Journal of Network and Information Security
Volume 5 Issue 2 2017
ISSN.: 2321-6859

Assessment of Cloud Computing Security Risks for E-Governance Infrastructure

Riktesh Srivastava
Associate Professor, Information Systems Skyline University College Sharjah, UAE.

Abstract: The advances in web-based technologies is changing the way we work and interact. These changes are also stirring the approach government interacts and associates with citizens, businesses, employees and keeping affiliations with other local or federal governments. Governments have strained and still incessantly pondering on the methodologies to improve these interactions and deploy services (called e-services), though, faced numerous challenges in developing and implementing web-based technologies. Apart, these technologies were expensive in terms of labor cost and consumes enormous capital investments. Advent of cloud computing helped the governments sought the issues, as usage of cloud computing reduces IT labor cost by 50% and improves capital utilization by 75%. Even after spotting the benefits of using and deploying services in cloud, governments have been slower in appreciating the profits of cloud computing. The main causes for this cynical approach are security and data protection. The paper conducts the risk valuation for employing e-services in cloud computing architecture and ascertains the types of risks allied. The study will assist as guideline for government departments to implement e-services on cloud models.

Keywords: Cloud computing risks, e-Governance Infrastructure, Slave data center, Master data center

I. Introduction

E-governance is a process of enhancement in the mode governments offer e-services which can be automated and linked to various other entities. Connecting these applications aids government in decision making and policy administration. Fig. 1 below illustrates the offering of e-services to four different types of entities, namely businesses, citizens, employees, and government itself [1].

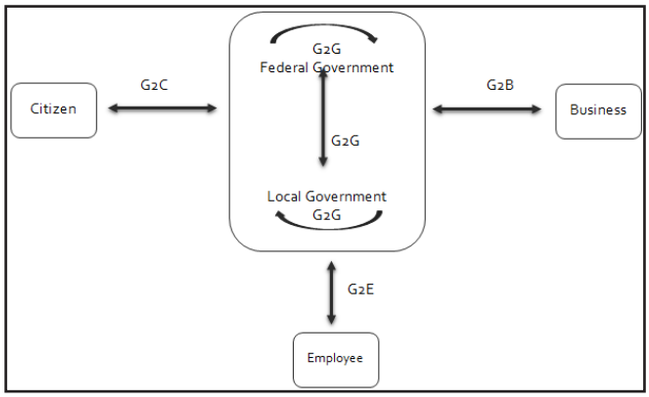

Fig. 1: E-Governance Applications

The comprehensive classification of e-governance implemented on cloud are exemplified in Table 1 below:

Table I: Types of E-Governance

Types of e-Governance	Explanation
G2B (Government to Business)	Interactions between Government and Businesses [2]. Some of the examples includes: issuance and renewal of trade licenses, payment of taxes etc.
G2C (Government to Citizen)	Interaction between Government and Citizen [3]. Some of the examples includes: Renewing of driving license, payment of traffic fines, renewal of house contract etc.
G2E (Government to Employee)	Refers to relationship between e-government and its employees [4]. Examples include: Giving access to employees to perform e-services.
G2G (Government to Government)	This comprises of providing the services, sharing databases and resources between different government departments and agencies [5]

In mandate to deliver the above stated four types of e-governance, United Nations e-Government Survey [6] offered a mechanism of interaction of government with stakeholders called "e-Strategy", as stated below:

- e-Strategy = SS+DD+II

where,

SS→ Static + Supply based

DD→ Dynamic +Demand Driven

II→Interactive + Integration

The strategy elaborates the e-Government development stages from Static to Interactive and Integrated applications. Government has countless applications that should be interactive and integrated [7]. As mentioned in the strategy, with the advent of internet technologies, the citizens where now demanding the continuous interactions with various government departments. Owing to this high demand, present study contains an execution of an updated e-Strategy, termed e-Revised-Strategy, which includes additional parameter, CC, to be added, where, CC depicts cloud computing.

- e-Revised-Strategy = SS+DD+II+CC

Although there are many benefits of adopting cloud computing, there are also some major obstacles to adoption. One of the main barriers is security risks pertaining to privacy [8]. Security concerns relate to risks such as external data storage, reliance on public internet, and integration with internal security. Also, exposing services on web, it provides way for intruders to gain unauthorized access to these applications [9]. This insecurity has continually led Governments to argue that interactive and integrated applications is number one threat [10]. Traditional security mechanisms are no longer enough for cloud computing in the current form [11]. The study is a categorization of security risks for implementing e-governance through cloud computing.

Section 2 presents the adoption models for three stages of e-Strategy. Section 3 exemplifies e-Revised-Strategy and introduces the cloud computing infrastructure. Section 4 explains the detailed analysis of security risks pertaining to adopted infrastructure. Section 5 concludes the illustration.

II. E-Governance Adoption Models-Earlier Stages

In order to narrate e-Strategy to cloud computing, it is essential to study a bit of past (called stages) of e-Governance adoption models. The initial phase of e-Governance was static, wherein, the government created the website and uploaded the contents as web pages. All the four types of stakeholders (G2G, G2E, G2B, and G2C) can only view the contents, without any interaction. Sometimes, the contents of website were not uploaded for years, leading to deceptive information flow. This is SS state of e-Strategy as mentioned in Fig. 2 below.

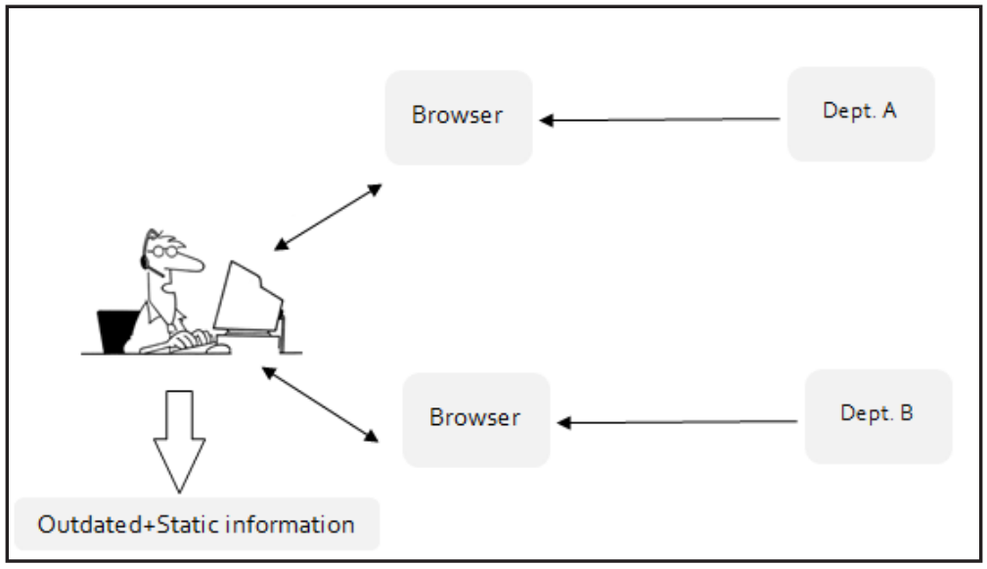

Fig. 2: SS State of e-Governance Model

Later in the late 90s, almost every government started using databases for an updated and dynamic information flow as stated in Fig. 3. Although the information received was updated, the component of interactivity was still absent. This means that citizens, businesses, and other government departments cannot interact with each other and depends on traditional modes of communication.

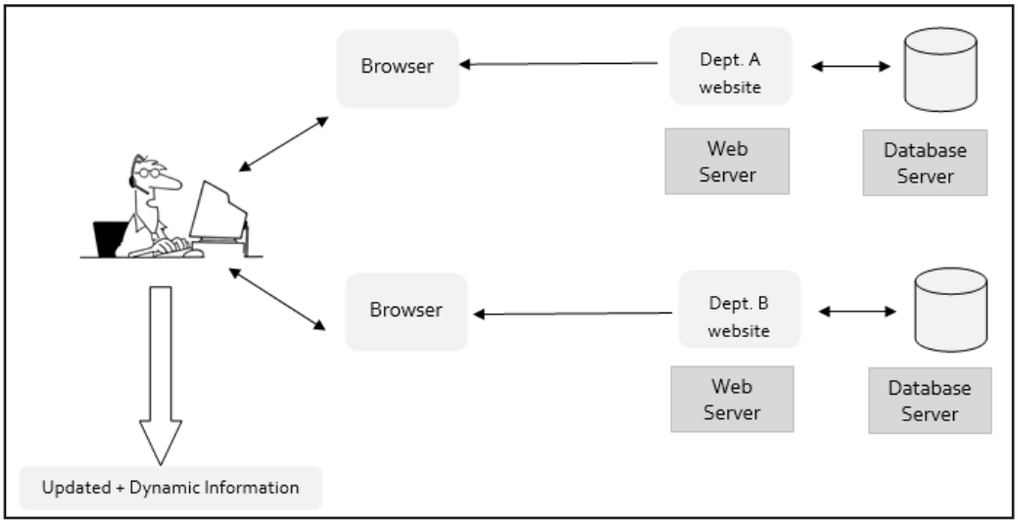

Fig. 3: DD State of e-Government Model

The shift from DD to II (Interactive and Integration) requires the current e-Governance model to be changed technically. The presence of Application Server(s) in the Model, which makes the communication interactive and thus requires a major drift in the complete implementation. Application Servers is used to generate business logic and interacts with database Server more efficiently.

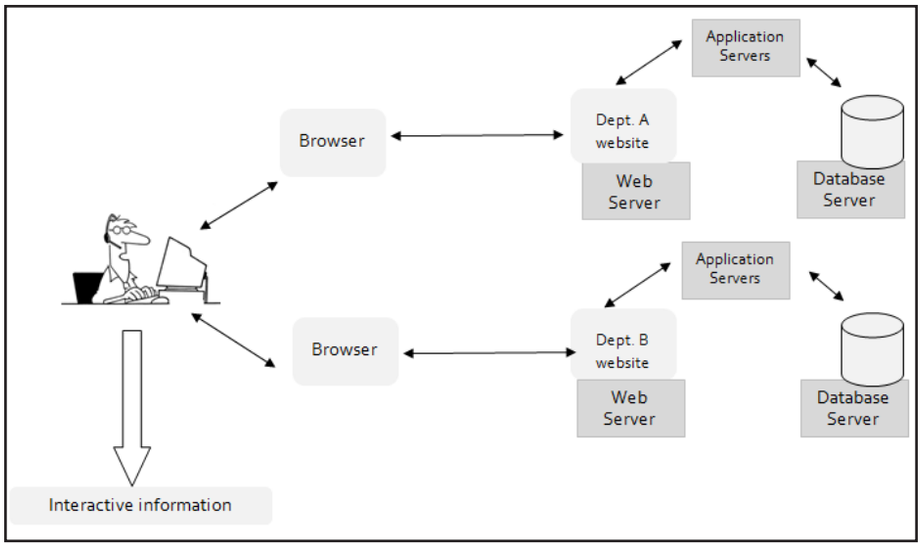

Fig. 4: II State of e-Governance Model

The architecture as mentioned in Figure 4 was sufficient to provide timely interactions and e-services to all four customers of e-governance. However, there were following 5 technical challenges for maintaining the architecture [12], which includes:

Application Life Cycle Management: In order to maintain II state of e-governance, there was need to safeguard security and cost-effective management of structured data. Many government departments continued their own application and database servers, resulting in duplication of resources.

Software Licensing and Support: Every government department needs to procure and obtain support for same type of software's, which was unwieldly job.

Scalability: The architecture cannot match the scalability required over time.

Accountability: None of the government departments were accountable for system failure (though these systems were owned by them) and were exclusively reliant on on third party support.

Modifiability: Since the architecture was difficult to scale, architecture modification was much problematic task to accomplish.

As mentioned, although the infrastructure for II state solved majority of glitches, maintenance and continuous upgrade was a major challenge.

III. E-Governance Infrastructure Using Cloud Computing-CC State

The most accepted e-governance infrastructure [13] was adopted for the study. The complete infrastructure is divided into two parts, as depicted in Fig. 5 below:

- Master Data Center
- Slave Data Center

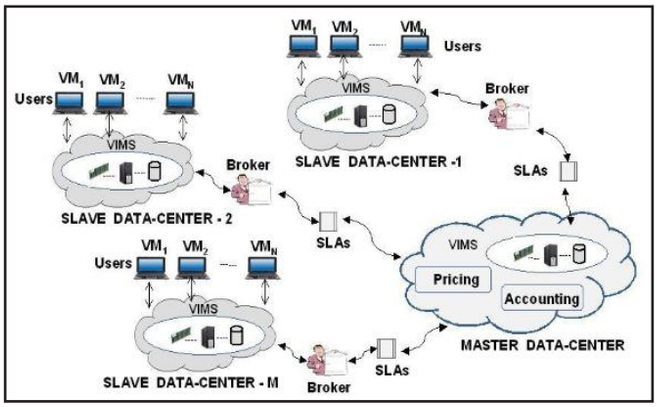

Fig. 5: Cloud Computing based e-Governance Infrastructure

It must be noted here that the security analysis piloted is not for SaaS, PaaS or IaaS Cloud adoption model, rather follows the generic configuration of security exploration.

Master Data Center is the main data center and Slave Data Center is the data center for individual government departments. The employees of individual departments are connected to Slave Data Center through virtualization (VMs), and the Slave Data Center is connected to Main Data Center through brokers/SLAs through Internet connection.

Based on Fig. 5, the components of e-Governance Infrastructure are:

- Master/Slave Data Centers: Master Data Center is the main data center hosted in public cloud and provides the services required for Slave Data Centers. It works on pay as you go concept.
- Brokers: Brokers are an optional service. If opted, then brokers maintain the log of pay as you go model.
- SLA (Service Level Agreements): Quality of Service and customer log is maintained at SLA's.

IV. Identification of Security Threats for Cloud Computing based e-Governance Infrastructure

Section 3 mentions the e-Governance infrastructure that can be separated into 3 parts. Part 1 mentions virtualization threat, part 2 evaluates communication threats and part 3 identifies data threats. In order to recognize the security threats, the complete analysis is divided into three sections, namely,

Part 1 [Slave Data Center Security]: This part is generally associated to VM security issues.

Part 2 [Cloud Computing Communication Security]: Part 2 is typically allied to security issues of data movement between Slave Data Center and Master Data Center.

Part 3 [Master Data Center Security]: Part 3 classifies the security related to the Master data center, which includes security issues are relating to resource allocation and data management.

A. Security Threats at Part 1

The security threats of part 1 are mentioned in Table 2 below:

Table II: Security Threats for Part 1

Part 1 Security Threats	Description
Resource allocation at VM	Unrestricted allocation and deallocation of resources with VM [14]
Uncontrolled Migration	There are situations when we need to migrate VM from one server to another due to fault tolerance, load balance and hardware failure [15], [16]
VM Snapshots	VMs can be copied to provide better flexibility, which leads to data leakage [17]
Rollback Error	VMs need to be rolled back for restoration, but patches applied after the previous state goes [16]
Cloud Cartography	VMs are mapped to an IP address, which can be accessed by anyone within the cloud [18]
Placement of VM Images	Creation of VM images in public repositories, may result in unwanted access [19]
Virtual Bridge	Sharing of Virtual Bridge by several VM (Virtual Bridge virtualizes disparate networks into one logical WAN) [20]
Load Balance	For 24x7 Cloud service availability, Load Balancer are used, which is prone to penetration testing [21]
VM Escape	Technique designed to exploit the hypervisor to take control of Cloud Infrastructure [22]
Spoofing Virtual Networks	Malicious VM can redirect packets from/to other VMs [23]

Part 1 Security Threats	Description
Malicious VM creation	User with a valid account can create VM image containing malicious code and store it in repositories [24]
VM Hopping	This condition happens when one VM tries to gain access of another VM [25]

B. Security Threats at Part 2

The security threats of part 2 are mentioned in Table 3 below:

Table III: Security Threats for Part 2

Part 2 Security Threats	Description
Malware Injection Attack	Cloud Computing offer Web-based applications for users to access application servers via a web browser. Such a service is prone to attacks [26] such as cross site scripting, injection flaws, information leakage and improper error handling, broken authentication and session management, failure to restrict URL access, improper data validation, insecure communications, and malicious file execution. [27]
Wrapping Attack	Wrapping attacks use XML signature wrapping (or XML rewriting) to exploit a weakness when web servers validate signed requests. [28]
Malicious Code Attack	Spyware and Adware Trojans are often installed without the user knowledge and record the user's behavior when accessing the data from the Master Data Centers and also user can even download other malicious software. [29]
DDOS Attack	It is a type of attack on a network that is designed to bring the network down by flooding it with useless traffic. [30]
Phishing	Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. [29]
Packet Sniffers	Interception of Data packets to and fro from SDC to MDC and vice versa. [30]
Communication Line Tapping (Hijacking)	Hijacking occurs when intruder is actively monitoring, capturing, and controlling communication transparently. [30]

C. Security Threats at Part 3

The security threats of part 3 are mentioned in Table 4 below:

Table IV: Security Threats for Part 3

Part 3 Security Threats	Description
Insecure Interfaces and APIs	Individual Departments still use legacy systems and the services can be accessed through APIs (SOAP, REST or JSON). The security of the cloud depends upon the security of these APIs. [15]
Data Remnants	When data is moved from one server to another in MDC, traces of data cannot be completely removed. [31]
Data Colocation	Data can be collocated with the data of unknown owners (competitors or intruders) with a weak separation. [32]
Data Backup	Data backup by untrusted third party providers. [33]
Undisclosed Data Location	Information about data location is usually not provided to users. [34]
Data Storage	Data is often stored, processed and transferred in plain text.
Data Leakage	Data Leakage happens when it goes in wrong hand while being stored, processed or transferred. [35]
Customer Data Manipulation	User get access to data while being transferred between SDC and MDC. The attacks includes SQL injection, command injection, insecure direct object references and cross-site scripting.

V. Conclusion

The study is an attempt to recognize two major characteristics pertaining to adoption of cloud computing for e-Governance. The first one is identification of three parts of cloud computing complete infrastructure thereby revision of e-strategy (named as e-Revised strategy) and secondly, recognition of security risks at each of these three parts. The paper will prove helpful for decision makers to evaluate the risk first and furthermore deploy the security measures accordingly. The study does not confirm the security measures to be taken for risks mentioned, and is part of future research to be conducted.

References

[1] M. A. K. Badri, "A Path analytic model and measurement of the business value of e-government: An international perspective," *International Journal of Information Management,* pp. 524-535, 2008.

[2] J. Rowley, "E-government stakeholders: Who are they and what do they want?," *International Journal of Information Management,* pp. 53-62, 2011.

[3] L. P. V. B. Torres, "E-government developments on delivering public services among EU cities," *Government Information Quarterly,* pp. 217-238, 2005.

[4] H. S. Chourabi, "E-government: Integrated services framework," In *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, 2011.

[5] L. P. V. A. B. Torres, "E-government developments on delivering public services among EU cities," *Government Information Quarterly,* pp. 217-238, 2005.

[6] H. Qian, "Global perspectives on e-governance:from government-driven to citizen-centric public service delivery," UN, 25-28 October 2010. [Online]. Available at http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN040614.pdf. [Accessed 11 December 2016].

[7] V. Varma, "Cloud computing for e-governance," *The Financial Express,* India, 2013.

[8] KPMG, "From hype to future: KPMG's 2010 cloud computing survey," 2010. [Online]. Available: www.kpmg.com.

[9] T.-S. Chou, "Security threats on cloud computing vulnerabilities," *International Journal of Computer Science & Information Technology,* vol. 5, no. 3, pp. 79-88, 2013.

[10] K. S. L. Mather T, Cloud Security and Privacy, Sebastopol,CA: O'Reilly Media, Inc., 2009.

[11] L. P. Wenjuan Li, "Trust Model to enhance security and interoperability of cloud environment," In *First International Conference, CloudCom 2009, December 1-4, 2009. Proceedings*, Beijing, China, 2009.

[12] IIITHydWhitePaper, "Cloud Computing for E-Governance," 01 01 2010. [Online]. Available: http://search.iiit.ac.in/uploads/CloudComputingForEGovernance.pdf.

[13] S. M. Reddy, E. Mruthyunjaya, and J. Srikanth, "Cloud computing architecture supporting e-governance," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 2, no. 8, pp. 370-375, 2012.

[14] V. Winkler, S*ecuring the Cloud Computer Security Techniques and Tactics,* Waltham, MA: Elsevier Inc., 2011.

[15] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," In *7th International Conference on Informatics and Systems (INFOS)*, Postdam, Germany, 2010.

[16] R. M. Garfinkel T, "When virtual is harder than real: Security Challenges in virtual machine based Computing environment," In *10th Conference on Hot Topics in Operating Systems*, Santa Fe, NM, USA, 2005.

[17] Rittinghouse, J. W., & Ransome, J. F. *Security in the Cloud, Cloud Computing: Implementation, Management and Security,* CRC Press, 2009.

[18] T. Ristanpart, E. Tromer, H. Sacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," In *16th ACM conference on Computer and Communication security*, Illinois, USA, 2009.

[19] M. A. Morsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," In *APSEC 2010 Cloud Worksho*p, Sydney, Australia, 2010.

[20] H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in cloud computing," In *5th International Conference on Computer Sciences and Convergence Information Technology*, Washington, USA, 2010.

[21] C. Shaffer, "Identifying load balancers in penetration testing," The SANS Institute, 2010.

[22] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," In *17th International Workshop on Quality of Service*, Washington DC, USA, 2009.

[23] J. S. Reuben, "A survey on virtual machine security," Helsinki University of Technology, Helsinki, 2007.

[24] Grobauer B, Walloschek T, Stocker E, "Understanding the cloud computing vulnerabilities," *IEEE Security Privacy,* vol. 9, no. 2, pp. 50-57, 2011.

[25] A. Jasti, P. Shah, R. Nagraj, and R. Pendse, "Security in multi-tenancy cloud," In *IEEE International Carnahan*

Conference on Security Technology, Washington DC, 2010.

[26] Symantec White Paper, *Web Based Attacks,* Symantec, 2009.

[27] P. P. Ramgonda, and R. R. Mudholkar, "Cloud market cogitation and techniques to averting SQL injection for univers," *International Journal of Computer Technology and Applications,* vol. 3, no. 3, pp. 1217-1224, 2012.

[28] M. McIntosh, and P. Austel, "XML signature element wrapping attacks and countermeasures," In *Workshop on Secure Web Services*, New York, 2005.

[29] A. Ahmad, "Type of security threats and it's prevention," *Int. J. Computer Technology and Applications,* vol. 3, no. 2, pp. 750-752, 2012.

[30] N. Reeshil, "Different types of network attacks and security threats and counter measures," Hub Pages, 08 02 2013. [Online]. Available at http://hubpages.com/technology/Types-of-Network-Attacks. [Accessed 03 04 2016].

[31] L. Ertaul, S. Singhal, and S. Gokay, "Security challenges in cloud computing," In *International Conference on Security and Management, SAM'10*, Las Vegas, USA, 2010.

[32] J. Viega, "Cloud computing and the common man," *Computer,* vol. 42, no. 8, pp. 106-108, 2009.

[33] M. Townsend, "Managing a security program in a cloud computing environment," In *Information Security Curriculum Development Conference*, New York, 2009.

[34] W. A. Jansen "Cloud hooks: Security and privacy issues in cloud computing," In *Proceedings of the 44th Hawaii International Conference on System Sciences*, Washigton, USA, 2011.

[35] "Top threats to cloud computing V1.0," *Cloud Security Alliance,* 2010.

[36] C. Babcock, "9 worst cloud security threats," *Information Week.* Available at http://www.informationweek.com/cloud/, 2013.

[37] D. Lukan, "The top cloud computing threats and vulnerabilities in an enterprise environment," *Cloud Tech.* Available at http://www.cloudcomputing-news.net/news/2014/nov/21/top-cloud-computing-threats-and-vulnerabilities-enterprise-environment/), 2014.