SFLC.in
K-9 Second Floor, Birbal Road,
Jangpura Extension,
New Delhi-110014
Phone : +91-11-43587126
Email : mail@sflc.in

To

July 25, 2016

Shri A Robert J Ravi, Advisor (QoS)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
J L Nehru Marg, Old Minto Road
New Delhi – 110012
Email: advqos@trai.gov.in

[*Via electronic distribution*]

Re: Comments on the Consultation Paper on Cloud Computing

Sir,

SFLC.in is a New Delhi based not-for-profit organization that brings together lawyers, policy analysts, technologists, and students to protect freedom in the digital world. We promote innovation and open access to knowledge by helping developers make great Free and Open Source Software (FOSS), protect digital civil liberties by providing pro-bono legal advice, and help policy makers make informed and just decisions with the use and adoption of technology.

We thank TRAI at this juncture for initiating this important public discourse, especially considering the significance of Information and Communication Technologies with regard to state initiatives such as Digital India. Attached with this mail are our comments on the Consultation Paper, and we look forward to a fruitful discourse.

Yours sincerely,
Mishi Choudhary
Executive Director

sflc.in

Responses to the Consultation Paper on Cloud Computing

Introduction

TRAI's consultation paper on Cloud Computing presents valuable information gleaned from industry analysis and observation of other government policy documents. It raises important issues---about security, privacy and competition policy---that other government policy-makers around the world are facing. We look forward to working with TRAI and other GoI policy-makers on these indeed serious questions.

But the consultation paper does not take account of the most important issues for policy-makers about the Cloud, because they are not well-captured by the industry analyses on which their framing of the questions is built.

The purpose of the software techniques---virtualization and storage pooling---we call "the cloud" is to making computing capacity fluid and place-independent. In a "cloud" network, data and computer programs migrate around the net, so our data processing can occur on any hardware, and be stored anywhere in immense pools of storage that are efficient and cost-effective to use. For large businesses and governments, this means using computing resources frugally. In a world without virtualization and storage pooling, computers are always partially idle because programs that could use their power aren't running there, and data is inefficiently stored because everyone buys a silo for his barn, but doesn't need all the space.

This flexibility doesn't only mean that inequalities between computing resources and requirements can be smoothed out inside large enterprises. It also means that computing resources can be a public utility, so that access to computing resources isn't determined entirely by the ability to pay.

Many young educated Indians could run useful services and provide useful businesses for themselves and employment to others if they could place a server on the public Internet. But reliable electricity is not available around them, connectivity is expensive, and they cannot afford the infrastructure hardware, like routers. But a truly public cloud, citizen computing, can give them for Rs100/month a *virtual server* that would enable them to be full citizens of the Web, engaged in e-commerce, financial technology, the 21st-century world.

Cloud APIs are the roadways of the 21st century. They set the rules by which data and computing resources move to where they can work most efficiently, reducing cost and complexity, not just---as the consultation paper always sees the world---for platform companies and their users, but for the producing young citizens of the digital society, who make the startups, provide the education, push forward the national mind. (The consultation memo is fortunately too pessimistic on the path of convergence on free and open APIs. The call for "standardization" is largely an industry tactic by proprietary cloud API owners such as VMWare and Amazon Web Services, to give them a "standard" defense against the free and open APIs implemented by FOSS products from OpenStack to ganeti and libvirt, which are taking over, providing interoperability and threatening their market incumbency.)

So the role of cloud computing in national development is not limited to IaaS installations providing utility computing to individual users who will now have an inexpensive server as well as a smartphone. Very cheap hardware, such as Rs.2500 Raspberry Pi computers in schools, can using these Cloud APIs server as gateways to sophisticated computing resources in every village. Instead of just learning to use Facebook on a phone, and calling that "technological literacy," a cloud of inexpensive devices acting as part of a "national cloud" provides educational and business opportunities to whole population that can only accrue to businesses and wealthy individuals in a world where I have to buy the computers I compute with.

So the consultation should expand to include questions such as:

- How can cloud computing bring enhanced access to technical resources for learning and "citizen computing" to all of our people, regardless of ability to pay?
- How can cloud infrastructure leap out of the data center into the cheapest and most accessible hardware to which citizens have access, so that everyone can join "the Cloud" as they can attach their phones to the Net?
- How can free software in the cloud enable young people to be more than users of platforms, and become instead skilled builders, using the resources commonly available in the cloud to make their livings improving the lives of people and businesses around them?

It is perfectly right for TRAI to consider, as this paper does, the role of government in purchasing software and regulating market participants offering digital services. But something even more important will be lost if TRAI does not also consider these technological disruptions from the vantage of the social architect, understanding how these new technical materials can be used to improve the lives of ordinary people, and the intellectual development of Indian society.

Specific responses

Question 14: 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 to moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

The use of cloud services involves certain legal issues with respect to cross border transfer of data due to the multiple jurisdictions the services function in. The use of these services need to address issues of privacy and security of user data when it is transferred from one jurisdiction to another by the Cloud Service Provider (CSP). The diversity of legal mechanisms, their application, or the lack thereof in many countries have raised issues about the effective transmission and storage of data in cloud services. While encouraging the use of cloud services in the country, it is important to ensure that there are regulations in place that clarify the principles that should be followed by CSPs while shifting the data of their users from one jurisdiction to another.

Around the globe, there are existing frameworks being followed by different countries to regulate such cross border transfer of data. The 1995 Data Protection Directive of the European Union entails under Article 25 that cross border transfer of personal data of users in its territory only be permitted to regions or States that have adequate privacy and data protection laws as per the EU standards.[1] The businesses and other entities in States that receive an adequacy status from the EU, are therefore eligible to indulge in cross border transfer of personal data of users in the EU. Recently, the EU & US revised their earlier Safe Harbor agreement for such transfer of data as per the European Court of Justice order that recorded that practices of bulk surveillance by the intelligence agencies in the United States were not in compliance with the data protection laws in the US. The renewed version of this agreement, known as the Privacy Shield has been criticized for not fully eliminating the concerns of bulk surveillance practices in the United States and permitting it in six expressive categories of- measures to detect and counter threats stemming from espionage, terrorism, weapons of mass destruction, to the Armed Forces or military personnel, as well as transnational criminal threats related to the other five purposes, and will be reviewed at least on an annual basis.[2] However, it has laid down seven privacy principles that are worth mentioning and

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; last accessed on 25th July, 2016

[2] Recital 74, Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protetion provided by the EU-US Privacy Shield; available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf; last accessed on 25th July, 2016

should be followed to enable any system of cross border transfer of data among various jurisdictions. These principles are[3]:

1. Notice: Individuals must be informed that their data is being collected and how it will be used. The organization must provide information about how individuals can contact the organization with any inquiries or complaints.
2. Choice: Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.
3. Accountability for Onward Transfer: Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
4. Security: Reasonable efforts must be made to prevent loss of collected information.
5. Data Integrity & Purpose Limitation: Data must be relevant and reliable for the purpose it was collected.
6. Access: Individuals must be able to access information held about them, and correct or delete it, if it is inaccurate.
7. Recourse, Enforcement & Liability: There must be effective means of enforcing these rules.

The Internet in general transcends boundaries and jurisdictions, thereby making it difficult to apply traditional laws of territorial jurisdictions to its multifarious dimensions. This was further evidenced by a judgment issued by the Second Circuit Court of Appeals in New York in the matter of Microsoft Corporation v. United States of America, where it was said the Government did not have the authority to compel Microsoft to produce the contents of a customer's email account stored exclusively in Ireland.[4] Self regulatory mechanisms in the hands of intermediaries and industry standards that have been applied in absence of any substantial uniform regulation have failed to prove effective. The revelations made by the Snowden leaks in 2012 are a brazen illustration of this; wherein services registered in the United States were providing personal data of foreign nationals held by them to the US intelligence agencies when demanded.[5] Therefore, self regulatory practices employed by individual intermediaries & services should function under the overarching and

[3] Annex II, EU-US Privacy Shield Framework Principles issued by the U.S. Department of Commerce, Page 4 to 7; available at: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf; last accessed on 25th July, 2016

[4] Zack Whittaker, In privacy victory, Microsoft wins appeal over foreign data warrant, available at: http://www.zdnet.com/article/microsoft-wins-appeal-over-warrant-for-overseas-emails/

[5] NSA's Prism surveillance program: how it works and what it can do, James Ball, 8th June, 2013, The Guardian; available on: https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google; last accessed on 25th July, 2016

comprehensive scheme of a data protection law, with enumerated provisions on cross border transfer to ensure the protection of privacy of the users & security of the data.

In India, the lack of an overarching and comprehensive privacy and data protection law makes it difficult to evaluate adequacy of other countries wherein the data of Indian citizens would be transferred through these CSPs. The efforts for finalizing a law on these lines are underway, and we hope that it includes a provision for efficient & secure cross border transfer of data among other things. As per the limited scope of this paper, the cross border transfer of data in terms of cloud services, the disclosure guidelines for various CSPs should broadly follow from the Privacy Shield principles enumerated above. In addition to these, a regulation for such transfer of data between jurisdictions should include the following three principles as well:

- Consumer protection & grievance redressal: An appropriate methodology for the user to lodge a complaint in their home country in their data is misused across borders in the foreign jurisdiction.
- Obligation to protect citizens' data from access by foreign intelligence services: There should be an explicit clause that excludes the transferred data from the purview of access by foreign intelligence agencies, or provisions such as bulk collection or processing by these agencies.

These principles formulate a comprehensive framework to evaluate a complete and secure system of transmission of data from one jurisdiction to another, while balancing the privacy & choice of the user.

Question 15: What policies, 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?

From a lawful interception perspective, the Information Technology Act, 2000 (IT Act) already authorizes Central and State Law Enforcement Agencies (LEAs) to intercept, monitor and decrypt data and meta-data travelling over domestic Internet networks. The operative provisions in this regard are Sections 69 and 69B of the IT Act read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, and the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

Even a perfunctory examination of Sections 69 and 69B of the IT Act will tell us that the lawful interception provisioned under these Sections extends to “any information stored on a computer resource”, regardless of the characteristic attributes of said computer resource. All cloud computing data that traverses Indian Internet networks is therefore subject to lawful interception as per the provisions of the IT Act and Rules mentioned above. Further, the Sections require any person/intermediary in charge of the computer resource to extend all surveillance-related assistance to LEAs when called upon to do so, and failures in this regard are punishable with imprisonment for up to seven years and fines. By virtue of the IT Act's broad definition of the term “computer”, any data that is generated, stored or transmitted over any hardware (including servers, PCs, laptops, phones and tablets) or even software is capable of being surveilled by LEAs, and the obligation to assist LEAs in this regard accrues to all persons/intermediaries in charge of said hardware/software.

As regards ensuring compliance with lawful interception requests by overseas cloud service providers, certain practical difficulties do emerge owing to the absence of binding obligations on overseas providers to submit to Indian jurisdiction, but this is hardly endemic to India or its regulatory setup. The Internet by design operates without regard to national and regional boundaries, with content and services terminating in one jurisdiction often originating from one or more external jurisdictions. Since lawful interception obligations are determined largely by national jurisdiction and geography, LEAs will be unable to make interception requests directly to cloud service providers without an "in country" presence.

Some countries have sought to exert greater control over citizens' data through strict data localization laws i.e. through legal provisions mandating the retention of citizens' data within national boundaries. Russia’s new data localization law, Federal Law No. 242-FZ for instance, was adopted as a set of amendments to Russia’s On Personal Data Law in July 2014 and came into force on September 1, 2015.[6] The law requires “operators” to collect, store, and process Russian citizens’ personal data using databases located within Russia.[7] Additionally, operators also must inform Russia’s Roskomnadzor, the state body that oversees telecommunications, information technology, and mass communication, of the location of the servers where Russians’ personal data is stored. Internet addresses that are found to be out of compliance with the law may be blocked.[8] While strict data localization laws such as these may appear to be potential workarounds that allow greater

[6] *Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions)*, available at: https://pd.rkn.gov.ru/authority/p146/p191/, last accessed on July 25, 2016

[7] Courtney M Bowman, *A Primer on Russia's New Data Localization Laws*, August 27, 2015, available at: http://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/, last accessed on July 25, 2016

[8] Ibid.

control over citizens' data and by extension, easier conduct of lawful interception by LEAs, this is far from true. In fact, the practical difficulties – both technical and financial – involved in restricting online activities to particular geographic boundaries may prove crippling for smaller Internet-based entities without vast resources at their disposal. The ability to distribute on-line service infrastructures across the world are crucial for a number of reasons including significant cost reductions, and the increase in complexity and costs that would inevitably come with data localization mandates may motivate Internet-based entities to leave the market entirely.

The above factors considered, Mutual Legal Assistance Treaties (MLATs) with specific provisions on the procurement of lawfully intercepted data from overseas cloud service providers could be a more sustainable solution. MLATs have long played important roles in cross-border cooperation in criminal investigation. In general, such treaties seek to expedite and assist cross-border cooperation in criminal investigations. Usually each country will designate an authority for direct communication between the countries or jurisdictions in such instances where cross-border assistance may be required.[9] However, no MLAT gives open permission for cross-border surveillance to occur; they merely operate, in the most part, to create open lines of communication.[10] Dedicated MLATs would nevertheless serve to ease much of the difficulties involved in securing lawfully intercepted information from overseas content and service providers including, but not limited to cloud service providers.

Question 16: 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.

Companies offering cloud computing services should not be mandated to obtain separate licenses for providing their services to users. This is because they use pathways that are owned by telecommunication operators who already license the spectrum that is used for transmitting the content. Once, the pathway has been licensed, all content should be allowed to freely pass over this pathway with no application-specific discrimination. Technically there is no difference between data packets whether they carry voice or a web page. Hence, there is no reason to treat them differently. Operationally, a license regime for Internet Services will be problematic as if each country starts adopting such a stance an Internet Service will have to obtain license from each and every country.

[9] United Nations Office on Drugs and Crime, *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime*, ISBN 978-92-1-148246-1, 2009, p. 10, available at: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf, last accessed on July 25, 2016

[10] Ibid.

A telecommunications company operating in one country can interconnect with providers in other countries because of the standards and inter-connect arrangements managed by International Telecommunications Union (ITU). This is not the case in the case of Internet Services.

Governments across the world while negotiating the International Telecommunication Regulations (ITRs) at the World Conference on International Telecommunications 2012 chose to keep Information Services from the ambit of the Regulations and restricted it to only the traditional telephony. Even Indian Telecommunications Operators (represented by the Cellular Operators Association of India at the conference) were against inclusion of Information Services under the ITRs. The proposal to regulate cloud service providers is against the stance adopted by India and the telecommunication companies at an International forum.

Refrainment from overly burdensome regulations as applicable to Internet-based services is also reflected in the National Telecom Policy 2012 (NTP), which was notified with a view to formulate a clear policy regime for making available affordable and effective communication systems for citizens, and “enabling seamless delivery of converged services [of voice, data, video, internet telephony (VoIP), value added services and broadcasting services] in a technology and service neutral environment.” (Para 3.1 NTP). The preamble of the NTP states: “Telecommunications is no longer limited to voice. The evolution from analog to digital technology has facilitated the conversion of voice, data and video to the digital form. Increasingly, these are now being rendered through single networks bringing about a convergence in networks, services and also devices. Hence, it is now imperative to move towards convergence between telecom, broadcast and IT services, networks, platforms, technologies and overcome the existing segregation of licensing, registration and regulatory mechanisms in these areas to enhance affordability, increase access, delivery of multiple services and reduce cost. It will be a key enabler of equitable and inclusive growth. The policy aims to address and enable the coordinated action to respond to the dynamic needs resulting from confluence of telecom, broadcasting and IT sectors.”

Furthermore, on October 2011, India made its stance on Internet regulation clear at the 66th session of the UN General assembly. India recognized that the Internet was an “unprecedented global medium” that should be “inclusive, democratic, participatory, multilateral and transparent in nature”. India pointed out that the Internet had grown in size and scope, and the task of Internet governance required “quick footed and timely global solutions and policies, not divergent and fragmented national policies.”

Moreover, cloud service providers are already regulated by a number of general and specific legislations that prescribe numerous general, technical, financial, and security related conditions that they must necessarily comply with. Some of the existing legislations that apply to cloud providers are:

- Information Technology Act, 2000
- Consumer Protection Act, 1986
- Payment and Settlement Systems Act, 2007
- Indian Copyright Act, 1957
- Income Tax Act, 1961
- Customs Act, 1962
- Central Excise Act, 1944
- Foreign Exchange Management Act, 1999
- Prevention of Money Laundering Act, 2002

As cloud service providers are already regulated under the above legislations, we submit that additional regulatory frameworks would be excessive and would hinder the growth of cloud computing in India. We feel the purpose of ensuring comprehensive regulation of cloud computing would be better served by a review of how the existing regulations apply to cloud service providers and making necessary amendments based on the findings, rather than establishing a dedicated regulatory framework from scratch. Regulations and laws prevailing over telecommunication services such as entry fees, spectrum allocation and charges, tariff regulations etc. cannot be imposed on cloud services for the reason that regulation of websites and apps provided on the Internet would have a direct impact on start-up companies and new entrants who will be forced to comply with regulatory costs notwithstanding the cost of setting up the website in the first place which is very low or even negligible. The Internet provides an opportunity to everyone, be it college students who are constantly coming up with great, innovative business ideas (social networking website Facebook was set up by Mark Zuckerberg in his hostel dorm room) and even people in rural areas who are able to sell their products on the internet. Over-regulation would mean a loss of all such opportunities and a sudden hindrance to innovation.

Question 17. 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?

As noted by the Consultation Paper itself, the IT Act has broad territorial jurisdiction that extends to computer networks outside the country as well. Under Section 75 of the Act, this jurisdiction can apply to an offence or contravention (say that of sensitive data protection rules) as long as it involves a computer, computer system or computer network located in India. However, as discussed in our response to question 15, certain practical difficulties do exist in ensuring compliance with domestic laws by overseas cloud service providers owing to the absence of binding obligations to submit to Indian jurisdiction, but this is hardly endemic to India or its regulatory setup. The Internet by design operates without regard to national and regional boundaries, with content and services terminating in one jurisdiction often originating from one or more external jurisdictions. Since lawful interception obligations are determined largely by national jurisdiction and geography, LEAs will be unable to make interception requests directly to cloud service providers without an "in country" presence. Under the circumstances, we recommend Mutual Legal Assistance Treaties (MLATs) with specific provisions on the procurement of lawfully intercepted data from overseas cloud service providers as a potential solution to the jurisdictional challenges involved therein.

Question 18. 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.**

Cloud computing technology promises to provide almost unlimited computational power, with high accessibility to information anytime, besides the ability to meet the peak load cheaply and rapidly to anticipate a sudden increase in demands. Moreover, this technology provides an opportunity for developers to develop their own applications and even platforms depending on their IT capabilities.[11]

The Government of India needs to boost Digital India initiative and in light of that needs to take steps for promoting cloud computing in e-governance projects, establish more data centres and encourage the use of cloud computing by business and private organisations. It is commendable that the government has already taken significant steps by starting initiatives to promote cloud

[11] A. Tripathi, B. Parihar, “E-governance challenges and cloud benefit”, 2011 IEEE International Conference on Computer Science and Automation Engineering, 2011, pp.: 351-354

computing in industries such as health, education and also for different other over public & governmental services.

However, in our understanding all these various issues are linked together and there are a few critical success factors[12] that can be considered as cornerstones for any in such initiative to succeed. Thus, the first step the government can take now to further promote cloud computing in e-governance projects is to steer the development cycle to a faster pace by using policy initiatives to set milestone based objectives for adoption of cloud architecture in e-governance projects.

When the government itself becomes the users & adopters of new technologies, this action sets an example and facilitates and promotes the adoption of technology amongst other segments of the society comprising of both public and private entities. Thus, setting milestone-based objectives through adoption of new policies will encourage and promote cloud computing in not just e-governance projects but amongst all segments of the society.

Apart from e-governance projects, it is also important that use of cloud computing is prompted amongst business and private organizations. For this purpose tax benefits may be provided to such organisations, as creating tax benefits would incentivise the use of cloud computing and encourage these organisations to adopt the new technology. This approach has been highly successful internationally and even in India our government provides various incentives for specific industries such as power, ports, highways, electronics and software or incentives for units in less-developed regions or incentives for units producing exports or in export processing zones and SEZs. Software companies are currently granted a tax holiday on income generated, under Sections 10A and 10B of Indian tax laws, out of Software Technology Park of India (STPIs) — a concession that brings down the effective tax rates to 12-15 per cent, compared with the peak effective corporate tax of 33 per cent. A similar approach would facilitate the adoption and promotion of cloud computing amongst business & private organizations.

For establishment of data centres, it is essential that a joint collaboration with private entities and corporations should be taken. As seen in the last couple of years, private corporations like IBM, Microsoft and Oracle facilitated the establishment of lot of data centres in the country and many other are interested, thus a joint collaboration would help government not to just get more foreign investments but also creation of new jobs while facilitating the establishment of data centres.

To further boost Digital India initiative it is also important for government to involve more people

[12] Mahdi Mollahasani, Implementation of E-Government Based Approach on Cloud Computing, available at: https://www.academia.edu/7048844/Implementation_of_EGovernment_Based_Approach_on_Cloud_Computing

and adopt open standards. One of the biggest hurdles faced by people to adopt to cloud based technologies is the user interface and interoperability issues that come with such technologies. This perspective of the problem has to be given serious consideration because as many number of activities and initiatives the government might take, but such problems will keep hindering their path unless they are dealt with.

There is need to have a holistic view of development and amongst the different approaches suggested based on different international cloud standards, the best one to deal with issue of interoperability in cloud is the Open Cloud Computing Interface (OCCI). It builds upon World Wide Web fundamentals by using the Representational State Transfer (REST) approach[13] for interacting with services. It not only covers Infrastructure-as-a-Service (IaaS) based offerings but the interface can be extended to support Platform and Software as a Service offerings as well.[14] OCCI is also compatible with existing standards such as the Open Virtualization Format (OVF) and the Cloud Data Management Interface (CDMI).[15]

Question 19. 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?

Yes, in the light of Digital India Initiative started by the Government of India as well as other initiatives such as deployment of State Wide Area Networks (SWAN), Megh-Sikshak and the ‘GI Cloud’ Meghraj, to name a few, shows our government’s efforts to migrate different e-govenance platforms to cloud architecture & thus, it becomes imperative that there should be a dedicated cloud for government applications.

The National Policy on Adoption of Open Source Software for Government of India mandates all e-Governance applications and systems of the government to use Open Source Software as the preferred option. In combination with the Policy on Open Standards for e-Governance, it is clear that cloud solutions deployed for government applications have to be based on Open technologies.

[13] Fielding, Roy Thomas (2000), Architectural Styles and the Design of Network-based Software Architectures (Ph.D.). University of California. This chapter introduced the Representational State Transfer (REST) architectural style for distributed hypermedia systems. REST provides a set of architectural constraints that, when applied as a whole, emphasizes scalability of component interactions, generality of interfaces, independent deployment of components, and intermediary components to reduce interaction latency, enforce security, and encapsulate legacy systems. It is available at: http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

[14] A. Edmonds, T. Metsch, and A. Papaspyrou, "Open Cloud Computing Interface in Data Management-related Setups," Springer Grid and Cloud Database Management, pp. 1–27.

[15] Andy Edmonds, Thijs Metsch, Eugene Luster, An Open, Interoperable Cloud, available at: https://www.infoq.com/articles/open-interoperable-cloud

Such a ‘Government Cloud’ can have the following characteristics:

- Use open standards based cloud computing technologies for enabling multiple interoperable cloud environments.
- Such cloud environments may be managed and used at different levels of governance e.g state government, rural and urban local government bodies etc.
- They can easily be deployed together or separately depending on their scale of operation and availability of resources and can be transitioned between such stages with little effort.

The above model avoids the problems that come with deploying a centralized, national cloud that has to manage the dynamically growing demands across the country. Usage of open standards based technologies also enables easy migration of user-data across from one deployment to any other without fear of vendor lock-ins.

A number of governments around the world have started similar initiatives. Following are a few examples[16] of such initiatives:

Singapore

The Singapore Government has a multi-prong approach for cloud computing, keeping this perspective that different type of cloud works for different needs with each model providing its assurance & benefits:[17]

- Leverage commercially-available public cloud offerings for proper needs so as to benefit from lower cost of computing resources.
- Implement a private government cloud (G-Cloud) for whole-of-government use where security and governance requirements cannot be met by public clouds.
- Enable interoperability between G-Cloud and agency Clouds through a set of internal G-Cloud standards.

The Singapore Government Cloud or G-Cloud is the next generation whole-of-government infrastructure. It is aimed at providing efficient, scalable and resilient resources for cloud computing

[16] S Hashemi, K Monfaredi & M Masdari, *Using Cloud Computing for E-Government: Challenges and Benefits*, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:7, No:9, 2013, P. 1244, available at: http://waset.org/publications/17212/using-cloud-computing-for-e-government-challenges-and-benefits

[17] Cloud Computing for Singapore Government, available at: http://www.egov.gov.sg/egov-programmes/programmes-by-government/cloud-computing-for-government

and designed to meet different levels of security and governance requirements:[18]

- High Assurance Zone – a physically dedicated computing resource pool which will only be used by Government to serve its high assurance needs.
- Medium Assurance Zone – a computing resource pool which will be shared with non-government cloud users to lower cost of computing resources for Government.
- Basic Assurance Zone – a computing resource pool which is shared with public cloud users.

Common services on G-cloud include business analytics, customer relationship management and web content management, software as a service and platform as a service. The G-Cloud is aimed at enabling standardization, sharing of computing resources and applications at the government level, and thus generating cost savings.

USA

The official web portal of the United States government is one of the busiest website portals in the world as it receives approximately 342,000 visits daily.[19]

It is designed to help citizens to connect with the government departments efficiently. However, users frequently suffered long delays and downtimes during high traffic periods, such as voting seasons, monthly unemployment statistics release days, and natural disasters. In order to overcome this problem, U.S.A government decided to develop new IT hardware devices, which stays Idle most of the time when there is no high demand to access the web portal.[20]

Apart from using more power and it boasts of additional security features such as multifactor authentication and also physical security at cite of the data center buildings. But such a setup costs a lot for maintenance as the General Services Administration (GSA) spent around approximately two million dollars for software licenses and hardware upgrades in addition to 350,000 US dollars for staff costs each year.[21]

However, by shifting to cloud it helped in reducing costs (upto 90 %), while improving their system's flexibility & capabilities by adding automation, resulting into a scenario where customer requests are being handled in real time.[22]

[18] Ibid.

[19] D.C. Wyld, Moving to the cloud: An introduction to cloud computing in government. Washington, DC: IBM Center for the Business of Government, available at: http://faculty.cbpp.uaa.alaska.edu/afgjp/padm601%20fall%202010/Moving%20to%20the%20Cloud.pdf

[20] Mahafuz Aziz Aveek, Md. Sakibur Rahman, "Implementing E-Governance in Bangladesh Using Cloud Computing Technology", BRAC University, Dhaka, Bangladesh, 2011

[21] Ibid.

[22] Toby Velte, Anthony Velte, Toby J. Velte, Robert C. Elsenpeter. Cloud Computing: A Practical Approach. New

UK

The UK government has also come up with their own “G-Cloud” as part of their strategic priority for a government-wide cloud computing network. It is part of their Digital Britain Strategy of which one of the most important aspects being increasing IT use in government & online migration of different government services.

For fulfilment of this goal, UK’s It procurement efforts have been focused on making their government a leading force as users of cloud computing. Their aim is to use their position as the lead procurer of services, to drive up standards & in some cases set standards in many areas of public sector like education, health & defence and to provide an investment framework for research & development.[23]

Japan

The National government of Japan has undertaken a major cloud computing initiative dubbed as the “Kasumigaseki Cloud”, named after the section of Tokyo where many Japanese government ministerial offices are located.[24] The initiative’s aim is to develop a private cloud which would host all of Japanese government’s computing. According to Japan’s Ministry of Internal Affairs and Communications (MIC), the Kasumigaseki Cloud will provide greater information and resource sharing and promote more standardization and consolidation in the IT resources of government and by consolidating all governmental IT under a single cloud infrastructure, the Japanese government believes it will see not just reduced costs and operational benefits, but more “green,” environmentally friendly IT operations.[25]

The Kasumigaseki Cloud is part of the Digital Japan Creation Project and it represents a governmental effort aimed at using IT investments (valued at just under 100 trillion yen) to help spur economic recovery by creating several hundred thousand new IT jobs in the next few years and doubling the size of Japan’s IT market by 2020.[26]

Thus, in light of the above having a dedicated cloud for government application & services seems to be the most logical step considering current government initiatives, international trends & benefits

York: McGraw Hill Professional, 2010, PP.274

[23] Supra. 11

[24] R. Hicks, “The future of government in the cloud,” FutureGov, 6(3), pp. 58-62, May 2009.

[25] David C. Wyld, The Cloudy Future of Government IT: Cloud Computing and the Public Sector around the World, International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, January 2010, pp.1-20.

[26] As J.N. Hoover, “Japan hopes IT investment, private cloud will spur economic recovery: The Kasumigaseki Cloud is part of a larger government project that's expected to create 300,000 to 400,000 new jobs within three years,” InformationWeek, May 15, 2009, available at: http://www.informationweek.com/shared/printableArticle.jhtml?articleID=217500403

that such a dedicated government cloud can provide.

We also need to understand the importance & relevance of a multi-tenant environment. Multi-tenancy or in other words resource pooling refers to a such an architecture in software environment where a single instance of software that runs on a server can work for different groups of people, while each is isolated from other.

A tenant is essentially a group of people say for example any organisation or company who share a common access with each having specific privileges to the software instance. With a multitenant architecture, a software application is designed to provide every tenant a dedicated share of the instance - including its data, configuration, user management, tenant individual functionality and non-functional properties.[27]

Many regard this Multi-tenancy architecture to be one of the major attributes of cloud computing. To make the above discussed architecture work, virtualization technologies are used. However, it's known fact that these underlying components that make up this cloud infrastructure are not designed to offer strong isolation amongst different tenants and there is always a risk of guest operating systems gaining huge amounts of access or control to the platform itself which makes it bit vulnerabilities.

Thus, it becomes highly imperative that a dedicated government cloud which has higher security needs should not be shared with outside entities from private or public sector. A private government cloud work better than a public one, but if the Government of India still feels a need to create a platform accessible different segments, then different approaches such as either a separate dedicated public and private cloud or different hybrid cloud models could be explored.

[27] Krebs, Rouven, Proceedings of the 2nd International Conference on Cloud Computing and Services Science (CLOSER 2012), SciTePress, available at: http://se2.informatik.uni-wuerzburg.de/pa/uploads/papers/paper-371.pdf