ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

Security Risks & Migration Strategy For Cloud Sourcing: A Government Perspective

Dr Mansaf Alam, Shuchi Sethi

Abstract -- Governments of various countries all over the globe, irrespective of their economic & technological standing on the world stage, are realizing the benefits of cloud computing and devising strategies to migrate their IT systems to the Cloud, a trend also called Cloud sourcing. In this paper, we identify the prerequisites government agencies should consider before moving to the cloud. Then we examine various security challenges government organizations may face in the process of Cloud migration and the possible options to mitigate these security threats. Finally, we discuss multiple cloud deployment options and propose a strategy for the government agencies planning to opt for cloud sourcing.

Keywords- **Cloud Sourcing; Cloud Computing; Government; Security Risks; Cloud Migration Strategy;**

I. INTRODUCTION

Cloud computing is a revolution in the manner the power of computing is used and it has a potential to significantly impact the way both developing and developed nations handle their IT operations[2][7]. The budget pressures will take governments towards the option of hybrid and even public clouds. As cost is reduced in IT spending, tax payer's money can be used in other welfare activities for citizens. Governments across the world are enthusiastic to embrace cloud sourcing due to its advantages such as massive cost reduction (about 50% to 90%), de-duplication of citizens' data across government institutions, operational efficiency of government staff by consolidating services and data storage on cloud, reduction in time for new service developments, scalable easy scalability, responsive to urgent needs and emerging technologies, and moreover better disaster management if one area of a country is affected by some calamity then backup data can be provided by cloud provider to keep things going on smoothly. And as Microsoft puts it - Its cheaper, faster and greener. [9] Gartner uses the term cloud sourcing to refer to the way that organizations provision services. In this paper, we discuss how government should go about cloud sourcing. One principle by Schwartz says that a context business practice should be moved to cloud while core practices should be tightly secured*.If we go by this theory in government then a few areas can be identified where government should initially plan to move to cloud and later as trust in security of cloud is increased some non mission critical core practices can be put on cloud. However, inspite of many of the known benefits of cloud computing, many hurdles are expected in moving to cloud – one of them being the reluctance from within the government as with any government change isn't welcome. Vivek Kundra, former white house CIO quoted that in human body if white blood cells perceive anything as virus they attack it and in government any change is treated as virus and arguments used in favor are related to security hazards in cloud adoption. Some hard work is needed to convince the government that the security risks involved in cloud adoption can be mitigated to a great extent. We will discuss some of these security risks in the next section. Besides, there are certain prerequisites to be taken care of before a country's government IT operations move to cloud[23][30]. These are depicted in figure 1.

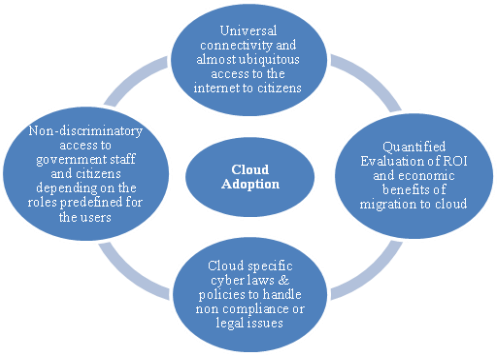


Fig 1

*Core is any activity that creates sustainable differentiation in the target market resulting in premium prices or increased volume. Core management seeks to outperform all competitors. Context is any activity that does not differentiate the company from the customer's viewpoint in the target market. Context management seeks to meet appropriate accepted standards.

II. SECURITY RISKS TO GOVERNMENT CLOUDSOURCING

Despite the fact that cloudsourcing offers major advantages to governments of the countries in running their IT operations, there are many challenges ascribed to the cloud model. In this section we discuss the one most feared risk that government agencies cite with respect to cloud migration, viz., Security.[10][[13][24] Different categories of security risks are described below, and in next section, we provide multiple mitigation techniques for each risk. SR1 – Security risks due to resource sharing in Multi-tenant cloud environments: Large scale sharing of IT resources (such as hardware, OS, applications, platforms) is not something the government agencies are familiar with based on their experience with traditional IT systems. Multi-tenancy is one of the crucial feature of cloud computing that leads to cost reduction for end users, however it opens up possibilities for information security risks and data theft since the tenants sharing common resources may access each others' data, virtual machines, or network traffic[12][21]. SR2 -

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

Concerns over data protection: Confidentiality, Integrity & Availability of sensitive government and citizens' data: This is the most important concern raised by any prospective user of cloud computing, however in case of government, since the stakeholders are citizens, government employees or highly sensitive government departments, the stakes are extremely high. This calls for clear understanding on part of decision makers to understand the extent of security that cloud environment would provide and accordingly select the application and services that should be moved to cloud. SR3 - Lack of visibility of cloud vendors' security measures to government agencies and service consumers: There is a certain level of transparency needed in the cloud by government stakeholders to be able to monitor and audit the security measures implemented by cloud vendors. However, these security measures are proprietary to the vendor and government law can also not enforce the cloud vendor to give away their competitive advantage.

SR4 - Lack of Control with government agencies and service consumers over security policies enforced by cloud providers: There are 2 growing concerns that arise due to lack of control by government IT department. One is location and policies to protect workloads are not known to the cloud users so they may feel they are unable to control their workloads as some policies can technically affect the application speed etc .Second is the security policies the IT department wants to enforce at different levels like data level, application level, network or geographic level which may be shared by many organizations having different non homogeneous policy needs and moreover there is no automation possible for such cases. SR5 - Application and Account level security issues: As cloud is a model based on internet which has its own security concerns like hacking where accounts can be misused, this is aggravated due to new cloud specific Interfaces and APIs in use that are not tested for security over time. SR6 - Security compromise due to weak Identity, Access Mgmt & Authorization techniques: The issue is which access control mechanisms should be applied and which credentials can be super safe and how safe and authentic is the authorizing authority[31]. SR7 - Cloud based denial of service: As cloud is all network based we may have high latency which is more like denial of service as timely service is the core of governance[31]. SR8 - Incident response and computer forensics: This is very difficult to achieve due to its requirements of specific tools and training required to assess and analyze situation accurately and support argument with evidence. Without this cloud cannot be treated as secure.

III. MIGRATION STRATEGY TO CLOUD

Government, being a complex organization needs to make a strategy based on several factors. First decision needs to be taken as whether a service should be moved to cloud and find good reason to support it. Then move to which services to be moved to cloud and then what kind of cloud solution it wants to go for Government needs to study the factors and decide on pilot project it wants to go for, then choose among various Deployment and Delivery models. A few technical factors which help in decision making are:

- Budget
- Security
- Flexibility to customize
- Features needed
- Interoperable with existing application solutions

In this section, we start with proposing multiple cloud deployment options – based on SaaS, PaaS, IaaS, along with scenarios where each option is advisable [9][25]. We also provide detailed mitigation techniques for each of the security risks identified in previous section in Table 1 [10][13][24]. And finally, we present a strategy for government migration to cloud.

A. Deployment Options on Cloud SaaS:

Opting for this model by government can lower the cost associated with owning the expensive software .It allows for acquiring the software and resources in a quick manner which may otherwise take long and the government may get better features than it had planned for. This also benefits in terms of reduced staffing needs saving those costs and use the expertise of the providing company. One instance where this has proved useful is in the city of Carlsbad, California; Municipal government's IT has 100 employees and work in 22 departments. They needed an email solution. So by choosing cloud services they had 24 hrs a day support, disaster recovery, cost effective and also more secure with provider's latest security techniques.

***When to choose*:** Various areas where SaaS can be considered: email, collaboration and office solutions; Relationship management; payment processing; e government projects.

PaaS:

Provider provides environment to develop applications as per required features those can be multitenant and shared by many users. This provides better flexibility and interoperability than SaaS. One case where this has been implemented is by US DoD. It uses for emulating real time conditions for testing applications and pays only for time its used.

***When to choose*:** This model should be chosen when need software for collaboration but for multiple agencies; need applications that are to be shared by multiple users; need to move present applications to cloud; needs like government has to pull data from various sources and to display public data for transparency.

IaaS:

It provides ready to use data center at the time of spikes in demand but managing everything lies with government so it won't be reducing staffing needs rather may increase but it can save the hardware costs and time. Also this can prove very secure as government can implement own firewall and security strategies. To quote one successful instance GSA (General Services

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

Administration) expect to cut its hardware costs by 90% with the use of cloud. NASA Nebula gives access to its researchers through its community cloud in minutes while earlier it took months in procuring and configuring for each researcher. It can be used as SaaS, PaaS or IaaS.

***When to choose*:** Useful for citizen services and websites; testing large scale sensitive applications before it goes live; large amount of data needs to be stored securely free from terrorist or calamity threats.

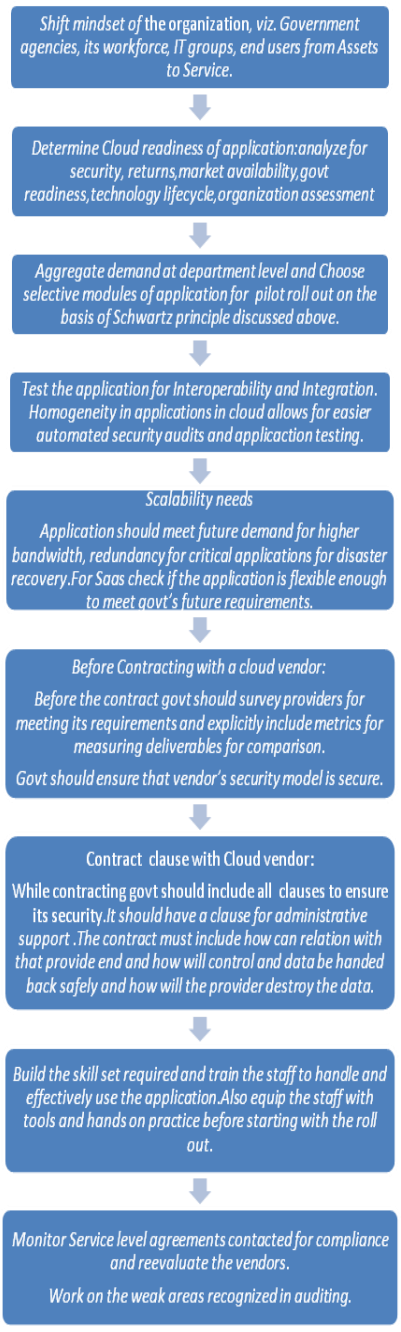
TABLE 1 Mitigation Techniques for Cloud Security Risks

Security Risk	Mitigation	
	Technique 1	Technique 2
SR1	Data Encryption • Separate encryption techniques should be used for separate stages of data. As with certain encryptions data can be processed in encrypted form so such option should be considered.	Application partitioning and Logical separation • VM be hardened and hypervisor should be isolated to enable access by authorized APIs. • Separate application parts which have different security needs.
SR2	Managing data separately based on its state. • At rest data needs to be prevented from tampering and keep encrypted. In transit connections be secured and encrypted and use signature for integrity. In processing data leakage should be prevented.	Information lifecycle management • Standard models like Create, Store, Use, Share, Archive, and Destroy have standard security practices that can be implemented as such.
SR3	Service Level Agreements • Customization of policies and transparency in cloud security policies of provider should be there	Monitoring • Centralized end to end monitoring including log files etc will give greater visibility and information about further specific security needs
SR4	Choose the right model • Though public model has less control than private but cost advantages are trade off, but while choosing deployment models government can prefer IaaS over SaaS if more control is critical need	Control over VMs, Application and Data • Software patches updation is must to keep VM secure and APIs should be secured and VM hardening be done based on standard procedures; this will allow more security controls and transparency. Besides data logs be prepared for data security control. To control the geographic location government can restrict areas where its data is kept and timely visit the centers.
SR5	Authentication and secure APIs • Make password policy strong and have session passwords and validations should be strong.	Encryption • Dedicated VPNs, secure cookies, using https and similar measures can ensure authentic access to some extent.
SR6	Access levels • At application level another access control may be provided besides provider level access control and different policies and techniques be followed. Digital identity can be given to government users which can be role based and it will automate the access control.	External Identity system • Authentication of source is done by a third party for the government that this data comes from trusted source.
SR7	More than one provider • If there is a service issue with one provider then there is a chance that the service from other provider is still available.	Contract terms • Government should have various clauses in contact for uptimes and also for redundancy so that availability is high.
SR8	Case Plans • Cloud providers should provide the government with various possibilities of worst cases and its plan chalked out in detail and role to be played by each party.	Recovery • Once the problem has been reported and registered for future also, the effect of it should be nullified by planned activities and recovery of any loss should be done as soon as possible.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

B. Proposed Strategy for Migrating to Cloud

Suggested steps for moving a service securely to cloud by the government [16]:



III. CONCLUSION & FUTURE WORK

For any technology to grow it should have standards that defines how it will function end to end. In absence of these standards fears and conflicts will persist and the technology cannot gain wide popularity and acceptance. So the authors believe that the proposed framework will to some extent prove to be a starting point. There may be a few non standard models being followed for moving to cloud but standardization of a model is needed for governments which will have certain defined steps for moving to cloud while giving flexibility in the model for adapting all practices and means of securing the data and applications by the governments IT team. The work towards standardizing certain procedures should begin that will ensure safety of parties involved and we may have the ultimate goal of government as a service which means there will be true democracy where the government reaches out to every citizen of the country with proper user of technology.

REFERENCES

[1] John van Huijgevoort, "Cloud Computing security in the Dutch Government", 2012.

[2] "State and Local Cloud Computing Case Studies", Online: http://www.info.apps.gov/content/state-and-local-cloud computing-case-studies.

[3] Jorge Casos, "Towards a European Cloud Computing Strategy', Secure Cloud 2012.

[4] "The US Government's Latest Move In Cloud Computing – FedRAMP", June 2012, Online: http://www.cloudtweaks.com/2012/06/the-us-governments-latest-move-in-cloud-computing-fedramp/.

[5] "UK government may miss cloud computing targets", BBC, May 2012, Online: http://www.bbc.com/news/technology-18103750.

[6] "Public-sector cloud computing: The good, the bad and the ugly", Computer World, May 2012, Online: http://www.computerworld.com/s/article/9226932/Public_sector_cloud_computing_The_good_the_bad_and_the_ugly

[7] "Exploring the Cloud: A Global Study of Governments' Adoption of Cloud", KPMG.

[8] Tal Garfinkel, Mendel Rosenblum, "When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments", Stanford University Department of Computer Science.

[9] Online:http://static.usenix.org/events/hotos05/prelim_papers/garfinkel/garfinkel_html.

[10] Security in the Cloud, Online: http://www.microsoft.com/industry/government/guides/cloud_computing/3-security.aspx.

[11] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST, US Department of Commerce, Special Publication 800-144, December 2011.

[12] Dr Antonio Mauro, "Cloud Computing Security for DoD/ Governments (US), 7th Annual IT Security Automation Conference, November 2011.

[13] Cloud Security Alliance, http://www.cloudsecurityalliance.org.

[14] NIST, US Department of Commerce, "Challenging Security Requirements for US Government Cloud Computing Adoption (Draft)", November 2011.

[15] "The 10 worst cloud outages", InfoWorld, June 2011, Online: http://www.infoworld.com/d/cloud-computing/the-10-worst-cloud-outages-and-what-we-can-learn-them-902?page=0,1.

[16] Armedia Blog, Posts tagged "Government Cloud Computing Security Concerns", Online:

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 7, January 2013

http://www.armedia.com/blog/tag/government-cloud-computing-security-concerns/.

[17] Vivek Kundra, "Federal Cloud Computing Strategy", February 2011, Online: http://www.scribd.com/doc/49043575/Federal-Cloud Computing-Strategy-Vivek-Kundra-U-S-Chief-Information-Officer.

[18] Government Clouds, Cloudbook, Online: http://www.cloudbook.net/directories/gov-clouds/government-cloud-computing.php.

[19] Salvatore D'Agostino, "Moving to the Cloud: A white paper produced by the Cloud Computing Use Cases Discussion Group", Version 1.0, February 2011, Online: http://cloudusecases.org/Moving_to_the_Cloud.pdf.

[20] European Network & Information Security Agency (ENISA), "Security & Resilience in Government Clouds", January 2011.

[21] Dr. Giles Hogben, "ENISA - Cloud Computing Security Strategy", European Network and Information Security Agency, 2011

[22] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma, "Cloud Computing Security - Trends and Research Directions", IEEE World Congress on Services, 2011.

[23] "Security Risks of Moving to the Cloud – Risk Assessment (Part 1)", October, 2010, Online: http://cloudshoring.wordpress.com/2010/10/05/security-risks-of-moving-to-the-cloud-risk-assessment-part-1/.

[24] Shahid N. Shah, "Cloud computing by government agencies. Meeting the business and security challenges in the Cloud", IBM Developer works, August 2010, Online: http://www.ibm.com/developerworks/industry/library/ind-govcloud/.

[25] Lee Badger, Time Grance, "Standards Acceleration to Jumpstart Adoption of Cloud Computing", NIST, May 2010.

[26] "Forecast: Improved economy in the cloud. An Introduction to cloud computing in government", A Microsoft U.S. government White paper, March 2010.

[27] "Government regulation looms over cloud security", Search Cloud Computing, 2010, Online: http://searchcloudcomputing.techtarget.com/news/1523889/Government-regulation-looms-over-cloud-security.

[28] "Feds resist cloud computing over security concerns", Info security, 2010, Online: http://www.infosecurity magazine.com/view/9307/feds-resist-cloud-computing-over-security-concerns/.

[29] 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.

[30] Peter Mell, Tim Grace, "Effectively and securely using the Cloud Computing Paradigm", NIST Information Technology Laboratory, 2009.

[31] David C. Wyld, "Moving to the Cloud" An Introduction to Cloud Computing in Government", IBM Center for the Business of Government, 2009.

[32] Gartner: Seven cloud-computing security risks, Online: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1, 2008.