-scheme that aims to computerize crime & criminal records of 14,000 police stations and 6,000 supervisory offices in the country & network them with an aim to bring about improved record keeping, reducing redundant data entry, better administration of police force, providing better tools to police force for detection & investigation of crimes and providing better citizen services. Sanctioned a substantial budget of Rs. 2,000 crores on 19 June 2009 by Cabinet Committee on Economic Affairs, it is one of the ambitious and path-breaking projects under E-Governance Plan of Government of India. NCRB is implementing the project with the software being developed by Large IT services provider in India.

² [http://ncrb.gov.in/cctns.htm](http://ncrb.gov.in/cctns.htm)
Challenges in Policing

The challenges in policing – especially when it comes to record keeping and sharing – are briefly discussed below:

Lack of computerization

Lack of computerization is one of the fundamental problems with maintenance of criminal records in police stations. Records, in most police stations in the country still continue with manual record keeping procedures. Wherever desktop based computers are available, they store the data locally resulting in risk of data loss in case of local hardware failures. Hence, in spite of computerization, police stations are mandated by rules to maintain physical copies of criminal records resulting in huge duplication of records.

Difficulty in sharing information

Since records are manual, it becomes difficult to search, retrieve and share information. The difficulty in sharing information applies at all levels – whether it is other police station in the country, office of supervisory police officials or other agencies which may have interest in the information, or even with citizens.

Administrative inefficiencies

Lack of information access also cascades into administrative inefficiency, as supervisory officials cannot have access to real-time and meaningful MIS reports or set in motion important and urgent course corrections. Further, it becomes laborious to generate specific MIS reports for specific purposes, such as Parliamentary or RTI (Right to Information Act) related queries thus making the system inflexible and in many cases unusable.

Low productivity

Impact of all the above challenges is low productivity on all parameters where output is dependent upon records being kept by police stations. For instance, if an investigating officer wants to trace identity of a criminal from finger prints recorded at the crime scene, it is a huge challenge in the current environment.

Advantages of Cloud adoption in Policing

Adoption of cloud in maintenance of police records can bring in a host of benefits, which shall address many of the above challenges presented above.

Data availability

As crime and criminal records move to the Cloud, data becomes accessible to multiple stakeholders – other police stations in the country, supervisory officials, other intelligence/law enforcement agencies, policy makers and even citizens. This will mean ease in workload of police stations, efficient investigations through better information sharing among police forces, better and closer supervision of investigations, smoother intelligence sharing and quicker response to citizen queries.

Reduced costs

Once the crime and criminal records are moved to the Cloud, Police forces, National Crime Records Bureau (NCRB), or other participating agencies do not need to own, maintain and safeguard IT infrastructure for storage of this data. Cloud based IT infrastructure will be shared across multiple agencies, with adequate safeguards built in for security.

Improved inter-agency/ inter-force coordination

When crime and criminal records move to the Cloud and become shareable with other agencies, required data, after appropriate clearances, can flow in real-time to the user agency, enabling a much better coordinated response to complex law and order, crime investigation or national security situation. For example, Intelligence Bureau may need to match finger prints of a suspected terrorist in NCRB’s digitized fingerprints database or CBI may want to search a vehicle’s details in Motor Vehicle Coordination System. All such queries become much easier in a cloud based environment.

Further, the process of granting clearance for access of this data can also be centralized and built on a Cloud based workflow system to make it standardized across the country and universally actionable.

Improved administrative efficiency, productivity and citizen services

Always available information makes supervision much more meaningful, improves productivity by removing multiple data entry and makes citizen access to the police records much easier. Real time alerts can be configured for various levels of users. For instance, supervisory officers of the level of Deputy Superintendent of Police (DSP), Additional Superintendent of Police (ASP) & Superintendent of Police (SP) can be notified if a case of say murder or rape gets registered; still senior officials can be notified if there is an emergency situation; there can be separate alerts for inter-agency information sharing, which can be delivered through multiple channels of SMS, email etc.
Concerns resulting from adoption of Cloud in policing

Conversion of data in local languages to common language

Data available in crime and criminal records in police stations is regulated by that particular state’s Police Manuals and different states will have it stored in various languages. Converting that data into the common language would mean a duplication of work for the police stations.

Data security

Policing in India is a state subject and police forces in the country are organized at state level. There can be concerns over a common, cloud-based, all-India database of crime and criminal records. Further, if various law enforcement/intelligence agencies are to be given access to the data, it could also raise serious concerns about data security.

Recommendations:

- Government of India has already conceived the CCTNS which seeks to computerize crime & criminal records in the country. It is recommended that CCTNS moves to the Cloud platform.
- It is also worthwhile to move applications of various law enforcement agencies like Intelligence Bureau, Central Bureau of Investigation, Enforcement Directorate etc. on the Cloud, which will bring about cost reduction to all the participating agencies in maintaining their respective IT systems. It would also bring about better coordination in important criminal investigations and intelligence sharing.
- Intelligence agencies of the Revenue Department, such as Directorate of Revenue Intelligence, Directorate of Investigations (Income Tax) can also be given access to such a system.
- Protocols allowing for information sharing on demand by various agencies can be set up. Similarly, protocols can be set up for real-time alerts to various agencies on occurrence of an event of special significance, say a terrorist threat being received.
- In order to tackle issues relating to data security, adequate security protocols should be evolved and implemented.
Conceptual Framework for a Cloud Policy in India

Some of the countries that are leading the way in Cloud adoption are the United States of America and the United Kingdom.

The US Government is taking steps towards implementing a ‘Cloud-first’ policy that will now require federal agencies to default to Cloud-based solutions whenever a secure, reliable, cost-effective Cloud option exists. Further, by adopting the Cloud business model, the Federal Government plans to consolidate data centers through virtualization. The Federal Government website also provides a shopping cart for US Government agencies to purchase applications from a catalogue of over 3,000 Cloud-based applications. The General Services Administration of America is moving its email service to the Cloud, which is provided externally through the use of a private Cloud.

The Government of United Kingdom has also undertaken a Government wide Cloud strategy. The British Government’s G-Cloud has a hybrid Cloud structure with a public-private architecture catering to multiple Cloud communities. The British Government is also building a Government Application Store, which is expected to be the only channel for IT services procurement by the British Government.

Governments in Asia are looking at Cloud services to bring in efficiencies in their ICT (Information and Communications Technology) usage. They are looking to enhance their own ICT infrastructure and reduce ICT spending while doing so. According to a recent Frost & Sullivan study, 2011 in the Asia Pacific region, 21 percent of the respondents in the Government vertical have adopted Cloud computing in one form or the other.1

In order to reap benefits of the Cloud, the Government2 needs plan its Cloud adoption efforts. We recommend the following aspects be considered to ensure that Cloud adoption leads to the desired benefits while minimizing the risks.

The NTP recognizes the need to “To promote Research and Development, Design in cutting edge ICTE technologies, products and services for meeting the infrastructure needs of domestic and global markets with focus on security and green technologies.”

The primary step towards enabling Cloud computing in Government is the formulation of a Cloud Policy. A Cloud policy will lay a foundation for a large scale adoption of the Cloud by various Government entities. As highlighted earlier in this whitepaper the US has come up with the Cloud First policy which requires Government agencies to evaluate Cloud computing options before making any new investments. The US Government has also set up the National Institute of Standards and Technology – a federal technology agency that works with industry to develop and apply technology, measurements, and standards to be used by industry as well as Government agencies.

Similar to this initiative by the US Government, the Indian Government should come up with a policy giving direction to Government agencies to adopt Cloud as well as to the Cloud service providers inclined towards providing services to Government. The Government also needs to establish a nodal agency which shall define the standards for procurement and usage of Cloud technologies by Government agencies.

The following section details on the aspects which need to be considered for laying of guidelines on adoption of the Cloud by the Government as a Cloud user.

---

1 http://www.frost.com/vprod/servlet/cio/232651119
Service pre-requisites

The Government needs to specify minimum baselines for acceptable standards with respect to security and governance for Cloud services offered by CSP’s. Some of the requirements are:

- Statutory compliance to laws, regulations, and agency requirements. The CSP’s will comply to any policies or regulations implemented by the Government. Therefore a set of necessary rules and regulations should be created by the Government.

- Data protection requirements for classified Government data with necessary security measures. Appropriate technical and procedural controls need to be provided by the CSP for data protection.

- Privacy and confidentiality to protect against accidental and nefarious access to information. The data on the Cloud may be personal and classified and a small leak can prove hazardous. The CSP’s will have to set up privacy related controls to ensure data confidentiality. The controls should provide access restrictions for different Government agencies from accessing personal citizen records unless required for a bona-fide purpose. Data integrity controls to ensure data is authorized, complete, and accurate. All the data stored must be protected from unauthorized changes.

- Data controls and access controls to determine where data can be stored and who can access physical locations. The access to the data on the Cloud must be given only to that person, to whom the data belongs. Access control is a necessity, and will define the success of the Cloud initiative.

- Governance procedures to ensure that Cloud computing service providers are sufficiently transparent, have adequate security and management controls, and provide the information necessary for the agency to appropriately and independently assess and monitor the efficacy of those controls.

- Quality of Service: There should be a mechanism in place to ensure the service vendors adhere to a particular quality metric in the provision of their services. Ensuring this will bring about healthy competition in the market and consequently give leverage to the Government in choosing the most reliable service provider.

- Disaster Recovery and Backup plans: One of the features of Cloud services is inbuilt redundancy and resilience. However, CSP’s which provide services to Government need to be mandated with minimum acceptable downtime and redundancy requirements in case of a disaster.

The policy framework under which the Cloud will operate has to be defined in terms of the ownership and control of the data that would flow or reside in the system, or data sovereignty, the network and availability of infrastructure to facilitate the establishment of physical data centers in India.

The policy should at a minimum address the following situations with regard to use of the Cloud and its users: A Cloud to be used by the government for its e-governance initiatives and other IT operations; a public Cloud to be used by private citizens and organizations in India, which will be established and operated by a CSP; and a private Cloud to be used by private citizens and the private sector.

In more substantive terms, the policy must be developed in a sufficiently flexible manner that allows for the rapid growth the Cloud computing industry promises to achieve and to enable India’s meaningful participation in providing international Cloud services as well as in any future international agreement on Cloud computing. The policy should aim to embody the open standard this technology is based on. Set out below are the recommendations on the conceptual issues that a Cloud policy in India should address.
Data and network sovereignty

Ownership and control of data

Provisions related to ownership and control of data will depend on the form of the Cloud, i.e., whether the Cloud is a private Cloud or a public Cloud, and whether the Cloud has been established in India, and the type of data being stored or transferred to the Cloud. By way of example, a Cloud being used exclusively by the government for its various e-governance applications and also its departments will elicit a higher level of data protection and security control than a Cloud being used by organizations as a SaaS.

The policy should:

- Mandate that the ownership and control of the data remain with the respective department of the Government or Indian entity. The Government owns a lot of sensitive data such as national defense related information or personal data of the citizens. Thus ownership and the protection it offers is one of the primary concerns for any technology adoption. This will leave open the possibility of outsourcing the operation of the Cloud while retaining control over the data.

- Allow a grading or categorization of the Cloud applications or use cases. China has implemented a cyber security standard, the Multi-Level Protection Scheme (MLPS) that classifies industries into 5 levels of information security and most key industries are classified at level 3 or above. While the MLPS imposes very stringent security requirements, which are not advisable, the classification of use cases will be helpful in maintaining appropriate security protocols. So, a sector such as health care could require a more vigorous degree of security protocol given the sensitive nature of the information dealt with; the education sector on the other hand could be part of a category requiring lower security protocols.

- Require that the CSP can only store the data on physical data centers within India and that the Cloud exists within and submits to the jurisdiction of Indian courts in addition to any other jurisdiction. This standard is also endorsed by NIST and takes on more critical importance with a government dedicated Cloud.

- Provide for sufficient extra-territorial reach. Section 75 of the Information Technology Act, 2000, as amended (the IT Act) exercises extra-territorial reach to offenses committed outside India, but it is limited to acts involving a computer, computer system or computer network located in India. Legislation needs to be enacted that will make offenses involving Indian data but committed outside India, (whether the data is resting abroad or processed abroad) a punishable offense. This concern has also been raised by the Department of Personnel and Training in the context of the draft Right to Privacy Bill. In addition, India should make similar provisions a part of any multi lateral agreement with countries like USA and the EU (which boasts of a concentration of CSP).

- Establish adequate protection in the event of bankruptcy of the CSP in terms of data ownership and retrieval within a reasonable period of time and protection against disclosure during the regulatory process that follows declaration of bankruptcy.

Ownership and Control of network

The network will be the pooled resources used in the creation of the Cloud and includes the virtual machinery. While large parts of the network such as telecom services and internet services will be governed by their respective licenses and industry standards, the Cloud policy should facilitate the classification of certain key networks and systems.

The policy should:

- Provide for the identification and declaration of certain networks as ‘protected system’ under Section 70 of the IT Act which allows the government to declare a computer, a computer system or computer network as a unauthorized access or attempted access to a protected system is a punishable offense under this section. This will also help identify critical IT assets and such IT assets can receive priority in terms of location and security protocols.

- Suggest the extent to which the pooled resources should be located within India based on the various types of Clouds and their users.

---


3 Network here refers to the pooled resources used in the operation and maintenance of the Cloud and is separate from the physical data center in which this network may or may not be housed.
Privacy and security of the data

While data ownership lies in the hand of the owner or provider of the data, data security and privacy is the responsibility of the CSP. The policy should allow room for the development of a negotiated protocol between the end user and the CSP which would be appropriate in the use of the Cloud.

The policy should:

- Recommend developing separate security policies for different types of use, such as IaaS or SaaS, or for different users such as the various government departments, as the case maybe. This approach has been used by the Department of Information Technology, Ministry of Communications and Information Technology with respect to state data centers. In addition to this, the CSP could be required to provide an overarching security and privacy commitment regarding any data held on the Cloud provided by him.

- Recommend developing security protocols and authentication standards to secure end point access to the Cloud, i.e., for remote access through smart phones etc. This should include separate standards and authentication for categories of users.

- Recommend provisions relating to Cloud auditing and performance monitoring by independent parties. The results of the audit which could include an audit of the privacy and security systems measured against indices of reliability, resilience, recovery and incident handling capabilities etc, and monitoring of the Cloud performance could be made a matter of public information.

- Set out clear exceptions for the access of data on Cloud, whether used by the government or otherwise. These exceptions should be limited to national security matters and when access is authorized by appropriate authorities. This may be contrary to Section 80 of the IT Act which grants police officers and other officers the power to enter any public place and search and arrest without warrant any person who is reasonably suspected of having committed or committing an offence under the act. The standard employed should be one similar to Section 132 of the Income Tax Act, 1961, as amended (the Income Tax Act). Section 132 of the Income Tax Act provides for search and seizure of book of accounts, documents, valuable articles etc only after a notice has been summoned and has not been answered or responded to. There are provisions for exceptions to what may be seized, limitations on how long the seized materials can be retained, validity of the order for the search and seizure etc. Similarly, Section 100 of the Code of Criminal Procedure, 1973, as amended, which relates to search of property, sets out details regarding a search in accordance with the warrant, witnesses to the search and inventory of any good taken into possession consequent to the search. It is crucial that similar standards be articulated given the sensitive nature of certain data being stored on the Clouds. In addition, given the transnational character of data and the myriad paths data may take, there is a risk imposed by external regulations such as the U.S. Patriot Act. The CSP and network provider may also have privileged users such as administrators etc who carry out maintenance or managerial operations. To manage such risks, CSPs should be required to ascertain the privileged users and define their access rights for customer data.

Recommend that Cloud services maintain a high service level. Adequate disaster recovery features need to be developed to ensure the continuity of Cloud services. In this regard the NTP-2012 aims to “Prescribe sectoral Standard Operating Procedures for effective and early mitigation during disasters and emergencies.” To create appropriate regulatory framework for provision of reliable means of public communication by Telecom Service Providers during disasters.”

- Mandate inbuilt redundancy and resilience features and set minimum acceptable downtime and redundancy requirements in case of a disaster.

- An appropriate dispute resolution mechanism may be set up to resolve the specialized and technical nature of disputes that may arise in connection with Cloud computing. The protagonists of this mechanism may be appropriately qualified to understand and appreciate the technical aspects of the dispute. Alternatively, the relevant government department or body may carry out special training for judges to help increase awareness of the special nature of disputes in Cloud computing.
Data Centers

The recently released data center risk index by Cushman & Wakefield referred to earlier, is a comprehensive index indicating the most optimal location for data centers. According to this index, energy supply and provision, bandwidth and ease of doing business are the most important factors. Significantly, this report has identified India as the country with the highest risk with regard to establishing data centers. The report also identifies power quality and outages and increasing IT loads as the most significant challenges together with strict barriers to foreign ownership with respect to investment in establishing data centers in India.

A German developed certification for data centers, the datacenter star certification classifies data centers into five tiers based on audits conducted by the company. The highest certification, tier 5 data centers includes, two redundant power supplies, heat dissipation performance levels (≥ 1500 W/m²). A similar classification developed by the Uptime Institute classifies a tier IV data center (the highest categorization) as operating fault-tolerant components, such as redundant capacity components, uplinks, storage, chillers, HVAC systems, servers etc.4

Providing for these standards is of crucial importance since any problem with data centers can cause downtime in the network or the Cloud which could result in severe losses. To encourage launching data centers in India, the government has to pro-actively provide for and guarantee these standards in terms of power supply etc. Providing for physical data centers in India will also ease negotiations on privacy and security provisions of an SLA.

The policy must:

- Guarantee supply of power and other infrastructure such as heating, cooling, provision and use of water and sanitation.
- Set out standards to be achieved by the government including measures in expanding broadband connectivity throughout India and develop the broadband policy to include higher download speeds.
- Include standards for physical security of the physical structure against natural calamities like earthquakes and against fall outs of political turmoil.
- Provide for other incentives such as tax breaks that will help lower over head costs related to total cost of ownership.

Other Provisions

- The foreign direct investment policy will have to be amended to include clear provisions regarding establishing data centers, security and lock-in provisions and other provisions for Cloud service providers. In addition, the Government will need to define how Cloud services will be taxed.
- Government IT procurement rules related to purchase of IT equipment will need to be amended to encourage Cloud use.
- In the long run the government will have to ensure that a handful of CSPs do not attain a dominant position in the market, that the market remains competitive and that the barriers of entry to the Cloud industry are low.
- Specifically, for any Cloud that the government may use or adopt, the following may be considered as key ‘customizations’ that will be required in light of the discussion in this white paper:
  - Accessibility to all sections of society including people in remote areas and to those who are differently abled.
  - Easy functionality on a multi-lingual platform and ability of services to provide information across languages by usage of translation technologies.
  - Ability to work on low bandwidth / offline: The state of internet connectivity in India is currently not at par with the rest of the world. While efforts are being made to upgrade the internet infrastructure, it is important that Cloud offerings for Government usage should be able to function smoothly even on low bandwidth or in conditions with intermittent or irregular connectivity.
  - Use of existing facilities: Utilization of existing Government facilities for Government-aided initiatives will help in keeping costs under control. For example, NIC owned data centers can be utilized to house common Cloud services to be used by other local Governments as well.
  - Interoperability: e-Governance solutions will span across multiple Government agencies and utilize data maintained by different agencies. In this context it is important that Cloud services for Government are built on open standards such that the services can interoperate and also pave way for new public utility platforms to be built on top of it.

• Ultimately, to undertake this policy and build on the Cloud infrastructure, India may require a dedicated nodal agency. This agency could be a quasi regulatory authority that can be tasked with articulating a Cloud policy based on the broad concepts provided above and acting as an ombudsman to all the relevant stakeholders in the Cloud sector. This is consistent with the recommendations of the NTP-2012 also recommends “setting up [of] a council consisting of experts from Telecom Service Providers, Telecom Manufacturing Industry, Government, Academia and R&D institutions. The council will
  – Carry out technology and product development forecast.
  – Evolve, and periodically update the national program for technology/product development.
  – Be a nodal group to monitor and ensure the implementation of various recommendations made for promoting indigenous R&D, IPR creation, and manufacturing and deployment of products and services.”

• Existing regulators such as the Reserve Bank of India (RBI) or Telecom Regulatory Authority of India (TRAI), Insurance Regulatory Development Authority (IRDA), and Securities Exchange Board of India (SEBI) will have to be directed to develop guidelines keeping in mind how the Cloud can potentially affect the entities they regulate. This is relevant to regulators across sectors but especially in sectors such as Financial Services and telecommunications who have traditionally been heavy users of information technologies.

• Define rules on foreign investments and taxation relating to Cloud services. The Government shall need to define its stance on how Cloud services will be taxed and the applicable taxation laws to certain services which may be packaged as products. In addition, the subject of encouraging CSPs to set up in India also needs to be addressed by definition of clear rules for allowing foreign investment and offering tax exemptions to CSPs who set up in India. In this regard the NTP recommends “Evolving a framework for financing the sector and streamlining taxes and levies for long term sustainability of telecom sector.”
Conclusion

The Cloud promises to revolutionize not just the Government but also industry as a whole. Further, the Cloud presents tremendous opportunities to fast track the healthcare and education sector in India. However, it will require careful development of a national Cloud strategy to ensure that maximum benefits of the Cloud accrue to the nation while minimizing the risks.

In essence, the Government needs to play a pivotal role in ensuring that Indian entities can take advantage of the Cloud revolution for economic growth without being encumbered by the challenges and risks arising from the Cloud.

The Government needs to work on dual goals of (1) protecting interests of Indian entities in relation to risks from Cloud adoption and (2) accelerating the adoption of Cloud in India. This will be possible only with cooperation between various government agencies and departments anchored by key ministries. The NTP-2012 also plans “to exploit individual strengths of organizations under DoT/DIT to their mutual benefit for ensuring these organizations to effectively flourish in the competitive telecom market while adequately supporting the security needs of the country.”

Summarized below is an illustration of indicative recommendation to lay a foundation for adoption of Cloud in India:

The key steps to be taken as per the above illustration are:

- Creation of a nodal agency for laying baselines for Cloud adoption.
- Empowering the nodal agency to develop a Cloud policy for adoption of Cloud by Govt. bodies and Indian citizens and organizations.
- Empowering the nodal agency to interpret existing laws such as IT Act 2000 in context of Cloud to ensure the interest of Indian entities in the Cloud.
- Empowering nodal agency to work with various government departments and ministries including state government to incentivize Cloud adoption in India.
- Launching specific projects in the area of Healthcare and Education for accelerating use cases outlined in this whitepaper.
- Defining policies and enact rules / regulations for incentivizing setup of Cloud providers in India.
The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the growth of industry in India, partnering industry and government alike through advisory and consultative processes.

CII is a non-government, not-for-profit, industry led and industry managed organisation, playing a proactive role in India’s development process. Founded over 117 years ago, it is India’s premier business association, with a direct membership of over 7100 organisations from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 90,000 companies from around 250 national and regional sectoral associations.

CII catalyses change by working closely with government on policy issues, enhancing efficiency, competitiveness and expanding business opportunities for industry through a range of specialised services and global linkages. It also provides a platform for sectoral consensus building and networking. Major emphasis is laid on projecting a positive image of business, assisting industry to identify and execute corporate citizenship programmes. Partnerships with over 120 NGOs across the country carry forward our initiatives in integrated and inclusive development, which include health, education, livelihood, diversity management, skill development and water, to name a few.

The CII Theme for 2012-13, ‘Reviving Economic Growth: Reforms and Governance,’ accords top priority to restoring the growth trajectory of the nation, while building Global Competitiveness, Inclusivity and Sustainability. Towards this, CII advocacy will focus on structural reforms, both at the Centre and in the States, and effective governance, while taking efforts and initiatives in Affirmative Action, Skill Development, and International Engagement to the next level.

With 63 offices including 10 Centres of Excellence in India, and 7 overseas offices in Australia, China, France, Singapore, South Africa, UK, and USA, as well as institutional partnerships with 223 counterpart organisations in 90 countries, CII serves as a reference point for Indian industry and the international business community.

Confederation of Indian Industry
The Mantosh Sondhi Centre
23, Institutional Area, Lodi Road, New Delhi – 110 003 (India)
T: 91 11 24629994-7 • F: 91 11 24626149
E: info@cii.in • W: www.cii.in

Reach us via our Membership Helpline: 00-91-11-435 46244 / 00-91-99104 46244

About CII
About KPMG in India

KPMG in India, a professional services firm, is the Indian member firm of KPMG International and was established in September 1993. Our professionals leverage the global network of firms, providing detailed knowledge of local laws, regulations, markets and competition. KPMG in India provide services to over 4,500 international and national clients, in India. KPMG has offices across India in Delhi, Chandigarh, Ahmedabad, Mumbai, Pune, Chennai, Bangalore, Kochi, Hyderabad and Kolkata. The Indian firm has access to more than 5,000 Indian and expatriate professionals, many of whom are internationally trained. We strive to provide rapid, performance-based, industry-focused and technology-enabled services, which reflect a shared knowledge of global and local industries and our experience of the Indian business environment.

KPMG is a global network of professional firms providing Audit, Tax and Advisory services. We operate in 152 countries and have 145,000 people working in member firms around the world.

Our Audit practice endeavors to provide robust and risk based audit services that address our firms’ clients’ strategic priorities and business processes.

KPMG’s Tax services are designed to reflect the unique needs and objectives of each client, whether we are dealing with the tax aspects of a cross-border acquisition or developing and helping to implement a global transfer pricing strategy. In practical terms that means, KPMG firms’ work with their clients to assist them in achieving effective tax compliance and managing tax risks, while helping to control costs.

KPMG Advisory professionals provide advice and assistance to enable companies, intermediaries and public sector bodies to mitigate risk, improve performance, and create value. KPMG firms provide a wide range of Risk Consulting, Management Consulting and Transactions & Restructuring services that can help clients respond to immediate needs as well as put in place the strategies for the longer term.
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.