Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review of Cloud Adoption Strategy for Indian Government

Dr.Ananthi Seshasaayee
Head PG & Research, Dept. of Computer Science
India

Sreevidya Subramanian*
Research Scholar, Vels University
India

Abstract— In this paper, we try to highlight the necessity of Governments to nurture cloud as a means to reduce expenditures arising out of Information Technology (IT).This paper will perform a deep dive analysis to review and investigate the potential savings of the government, focusing on IT data Centres and using a cost model that will boost government IT programs. This in-turn will invoke reduction of unemployment by giving the local IT sectors a chance for providing a significant long term cost savings through the adoption of cloud computing technologies.

Keywords— Hybrid Cloud, Grid, IaaS, CaaS, PaaS,Virtualization

I. INTRODUCTION

We often term our country as a developing country. What typically means by this term? Are we really in the same pace as that of other developing countries? This is largely a question of convenience for those who want to end up in debate programmes in the media. What is the key take away at the end of each of these debates and what we end up implementing as a result of these are crucial for our betterment and development. Government has thought of doing an IT Reform ("Re-formation") to enable utilization of cloud in to its data centres and to reduce not only the carbon foot print but also to reduce the overall total cost of operation. Let's do an in-depth review and analyse the goals set for the future by emphasizing the important criteria's for moving to cloud based governance.

Indian government announced a plan to convert the data centres that are currently being built for each of the state governments in to privately run private clouds. This ideal thought process eventually started in 2010, when the National e-Governance Plan was first made available to the common man via the internet. It was also decided that 16 of the state data centres will be built by end of 2010. But later on, the government wanted to change the setup and launched a revision to this plan by wanting these data centres to run on private clouds.

Reason for such decisions:

1) Long IT Infrastructure Procurement Cycles
2) Underutilization of resources
3) Lack of dynamic scalability
4) Lack of Proper Disaster Recovery model and drills.
5) Lack of Training schedules to educate Government staffs to move to IT operations.

II. CLOUD'S INFLUENCE TO DEVELOPMENT INITIATIVES

GI Cloud Initiative

This year February, the most awaited National Cloud initiative was moved in GOI and they had marked this as one of the vision for 2020. It is assumed that in 2020 the nation's population will hit an all-time high and hence the education and standard of living will demand a better living sphere for all the people. The very idea of adopting cloud stems its root from the J&K Government who were the first to implement this on a full scale. They had already established a cloud based e-Governance for issuance of birth and death certificates ration cards and other services.

This will also serve beneficial to share applications across departments and ministries with ease and having very less cost and pain of vendors providing a huge opportunity to promote e-governance and social development through mobile cloud. India's cloud computing policy is ranked 17th among 24 countries by the BSA Global Cloud Computing scorecard, which eventually shows our lack of interest in moving towards a greener and much better economy.

Initiative ≠ Everything

Many of the world's fastest growing economy are still considerate in facing the after effects of implementing cloud. The concern is more towards having a secure and stable environment. Considering Cloud for Government is of more importance than private sectors due to the fact that the nation's confidential data will be moved through in the cloud. In fact, many of the governments around the world are grappling with the security issues of cloud environment.

Key Pillars of NeGP

The following are considered the key pillars of National e-Governance Policy:

- State Wide Area Networks (SWAN)
- State Data Centres (SDC)
- National Service Delivery Gateway (NSDG)
- State Service Delivery Gateways (SSDG)

- Common Service Centres (CSC)

Other initiatives are also in pipeline namely, National Data Centres (NDC), National Knowledge Network (NKN), National Optical Fibre Network (NOFN) and Cloud Task Force (CTF).

III. AREAS OF FOCUS FOR CLOUD ADOPTION – THE RIGHT APPROACH

Selecting a Cloud Service: Choosing the appropriate cloud service and deployment model is the critical first step in procuring cloud services;

CSP and End-User Agreements*:* Terms of Service and all CSP/customer required agreements need to be integrated fully into cloud contracts;

Service Level Agreements (SLAs): SLAs need to define performance with clear terms and definitions, demonstrate how performance is being measured, and what enforcement mechanisms are in place to ensure SLAs are met;

CSP, governing bodies, and Integrator Roles and Responsibilities: Careful delineation between the responsibilities and relationships among the Government agency, integrators, and the CSP are needed in order to effectively manage cloud services;

Security Standards: The uses of the NIST cloud reference architecture as well as agency involvement in standards are necessary for cloud procurements; Governing Bodies must clearly detail the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment;

Privacy & Audit: If cloud services host "privacy data," agencies must adequately identify potential privacy risks and responsibilities and address these needs in the contract; If the decision is made for migration of sensitive information on to cloud then stringent measures need to be identified in order to perform regular audits;

E-Discovery: Governing Bodies must ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed, and produced;

Right to Information Act: Governing Bodies must ensure that all data stored in a CSP environment is available for appropriate handling under the RTI act; and

E-Records: Government must ensure CSP's understood and assist them in compliance in accordance with the law.

These ten unique areas of focus are not an exhaustive list of unique issues with cloud computing. Through government working reviews of existing cloud contracts, reviewing industry and academia papers and studies, and speaking with procurement and legal experts across the Government, these ten areas are to be identified as requiring the most attention at this time.

Selecting the right cloud service

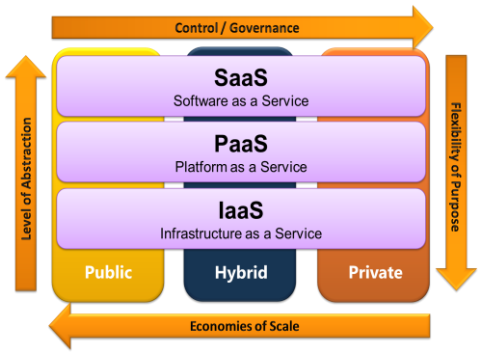
The primary driver behind purchasing any new IT service is to effectively meet a commodity, support, or mission requirement that the agency has. Choosing the cloud is only the first step in this analysis. It is also critical for Government agencies to decide which cloud service and deployment model best meets their needs.

A. Cloud Architecture

The National Institute of Standards and Technology (NIST) has defined three cloud computing service models and three Deployment models as given in the below diagram

Service Models	Description
Infrastructure	Provision Storage, Processor, Networking and other computing resources
Platform	Deployment of applications, libraries, services and tools
Software	Use of applications running on Cloud Infrastructure

Deployment Models	Description
Public Cloud	Does not allow a consumer to know or control who the other consumers of a cloud provider's environment are.
Private Cloud	can allow for ultimate control in selecting and accessing cloud
Community / Hybrid Cloud	Allow for a mixed degree of control and knowledge of other consumers



CSP and End-User Agreements

CSPs enforce common acceptable use standards across all users to effectively maintain how a consumer uses a CSP environment. Thus, use of a CSP environment usually requires Government agency end-users to sign the following:

1. Terms of Service Agreements (TOS) - TOS restrict the ways Government agency consumers can use CSP environments.
2. Non-Disclosure Agreements (NDAs) - These are usually requested by Government bodiesin order to ensure that CSP personnel protect non-public information that is procurement-sensitive, or affects pre-decisional policy, physical security, etc.

Service Level Agreements

1. Service Level Agreements (SLAs) are agreements under the umbrella of the overall cloud computing contract between a CSP and a Government agency.
2. SLAs define acceptable service levels to be provided by the CSP to its customers in measurable terms.
3. The ability of a CSP to perform at acceptable levels is consistent among SLAs.
4. SLAs should clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.) and require CSPs to monitor their service levels, provide timely notification of a failure to meet the SLAs, and evidence that problems have been resolved or mitigated
5. In order to incentivize CSPs to meet the contract terms, there should be a credible consequence (for example, a monetary or service credit), thus SLA set must include provisions for penalties if an SLA is not met.

CSP, Agency, and Integrator Roles and Responsibilities

There must be clear RACI matrix between CSP, Integrators and the Enterprise regarding the roles and responsibilities.

Security Standards

1. Standards Developing Organizations (SDOs) are continuing to develop conceptual models, reference architectures, and standards to facilitate communication, data exchange, and security for cloud computing applications.
2. Placing Government data on an information system involves risk, so it is critical for Government to ensure that the IT environment in which they are storing and accessing data is secure.
3. As such, all IT systems used by Government must meet the Regulations and Compliance requirements and related specific policies.
4. After the CSP's environment has gone through a security authorization, a Government must review the risks posed by placing Government data in that system, and if this risk level is acceptable, the agency may grant an authority to operate (ATO).

Privacy & Audit

Indian law had no stringent provisions dealing with privacy protection. The enactment of the Right to Information Act, 2005 gave a fillip to transparency in government dealings and concurrently provided some protection against the unwarranted disclosure of confidential information under that law. Stringent laws are to be enacted to avoid any data loss or theft. Audit Regulation requires Government bodiesto preserve audit logs:

- All audit/transaction files should be made available to authorized personnel in read only mode;
- Audit transaction records should never be modified or deleted;
- Access to online audit logs should be strictly controlled. Only authorized users may be allowed to access audit transaction files; and
- Audit/transaction records should be backed up and stored safely off site per agency direction.

E-Discovery

Government will have to locate, preserve, collect, process, review, and produce ESI that resides in CSP environments. Five key e-discovery areas have been identified for Government bodiesto consider when implementing cloud solutions:

1. Information management
2. Locating relevant documents
3. Preservation of data
4. Movement of documents and
5. Potential cost avoidance through the incorporation of e-discovery tools in CSP environments.

Right to Information Act

The Right to Information (RTI) Act also requires every public authority to computerise their records for wide dissemination and to pro-actively publish certain categories of information so that the citizens need minimum recourse to request for information formally.

E-Records

Record Management has always remained a critical activity of the government departments, as it is viewed as key to efficient administration. The Department of Administrative Reforms and Public Grievances must formulate proper guidelines on Record Management and preparation of Record Retention Schedule (RRS) for records common to all Ministries/Departments of Government of India to ensure that there is uniformity in retention schedule of records of common nature.

IV. CONCLUSION

Government bodies are adopting cloud computing services more and more rapidly. In this paper, we have analysed the important aspects to select the right cloud adoption model and based on all these rules and criteria's it is easy for us to step in to the much hyped cloud domain. As a conclusion we have highlighted a success story that was implemented for Government of Maharashtra (MahaGov Initiative). We conclude that similar approach needs to be rolled out to other states and monitored. The key criteria and features are listed below which serves as a role model for other governments to operate on.

TABLE I – Cloud Initiative Success Story of Maharashtra

MahaGov - Cloud Initiative				
Salient Features	**Key Achievements**	**Key Challenges**	**Replicable Features**	**Scalability**
MahaGov Cloud is the only State Government Cloud Setup in India.	Reduction in time for provisioning of infrastructure.	Start with – IaaS and PaaS before implementing SaaS.	The same cloud model can be adopted by other states.	On the fly scalability.
Only State Data Centre in India to be a member of APNIC/IRINN, making it vendor independent for ISP.	Efficiently utilize the resources as and when required.	Capacity planning needs to be done. CPU and RAM – should be in ratio. Licensing Policy – OS & DB.	Lower cost of ownership/operation.	Self-provisioning of resources.
First model in India where the Cloud services are offered for Government and by Govt.	Reduce downtime required for maintenance activity.	Public and Management Traffic –NICs to be sized.	Easy to provision Compute resources.	Automated resource allocation.
A rate chart for the same has been published.	Ease of management of huge infra available in SDC.	Backup and Replication – for entire Virtual Instance.	Latest technological updates.	Charges based on usage.
Maharashtra SDC is the only State Data Centre in India to complete IPv6 PoC	Auto scaling of resources based on utilization.	Awareness sessions – departments and developers.	Anytime, Anywhere Access	Better quality of service and performance.

ACKNOWLEDGMENT

My sincere thanks to my guide Dr.Mrs.Ananthi Seshasaayee who has always been motivating to me and helped me achieve my research writing cum analysis techniques.

REFERENCES

[1] Cloud Strategy and Indian Government Initiatives - http://deity.gov.in/content/gi-cloud-initiative-meghraj.
[2] WTO Released National cloud strategy - http://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/national_cloud_comp_e.pdf.
[3] Frost & Sullivan 2011 – Market Insight by Arun Chandrasekaran & Mayank Kapoor.
[4] http://www.cii.in/cloudreport - The Indian Cloud Revolution Report from CII.
[5] The Cloud Advantage for Education - http://newindianexpress.com/education/edex/The-cloud-advantage/2013/07/29/article1703684.ece.
[6] Indian Government decision to move its data centers to cloud - http://www.information-age.com/technology/cloud-and-virtualisation/2115938/india-government-to-convert-data-centres-into-clouds
[7] http://articles.economictimes.indiatimes.com/2013-05-07/news/39091309_1_cloud-computing-public-cloud-cloud-strategy - An India times exclusive report.
[8] http://www.enterpriseefficiency.com/author.asp?section_id=2405&doc_id=261933 – A Roadmap release.

[9] http://www.nextbigwhat.com/cloud-computing-policy-framework-from-indian-government-297/ - Analysis of adoption rate and readiness.
[10] http://www.ciol.com/ciol/features/186703/cloud-governance-why-indias-adoption-low.
[11] http://www.ibm.com/smarterplanet/in/en/smarter_cities/solutions/solution/B235026Q03312B40.html - Smart solution for governments.

