Comments:
Consultation Paper on "Cloud Computing"

Sistema Shyam TeleServices Limited (SSTL) welcomes the opportunity extended by TRAI to comment on its consultation paper on "Cloud Computing".

Our specific comment on the issues raised in the consultation paper is as below:

Q1. What are the paradigms of cost benefit analysis especially in terms of:
a) accelerating the design and roll out of services.
b) Promotion of social networking, participative governance and e-commerce.
c) Expansion of new services.
d) Any other items or technologies. Please support your views with relevant data.

1. The key cost components for designing and roll out of services are cost of servers, network, software cost, power and cooling cost, real estate and facility cost, support and maintenance cost, people cost.

2. Since these costs are very high for rolling out new services, the time taken for realizing the benefits from the services is also long. Consequently for smaller organizations investment in IT becomes a barrier for business growth, which does not have the required financial capacity to make large initial capital investments.

3. Larger organizations often employ various tools such as NPV (Net Present Value), or ROI (Return of investment), payback period to calculate the return on their investment made on IT.

4. Social networking platforms are generally available on cloud and enable organizations to launch their marketing campaigns in a timely manner and also offer various customer services.

5. This helps organizations to lower their marketing costs, getting quicker customer feedback and participative governance helps conceptualizing government flagship programs through crowd sourcing using cloud platforms.

6. Expansion of services requires augmenting infrastructure based on projected demand, however in case of any surge in demand, the fulfillment becomes difficult. In case of cloud based model, such scalability is inherent in the service model and hence it adds value for the service recipient.

Q2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organization?

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

1. Supply-side savings- Large-scale Data Centers (DCs) with lower costs per server due to reduced power and space cost along with low maintenance cost. Optimal use of their computing resource and large volume helps to reduce the procurement cost of hardware and software licenses.

2. Demand-side aggregation- Aggregating demand from cloud computing helps improving the utilization level of computing resources. Class of service and feature availability will improve as the demand will be consolidated.

3. Multi-tenancy efficiency- When changing to a multitenant application model, increasing the number of tenants (i.e. customers or users) lowers the application management and server cost per tenant.

Q3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

Choosing a cloud deployment model is a multivariate problem, cost is a key factor in determining a deployment model. Emphasizing an understanding of cloud cost is critical when selecting a type of deployment.

1. Endogenous factors like nature of the application, service availability (QOS), existing investment in IT infrastructure, regulatory/data security requirement, defined and available budget for the business enterprise are important parameter in selecting a deployment model.

2. Exogenous factors such market structure of cloud services (availability of number of players/providers), ongoing Industry trend for cloud adoption, governance framework etc. also has a bearing on selecting the cloud model.

3. Private cloud is generally deployed in large organization where consolidation and optimum utilization of hardware and data security is of prime concern without losing control over organizational data.

4. Private cloud is heavy on CapEx and personnel -- both of which are fixed costs, although over a medium term whereas a public cloud is primarily OpEx -- which conversely is primarily a variable cost, over either the short or medium-term depending on the cloud subscription model.

5. Large business setup may afford and opt to take the Private cloud deployment model whereas a SME may choose for Public Cloud. Depending on the need and requirement both can opt for Hybrid which is a mixed of Private and Public.

Q4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?

Following factors needs to be considered for secured migration path:

1. Technical interoperability
2. Syntactic interoperability
3. Semantic interoperability
4. Organizational interoperability
5. Data Portability
6. System/Application Portability

Q5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

1. Interoperability and System Portability of Cloud service.
2. Facilitate and Support development of interoperability standards.
3. During closure of business, cloud provider should be obligated to support porting of its customers to another provider.
4. Encryption of Data to ensure Data Security.

5. Restrict Cross-border movement of data.

Q6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

The Cloud framework should promote open stack platforms with standard API's, plugins sharable with all the partners, availability of latest software updates/upgrades, and compatibility with legacy software's and platforms. When using open source platforms cloud service providers should use secure coding practices with emphasis on output quality checks.

Q7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.

The desired QoS parameters should be benchmarked against guaranteed access to data and services, performance, security, resilience, reliability, self-service portals, response time and customer support, metering and billing accuracy, support in compliance of regulations. Regulatory and governing body should periodically publish QoS dashboards for all the cloud services providers.

Q8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

1. Cloud service provider should facilitate real time reporting on allocation and utilization of cloud resources, transparent reporting on SLA performances, and alert notification on billing threshold for protection of Bill shock.
2. Disputes should be addressed and resolved in accordance with signed agreement and if required help should be taken from Tribunal body or commission similar to TDSAT.
3. Cloud services contracts should focus on areas such as: Terms of Services (ToS), Acceptable Use Policies (AUP), privacy /security policy, Service Level Agreements (SLAs), etc.

Q9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.

1. Cloud service providers should publish escalation matrix for handling customer complaints.
2. Chief grievance officer name must be published on the website of CSP.
3. Multi-channel communication platforms should be in place for logging online complaint.
4. Customers should be guaranteed response within the agreed timelines.
5. There should be a review mechanism to audit and help in identifying shortcomings in the complaint handling process.
6. Regulatory body should also have a customer grievance redress cell for addressing customer escalations.

Q10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

Cloud Security Guidance should be put in place as per below provisions:

1. Ensure effective governance, risk and compliance processes exist.
2. Audit operational & business processes.
3. Manage people, roles and identities.
4. Ensure proper protection of data and information.
5. Enforce privacy policies.
6. Assess the security controls by 3rd party and obtain compliance certification.
7. Contract between the CSP and client must contain the specific security controls to be put in place, along with deterrence, if any.
8. The exit or termination specific data security requirements must be specified in the contract.

Q11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

1. Data transfer or data handling mechanism must be specified in the contract between the service provider and consumer specifically in the event of a termination/exit of the contract by either party.
2. The provision should include knowledge transfer, data handover, data cleansing, etc.

3. The service provider should provide data cleansing certificate to customer which will be subject to audit.

Q12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

1. Network level segregation for each client to be maintained through virtual LAN.
2. Data during transition should be encrypted with multi-level authentication (minimum two level controls).
3. Admin access to be maintained and access should be provided through Privilege Identity Management system.
4. Customer should have the knowledge of the location of the data hosted on the cloud.
5. Entire audit trail should be maintained by CSP for evaluation/tracking.
6. Information assurance process and tools to be employed to ensure confidentiality, integrity and availability of data assets.
7. Transparency in sharing security events with the clients.
8. Contracts must contain provision to protect clients from any kind of lock-in imposed by CSP.

Q13. What should be the roles and responsibilities in terms of security of
(a) Cloud Service Provider (CSP); and
(b) End users?

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

CSP:

1. Cloud service provider should maintain data segregation and confidentiality in the cloud.
2. In the event of termination/exit of contract, CSP must ensure cleaning of the data after transferring it to the client, also in case the Cloud Service Provider (CSP) closes its operations or whenever the user so desires.
3. Data security can be further enhanced by implementing firewall to isolate confidential information.
4. The mechanism for lodging complaints regarding security breach with the Cloud service provider by the user and the subsequent remedial

and corrective measures taken thereupon shall be provided. All such complaints shall be logged and stored for a specified period of time for external audit.

5. CSP should conform to mandated regulatory, legal, and general industry requirements (such as PCIDSS, HIPAA, SOX, etc.).
6. CSPs must inform the customers about any planned or unplanned changes in the cloud environment, and it has to be governed by change management processes.

End user:

1. End user should maintain the direct control to decide how and where the data and software is deployed, used, and destroyed in multitenant environment.
2. User credentials to be maintained in secured manner.

Q14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

1. The data security requirement for cloud service providers must be in line with the current data security/privacy requirements (IT Act 2008) or proposed privacy act.
2. Cloud Service Providers must indemnity to the clients against any breach of privacy for the end customers. The Client organizations are supposedly the data controllers for their end customers' data and are liable to protect customer confidentiality as per current IT Act.
3. Since the customer accounting information for most of the industries cannot be moved across the boundary of the country, it is imperative that the cloud service providers must set up their data center within the country.
4. In case of interoperability of cloud services, the service providers must declare to the clients which part of the data is shared by the third party, if any.
5. The copyright related issues on the material uploaded on cloud must be clearly mentioned in the contract with the clients along with the liability, if any.

6. In case the cloud service provider infringes the copyright, there should be provision to black list such CSPs from operating in India.
7. Similarly, if the client regularly uploads and downloads copyright material on cloud, then the CSP should restrict the service to the cloud client.

Q15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

1. Cloud service providers should be encouraged to have their data centers in India to protect the sensitive information moving outside the country.
2. From lawful interception point of view, only the communication services on cloud (e.g VoIP, unified communication etc.) should be included for services. Other cloud services, such as computing resources, storage, application etc. should be kept outside the purview of the LI as the corporates using these services would demand privacy and confidentiality to maintain their competitive edge.
3. To promote the use of Cloud services, the government must come out with an elaborate Privacy policy that includes the responsibility of both the Cloud providers and clients in protecting the sensitive information.
4. The regulatory body proposed to govern the operations of CSPs in India must specify the standard contractual clauses containing areas such as Data protection responsibilities- declaration by CSPs that under no circumstance, the data will move out of the local cloud (domestic cloud).

Q16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud service providers so as to subject them to the obligations thereunder? Please comment with justification.

1. A regulatory body (similar to TRAI or Real Estate Regulatory Authority) must be set up to govern the activities of Cloud Service Providers in India.
2. All CSPs must be registered with such regulatory body before commencing services.

3. CSPs must be governed by the data privacy acts of the country and provisions should be in place to delist CSPs in the event of any breach of privacy norms.
4. CSPs must declare the Security measures, including the tools that they deploy to protect the information on cloud as this will give added assurance to the clients for moving on cloud.

Q17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

1. CSP's platform should be integrated with respective law enforcement authority's platform.
2. The CSPs must submit periodic declaration with the authority (may be under the Ministry of Home Affairs) that none of the citizen centric information is moving out of country.
3. The regulatory authority can retain the right to audit the data handling process of the CSPs.
4. The authority should have the powers to delist the erring CSPs in case of breach of National Security of India besides imposing stringent penalty.

Q18. What are the steps that can be taken by the government for:
(a) promoting cloud computing in e-governance projects.
(b) promoting establishment of data centres in India.
(c) encouraging business and private organizations utilize cloud services
(d) to boost Digital India and Smart Cities incentive using cloud.

1. Clearly define regulatory framework around data privacy.
2. Encourage Cloud service providers to set up data centres in India by offering incentives such as cheaper land and power.
3. Develop skills around cloud services by promoting partnership between technical institutions and CSPs such that the CSPs are encouraged to build scale.
4. Interoperability would be the key in ensuring the success of mega projects like Smart city and Digital India, where, multiple technology service providers need to operate in an integrated fashion.
5. On Infrastructure front, the availability of high speed broad band is the major enabler for the cloud services and hence the government must

promote faster roll out of data services especially through the National Optic Fiber Network project.

6. Encryption policy would serve as another enabler for the faster adoption of Cloud services in India.

Q19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

1. Yes, there should be a dedicated cloud for government applications since there is immense opportunity for the government to monetize this data by offering the preferred services using various analytical tools. Moreover, the government or government monitored agencies will be in better position to effectively utilize this data without compromising the privacy.
2. The applications hosted for government officials or departments must reside in a separate container as these pertain to national security.
3. For e-government projects, multi-tenant environment can be used to accommodate various central and state government projects.
4. In these sensitive matters, the government should follow single CSP model to ensure ease of monitoring.

Q20. What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?

1. Availability of cheap and reliable power.
2. Availability of land at an affordable price.
3. Availability of technical skills to operate cloud data centres.
4. High speed connectivity.
5. Existing model of TERM cell (telecom) can be used for information sharing across states.

Q21. What tax subsidies should be proposed to incentivize the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centers and cloud services platforms in India?

1. Cloud services should be put under infrastructure sector to allow the tax benefits that are applicable to this sector.
2. Since Cloud is going to be a potent platform to enable many small and large businesses that will contribute significantly to Indian economy, it is important that suitable tax incentives must be offered to this sector.
   Since this is a capital intensive technology platform, the global experience indicates long gestation period for Cloud service investment. One of the ways to incentivize the CSPs for setting up datacenters is to offer subsidies in input material such as power.