IndraStra
www.indrastra.com | ISSN 2381-3652

MeghRaj — India's Cloud Initiative

indrastra.com/2018/04/MeghRaj-India-s-Cloud-Initiative-004-04-2018-005.html

By IndraStra Global Editorial Team

India has embarked on **MeghRaj**, a *National Cloud Initiative* aimed at hosting various government applications and services on the cloud. A common cloud platform can further enable local governments and it's instrumentalities to adopt e-Governance for rendering better citizen services, without requiring the setting up of significant IT infrastructure. The *National Cloud Initiative* 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 *Platform as a Service (PaaS)* and*Infrastructure as a Service (IaaS)*

In view of the **National Telecom Policy 2012**, the *Department of Telecommunications (DoT)* requested *Telecom Regulatory Authority of India (TRAI)*to examine the adoption of cloud computing services by government departments. The examination was initiated on the following points;

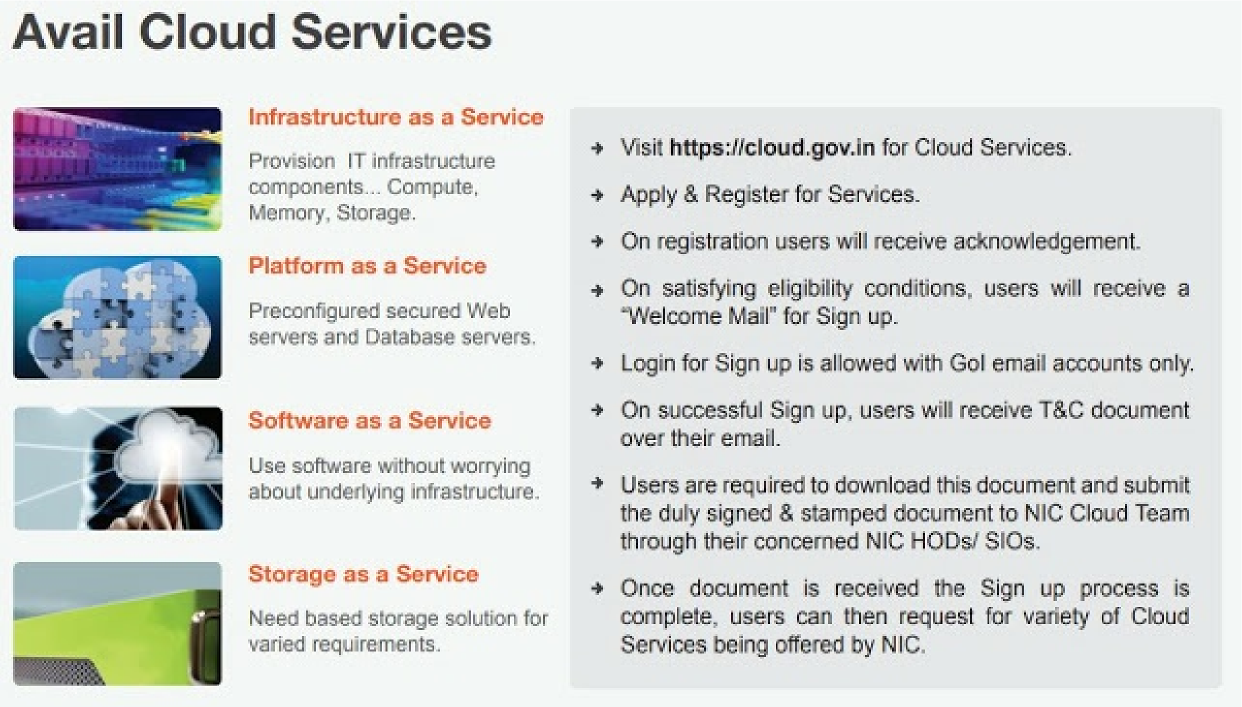
Government's adoption of cloud services (including the requirement of a separate cloud for the government);

- Steps for enhancement of cloud infrastructure in India;
- Cost-benefit analysis of adoption of cloud services; and

  Infrastructure challenges for the establishment of data centers (with relevance to the central, state and local governments).

In April 2013, *Government of India (GoI)* issued ***GI Cloud (Meghraj) Strategic Direction Paper*** along with ***GI Cloud (Meghraj) Adoption and Implementation Roadmap***. Through these papers, the GI Cloud was envisioned by the GoI to establish national and state data center assets (adapted for the cloud through virtualization) and connected through existing network infrastructure such as the *State Wide Area Networks (SWANs)*, *National Knowledge Network (NKN)*, as well as the internet. Based on demand assessment and taking into account security-related considerations, the paper suggested that government may also engage the services of private *cloud service providers (CSPs).*

On February 4, 2014, Former Union Minister of Communications and Information Technology, Kapil Sibal, **launched the National Cloud** under *"MeghRaj"* Initiative. Some of the features of the National Cloud included self-service portal, multiple Cloud solutions, secured *Virtual Private Network (VPN)* access and multi-location Cloud based on nodes which were set up across India in **National Data Centres** of *National Informatics Centre (NIC)*. This gave Departments a choice of hosting their applications in any of the nodes.



Avail Cloud Services

Infrastructure as a Service

Provision IT infrastructure components... Compute, Memory, Storage.

Platform as a Service

Preconfigured secured Web servers and Database servers.

Software as a Service

Use software without worrying about underlying infrastructure.

Storage as a Service

Need based storage solution for varied requirements.

- Visit **https://cloud.gov.in** for Cloud Services.
- Apply & Register for Services.
- On registration users will receive acknowledgement.
- On satisfying eligibility conditions, users will receive a "Welcome Mail" for Sign up.
- Login for Sign up is allowed with GoI email accounts only.
- On successful Sign up, users will receive T&C document over their email.
- Users are required to download this document and submit the duly signed & stamped document to NIC Cloud Team through their concerned NIC HODs/ SIOs.
- Once document is received the Sign up process is complete, users can then request for variety of Cloud Services being offered by NIC.

*Image Attribute: The screenshot taken from the **MeghRaj's Services Brochure***

NIC has setup Data Centres at Delhi, Hyderabad, Pune and is in the process of setting a National Data Centre at Bhubaneswar. NIC Data Centres provide shared hosting, co-location and now Cloud Services to the Government across India. Besides this, mini Data Centres are operational in all NIC State Centres to cater to the e-Governance requirements at the state level. These Data Centres provide round-the-clock operations and management of systems with onsite skilled personnel.

On June 10, 2016, *Telecom Regulatory Authority of India (TRAI)*issued a ***Consultation Paper on Cloud Computing ("CP")*** to identify and analyze industry issues in the cloud computing sector. The CP sought inputs from the public and industry stakeholders on the proliferation of cloud computing services and the requirement (if any) for regulation in the industry. The TRAI also sought inputs on specific issues including issues relating to the quality of service requirements, data security in the cloud, data portability, the location of data, billing and metering concerns etc.

According to **an analyst**, associated with Mumbai-based Nishith Desai Associates - *"the consulting paper seems to suggest a legal regime for cloud computing services; in fact, a licensing regime. This will amount to over-regulation. On the one hand, the paper says that CSPs may behave monopolistically and on the other hand it seeks to create entry barriers by introducing a licensing system."*

On April 3, 2017, the TRAI conducted an *open house discussion (OHD)* on the issues raised in CP. Industry representatives including some of the biggest technology and software companies globally and in India, including the likes of Microsoft, Amazon, Reliance Communications, Reliance Jio, Vodafone, AT&T, Oracle, etc. participated in the OHD. The participants were of a unanimous view that there was no requirement for a regulatory framework for the cloud computing industry and that excessive regulation and Government interference *'will kill the cloud in India'*. Representatives of the industry suggested a 'light tough regulatory approach' consisting of broad guidelines.

On April 21, 2017, The *Ministry of Electronics and Information Technology (MeitY)*issued guidelines on setting up of IT infrastructure by government departments using cloud computing technology with a clause mandating that all data must be stored within the country.

The guidelines do not discriminate based on the nationality of the vendor, but they do envisage the establishment of a panel of pre-approved CSPs. However, the notification for invitation released in May 2017 encourages entities that have not been empanelled to submit proposals, which would allow them to provide cloud services to the government if their applications for empanelment are accepted.

According to these guidelines, one of the most critical issues that need to be addressed in the *Cloud Service Agreement (CSA)* is the security of the data with respect to CSPs. This issue further poses a significant risk if the data is sensitive in nature. The ministry suggested following contractual terms which may be included in the agreements.

At the same time, there is growing interest in certifications in India, although no comprehensive laws or requirements are in place at this stage. The **National Cyber Security Policy 2013** briefly mentions the need to comply with global security standards but provides no further details. However, according to the latest MeitY guidelines, Departments need to ensure that the CSPs facilities/services are certified to be compliant with the following standards based on the project requirements:

ISO 27001 - Data Center and the cloud services should be certified for the latest version of the standards.

ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.

ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds.

ISO 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services.

PCI DSS - compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud – This standard is required if the transactions involve credit card payments.

MeitY with the help of *Standardisation Testing and Quality Certification (STQC)* is carrying out the audit and is in the process of certifying the service offerings of CSPs for the above-mentioned standards. Therefore, MeitY suggests, the respective departments may include the following clauses in their agreements;

The CSP shall comply or meet any security requirements applicable to CSPs published (or to be published) by MeitY or any standards body setup / recognized by GoI from time to time and notified to the CSP by MeitY as a mandatory standard

The CSP shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC (*The Departments may refer the Information Classification, National Information Security Policy, and Guidelines, Ministry of Home Affairs (MHA) while choosing to deploy on the cloud)*

Guidelines under the **GI Cloud Initiative (MeghRaj) policy mandate** that service providers offering cloud services to government agencies must ensure that all services provided, including data, will be guaranteed to reside in India.
There are specific data and server localization requirements on public records and data owned by the Government of India, imposed through regulatory structures and procurement contracts, For example, the National Data Sharing and Accessibility Policy imposes data localization requirements for weather data, undermining the capability of ICT companies to offer smarter cities and disaster management solutions.

There are also restrictions on the cross-border transfer of Government of India data under the **Public Records Act of 1993**, which prevents any person from taking public records out of India without the prior approval of the Central Government. However, there are no mandatory requirements directly applicable to private data collection by ICT companies.

Currently, there are 11 CSPs empanelled with the GoI for providing cloud computing services to government departments which include Microsoft Corporation, Hewlett Packard, IBM India, Tata Communications, Bharat Sanchar Nigam Limited (BSNL), Net Magic IT Services, Sify Technologies and CtrlS Data Centers. As of December 16, 2017, *Amazon Web Services (AWS)* has already been empanelled, while Microsoft and IBM were added by the third week of the December (2017). Bharti Airtel and Reliance Jio – the other two companies are in the process of getting empanelled with the government as CSPs.

Findings by BSA (The Software Alliance)

According to **BSA's 2018 Global Cloud Computing Scorecard**, India's ranking now has slid down to 20th out of 24 leading IT economies, compared to its ranking of 18th in 2016. The legal and regulatory environment for cloud computing in India is perhaps restricting cloud innovation in India, suggests the study.

The study highlights several other factors also, which might have affected India's ranking:

Laws and regulations in India have not entirely kept pace with developments in cloud computing, and some gaps exist in key areas of data protection; notably, India has not yet implemented effective privacy legislation, although work is underway to address this issue, say the study.

India has a comprehensive national cybersecurity strategy in place and strong cybercrime legislation. Some laws and standards in India are not technology neutral (e.g., electronic signatures), and these may be a barrier to interoperability.

This year's report notes that India imposes some local security testing requirements in addition to international testing requirements. These local testing arrangements have been the subject of criticism by India's trading partners, including the European Union.

There is a substantial gap in trade secrets protection in India, as there is no specific legislation in the country to handle and protect confidential information. Nevertheless, Indian courts have upheld trade secret protection on basis of principles of equity, and at times, upon a common law action of breach of confidence, which in effect amounts a breach of contractual obligation.

In addition, guidance for examiners on how to evaluate patent applications for software-enabled inventions is lacking, although the revocation of guidelines that would have prevented most computer-related inventions from being subject to patent protection if the novel hardware was not present is a step in the right direction. Furthermore, India still has not ratified the WIPO Copyright Treaty.