Response to
TRAI Consultation paper
On
Cloud

INTEL TECHNOLOGIES INDIA PVT LTD New Delhi

Anantha.s@intel.com

Q2

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

A typical cloud service provider invests tremendous amount of money in cloud infrastructure –including building space, power, back up facilities, security setup etc. These costs are amortized or spread over thousands/millions of customers. Because of this shared usage of common infrastructure, the cost for individual customer comes down

Q3

Enterprises consider various factors before deciding which type of cloud (private or public) to select. Below is a summary of such factors

No	Feature	Public	Private
1	Agility	Yes	Partial
2	Infinite Scalability	Yes	No (Limited)
3	Base Load	Not Economical	Economical
4	Core business critical Applications (Core Banking/Telecom Billing)	Not suited	Yes
5	Temporary Load (Dev, QA for few months)	Yes	Not suited
6	Seasonal Load (Marketing campaign, Tickets for rock concert)	Yes	Not suited
7	Flexibility in design, architecture, selection of particular HW, OS	No	Yes
8	Flexibility in contacting -SLA, SOW and Penalties	No	Yes
9	Data Sovereignty	Partial (issue in some cases)	Yes
10	Security	Yes	Yes

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?

Secure Migration can be accomplished by multiple technical approaches.

A more common approach is to have the ability to define "Secure Zones" extending across the clouds by leveraging Security technologies available at the server platform level. Also Security appliances adhering to industry standards can provide end to end encryption ensuring a secure migration of the workloads.

Another key aspect to note is that when workloads are moved across clouds, it needs to be ensured that the Layer4 – Layer 7 policies applicable for the workload are maintained consistently post migration as well to ensure smooth continuity of service post migration as well.

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?

Intel supports the unencumbered growth of cloud computing. At the same time, we recognize the importance of ensuring that appropriate privacy and security measures are in place.

1. The global nature of the cloud means that policies must address international dynamics and not create preferences for companies, products, or jurisdictions.
2. We support a standard-setting process that is global, consensus based, transparent, and industry-led.
3. We support strong global privacy standards because it is critical that consumers trust their devices and how their personal information is handled.
4. Globally, the best way to improve cybersecurity is to leverage industry initiatives and public-private partnerships and focus on the bad actors and their threats.

5. We support free trade agreements (FTAs) that require the free flow of data across borders and prohibit local server requirements in order for such information to move among countries.
6. High-speed broadband networks are critical for expanding and connecting to the cloud.

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?

We recommend open, industry based standards for interoperability rather than regulatory framework to enforce such interoperability. “Open Data Center Alliance” is one such organization promoting and shaping adoption of cloud computing. Open Data Center alliance advocates standards for “Work Load Mobility” , “VM Interoperability” etc. across multiple Cloud Service providers to ensure interoperability of cloud services at various levels of implementation and the large enterprise customers who have been part of the ODCA alliance have done PoCs, workshops on these topics and share the same with other customers in the alliance and also publish industry white papers for even broader adoption.

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.

Cloud Service providers usually share the QoS parameters of their services to the customer by publishing it as part of their catalogue or as part of the contract signed by them with the enterprise customer. These QoS parameters are more often reflective of their focus for specific types of customers as part of their business strategy. It’s not a usually a comparable parameter across diverse cloud providers.

However it helps to provide the criteria for the QoS parameters which the customer can utilize to categorize their business needs to evolve specific

metrics and then use the same to compare different Service providers from whom they are evaluating to buy the cloud service.

Typical criteria would include SLA on Availability, Service creation time, Latency, Security tools, policy and process, Auditable trail available for compliance requirement made available for the customer etc. Additionally criteria for how the Service provider is addressing compliance requirements like Data Sovereignty etc. should also be considered.

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?

As a standard most cloud service providers provide the billing charge back summary of the customer on the main portal page exposed to the customer while logging in. This would give information in terms of resource allocated, consumed, available etc and also associated summary of costs incurred by the customer.

In addition the service providers should be encouraged to provide detailed billing details in scenarios when any dispute arises.

A comprehensive monitoring, metering and reporting solution is more often deployed by the cloud service provider to provide these information.

Q9.

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

The end customers, be it individuals or enterprises need to have a mechanism to reach out to the cloud service provider either by email, phone or chat. The cloud provider needs to specify a timeframe for response and a timeframe for resolution of issues.

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 computing involves much more than just technology. ISO 27001 specifically looks at the holistic service organization that provides the cloud service to customers

We have following suggestions to achieve effective security & policy management in cloud computing deployments:

1. **Web Application Risk**

    - Assessment: Before or while consuming web applications, assessment of risk associated with Web application is required. We can standardize parameters to assess the risk associated with the web application and utilize these parameters to calculate Web Application Risk.
    - Examples:
        - Ratings of specific Web Application development team or organization
        - Security standards followed by Web Application E.g.: is it utilizing https or http etc.
    - This will help in following:
        - Will increase security and data protection of customer data
        - Highly secure web applications reduce the maintenance costs

2. **Data Residence within Geographies of Data Centers:**

    - Another security concerns of enterprises is the physical location of the data especially if they are located in another country because the laws of the host country apply to the machine and data residing on it. That becomes an issue if the host country does not have adequate laws to protect sensitive data or if the host nation becomes hostile and depends largely on the government concerned. The primary location of the data and any backup locations must be known to ensure these laws and regulations are followed.
    - Solutions offered by various vendors such as “Global Intelligence Routing” will help cloud computing adapting companies to better manage their data to stay within the permissible geolocation and they by meet the compliance requirements.

3. **Visibility & Control of Web Applications:**

- As organizations start utilizing Web Applications deployed in Cloud, it's highly important to understand (from both visibility & control point of view) various applications utilized by the organization. Cloud Access Security Broker (CASB) offer advanced and scalable cloud security services as well as meeting or exceeding compliance requirements.
- Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.

4. Visibility & Control of Virtualized Assets:

- As organizations start utilizing IaaS & PaaS services, it's important get visibility & control of virtualized assets.
- Public cloud providers such as AWS/Azure provide various connectors to help organizations to get this visibility & control.

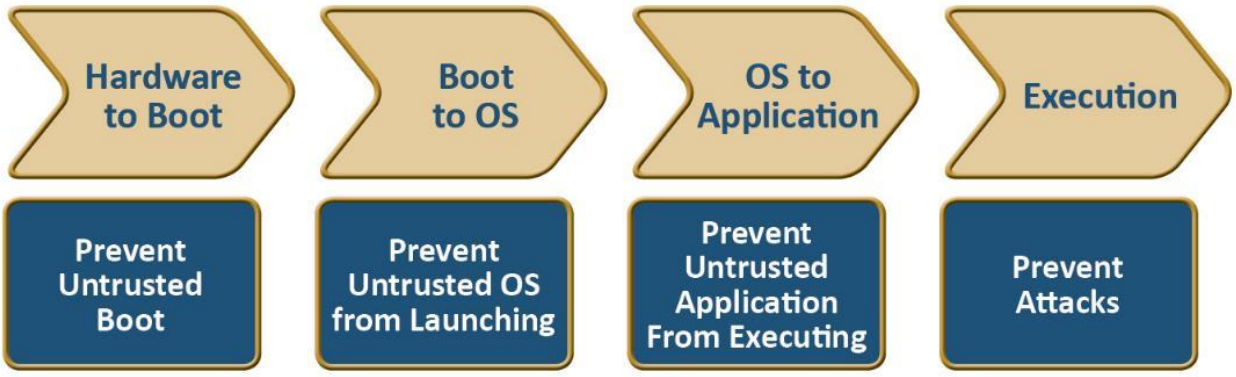
5. User & Entity Behavior Analytics:

- With the growing massive amounts of data, it's important for organizations to adapt Analytics to understand the specific users within the organization and virtualized assets deployed in the cloud are behaving w.r.to Risk. This is now easier to achieve with the cloud computing.
- UEBA helps enterprises address the key domains spanning insider threats, security management, data exfiltration, and identity and access management.

6. Trusted / Platform Boot Integrity

- It's highly recommended to utilize "Trusted/Platform Boot Integrity" by Cloud computing providers. This security mechanism when it's activated, the system on which web application is deployed, checks for each piece of software, operating system against databases of known good signatures that are maintained in the firmware and the firmware runs the software and the operating system. These type of security system are necessary for BIOS based attacks like:

- Protects hardware (Physical and Virtual Machines) and associated software
- Protects user and Machine from Malware, rootkit etc attacks



7. Automation of Policy Orchestration

- Orchestration products specially for Cloud Computing can simplify the inter component communication and connections to other apps and users and ensure that links are correctly configured and maintained.
- **Examples:**
  - Puppet, Spacewalk, ANSIBLE (Tower, Playbooks), Chef are various freeware tools available to achieve better policy orchestration in addition to various advanced solutions offered by vendors (for IaaS & PaaS)
  - ePO would be best fit here for McAfee specific SaaS solutions

8. Data Protection & Other Solutions

- **DLP (Data Leakage Prevention) / e-Discovery Solution** – Cloud service providers should have a e-Discovery solution and DLP solutions. If not customers should invest in these technologies to safeguard their assets in the cloud and stay in line with compliance requirements
- **Tenant Isolation** – Cloud uses shared resources (computing, memory, storage, network etc). Compromise of one tenant, should not affect others. CSPs should have an established policy and tools to manage and demonstrate this. CSP policy around co-location of

tenants should be reviewed and negotiated. Sometimes a casual tenant may leave their cloud resources vulnerable, exposing the risk to other serious tenants co-located physically

9. Security for Termination & Exit provisions

- **Staging/Testing/Production environments :** It's highly recommended to choose cloud service providers who have some facilities (and policies) for providing an isolated staging area were applications and services can be tested by customers before going live
- **Datacenter security** – physical security and location of the cloud hosting data center is important. Is it prone to natural threats like (Earthquakes, cyclonic storms etc.) or Political/ Terrorisms threats
- **Incident Monitoring, Reporting and Remediation:** Incident detection and reporting facility should be available and customer should have visibility into network/access logs. Cloud customer should get notified in timely manner if any machines are compromised. They should also have historical data available on the number of attacks detected and blocked. These help to understand how effective remediation policies of cloud service providers are.

Best practices for Cloud emerging recently

a) ENISA Procure Secure program started in 2012 and including a number of specific recommendations, e.g., government Cloud (https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
b) TCG (Trusted Computing Group) Multi-Tenant Trusted Architecture (http://www.trustedcomputinggroup.org/trusted-multi-tenant-infrastructure-faqs/)

General international standards including:

a) ISO/IEC 27034 on application security controls https://www.owasp.org/index.php/OWASP_ISO_IEC_27034_Application_Security_Controls_Project
b) ISO/IEC 15288 on systems engineering (http://www.iso.org/iso/catalogue_detail?csnumber=63711)

Self-certification frameworks

a) E.g., NIST Cyber Security Framework (CSF)

Q11.

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

- **Protection from Vulnerabilities & DDoS attacks:** Organizations are recommended to choose cloud computing providers that are not vulnerable to various attacks such as DDoS. Virtualized Intrusion Prevention Systems will be of great help and few vendors offer "Protection from DDoS as service"
- **Secure communications between Organizations & Cloud security Providers:** Organizations adapting to cloud computing require to ensure secure communication between the organization & cloud computing provider. IPSec tunneling is one proven technology in order to achieve the same. Use latest cyphers and strong keys to connect with Cloud Services.
- **Key and Encryption management**: Organizations adapting to cloud computing require to ensure that "Data at rest" is encrypted. Use latest cyphers and strong keys for secure access and storage of keys. Preferably store them off-cloud and make it available on "need-to-access" basis only

Q12.

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

Adaption of Containerization

- Major advantage of adaption to Cloud computing is if particular vendor's cloud computing service is unsatisfactory, the organizations have opportunity to migrate to other cloud computing provider. However, in order to achieve the same, organizations have very good migration strategy.
- Containerization will be of major help in order to accomplish this strategy. Containerization is a lightweight alternative to full machine

virtualization that involves encapsulating an application in a container with its own operating environment. This provides many of the benefits of loading an application onto a virtual machine, as the application can be run on any suitable physical machine without any worries about dependencies.

Q13.

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

CSP

Should clearly specify the following:-

1. Policies with respect the privacy of the individual data.

2. Terms of agreement (End user and for enterprises)

3. What is being offered with a reasonably detailed architecture– (technical details of computer, storage and NW throughput)

4. Service Level agreements (On availability, issue response, issue resolution)

5. Security Policy – what is being provided by default and what additional measures a customer should take.

End User:-

1. Read and understand how personal information is protected.

2. Provide consent to the terms.

3. Configure the security policies and setup as per individual /enterprise needs.

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?

Cloud security and privacy is linked to the emerging context of data interoperability, a standard way to permit privacy-preserving and secure functionality that requires multiple datasets in the Cloud. This work is typically linked to Cloud support for IoT because this aspect is the most important in this area. This approach has been described in several standardization and pre-standardization efforts, including:

a) NIST-convened international effort (public working group) on cyber-physical systems (deliverable for 1.0 framework at https://pages.nist.gov/cpspwg/)

b) IETF effort on semantic data interoperability at https://tools.ietf.org/html/draft-strassner-t2trg-semantics-and-iot-00

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?

We do not recommend separate law/regulation for the scope of cloud computing services. Our suggestion is Govt. should act like facilitator and enable the industry to grow through open standards and commitment to individual privacy.

We believe that current legislations governing IT services/IT infrastructure is sufficient to cover the cloud services. As the history of Indian IT services suggest proactive facilitation from the Govt. rather than the license based approach will enable growth.

Q18.

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

- ***Promoting cloud computing in e-governance projects.***
- ***Promoting establishment of data centres in India.***
- ***Encouraging business and private organizations utilize cloud services***
- ***To boost Digital India and Smart Cities incentive using cloud.***

We believe that the Govt. of India can take following initiatives on supply and demand side to promote cloud services:-

Supply Side

1. India shall endeavor to become the Data center destination for large MNCs, global, and Indian cloud service providers, for exporting cloud services globally from India. This will be challenging, as India doesn't have favorable climatic conditions w.r.t. countries north of tropic of cancer.

2. Indian government shall develop few Cloud Computing Parks for setting up large scale Tier 4 DC on the lines of software technology parks. Government shall consider offering incentives to companies with Data Centers in these parks, as offered to various export oriented industries. The incentives could be tax incentives, lower custom duties for equipment, electricity at attractive rates. These parks could be built in favorable climate zones, which are pollution free and have lower temperature, to keep low cooling costs and achieving low PUEs. These parks shall be connected through NoFN network and shall have reliable network connectivity from all leading Indian telecom service providers. Additionally it shall have reliable electricity supply from multiple grids.

Demand Side

1. Availability and access to a stable and high speed broadband connection will help cloud services to grow exponentially. In this regard the Govt. needs to expedite the investments in broadband connectivity through programs like National Optical Fiber Network (NOFN) etc. This will help citizens at the

remotest corners of the country to make effective use of eGovernance initiatives and also other cloud services

2. Govt. can mandate all are part of Govt. IT projects to be executed through cloud. This will help Govt. reduce immediate capex and convert some of the Capex into Opex

3. Pooling of IT requirements for Smart Cities and other similar projects will enable the Govt. to make better use of cloud services and get volume discounts in some cases.

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?

We believe that Govt. should make use of exiting cloud setups rather than going for a separate dedicated cloud. Setting up a separate cloud would involve capital expenditure from the Govt. and would defeat the purpose of going for cloud in the first place. Moreover, the Govt. would not be in a position to realize the economies of scale offered by the current cloud service providers.

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?

Availability and access to a stable and high speed broadband connection will help cloud services to grow exponentially. In this regard the Govt. needs to expedite the investments in broadband connectivity through programs like National Optical Fiber Network (NOFN) etc. This will help citizens at the remotest corners of the country to make effective use of eGovernance initiatives from state data centers

The best practice for information sharing is through web services (API calls). The state data centers can expose certain data (pre-agreed with the central

Govt. and other State Govt.) via web service. Any program can call such API and fetch the data.

Q21.

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

The Govt. should don the role of the facilitator rather than regulator for the promotion of the cloud services. It should encourage strong industry wide open standards for privacy, security and inter-operability.

For the creation of local data centers, apart from the above open standard, Govt. can think of considering large cloud data centers of certain size as Special Economic Zones with the associated tax benefits. This would incentivize the global players to setup large regional data centers to India.