Challenges and risks of cloud based e-Government establishments

Abdulmonam Alahrash
Libyan Academy
lahresh@gmail.com

Ayad Ali Keshlaf
Industrial Research Center
ayadali2005@gmail.com

Abubker Abdesadiq
Faculty of Science, Computer Dept.
Elmergib University
Abubkr.abdelsadiq@elmergib.edu.ly

Abstract

Cloud computing offers new solutions for many E-government problems by bringing advantages such as availability of services, scalability, and utilizing the existing Internet infrastructure. However, invoking cloud computing comes with numerous of challenges and risks, which need to be considered and tackled. This paper tries to identify cloud based challenges and risks in the Libyan E-government projects. A list of potential Libyan cloud based E-government challenges and risks has been identified and presented in this paper.

Introduction

A great movement from traditional computing technology to Cloud Computing technology including E-Government projects is taking place all around the world nowadays. This is through the benefits and advantages provided by the cloud computing technology (e.g. availability, scalability and establishment cost). In fact, the use of the term “Cloud” was emerged in 1994 to represent the Internet [1]. In 2006 Christophe Bisciglia, a senior engineer at Google has introduced the term “Cloud Computing” [2]. This new term is about the change of delivering the information technology recourses from traditional in-house computing to a new model that provides the computing as a utility like water, electricity, gas and telephone utilities [3]. The cloud computing has emerged as a result of the evolution of a number of intersecting technologies (e.g. supercomputing, cluster computing, grid computing, web services and service-oriented, etc..) and involves different prospective (technology and business) [3] [4] [5] which, introduces a new vision of the computing utilization.

The evolution of the cloud computing based on the ultimate evolution of virtualization, multi-core chips technologies and the development of new Internet technologies, such as, the web services and service-oriented architectures which have a significant contribution to the cloud computing framework (see Figure 1) [6].

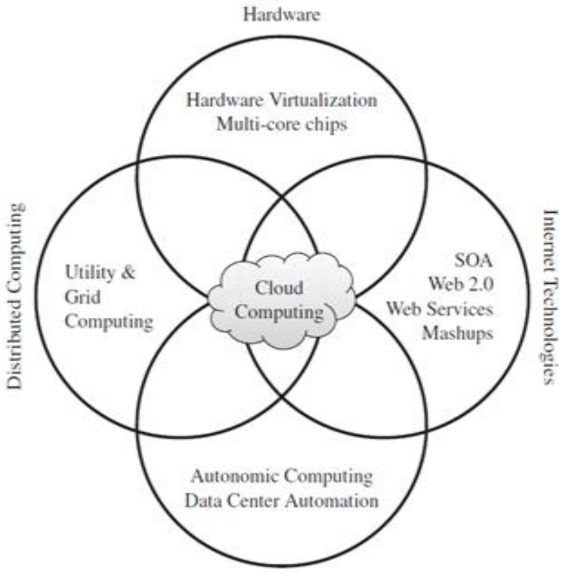

Figure 1: Convergence of various advances leading to the advent of cloud computing [6].

2. Related work

Usually, introducing and utilizing of new technologies is not free of risks. ISO 27005 defines risk as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization,”[7]. Cloud computing is not exceptional, as there are a number of new risks come with this technology. Generally, the risks associated with the cloud computing technologies are related to:

- Implementation and utilization.
- Policies that govern these technologies and its industry, and
- The security aspects.

Moreover, migration to a cloud-based solution brings some new challenges and risks which are related to security, privacy, connectivity, performance, control and dependency [4]. These risks are grouped into five main groups which are [8]: security and privacy, outsourcing risks, availability and performance, standards and legal issues, change management and organizational issues.

The top cloud computing risks as identified in [9] are: reduced governance, data location, data ownership, low visibility into virtual networks, increased attack surface, identity federation, new attack vectors, value concentration, extreme outages and reduced monitoring.

Risks in cloud environments must be considered at *service*, *data*, and *infrastructure* layers [10]. In COSO [11], external environmental factors (e.g., regulatory, economic, natural, political, social, and technological), as well as the organization’s internal factors (e.g., culture, personnel, and financial health), are considered when identifying and assessing risk events. It is important for IT leaders to identify and assess both traditional and new risk [21] and convey their assessments to their enterprise’s decision makers prior to entering into a cloud computing application [12].

3. Cloud based E-Government Risks

As part of this research the cloud computing risks are collected from many resources and categorized in an excel sheet. After deeply studying the collected data, cloud computing risks in the Libyan E-government projects could be categorized into three categories: Security Risks, Performance Risks and Managerial Risks, these categories will be described in detail in the following sections.

3.1 Security Risks

Securing data starts with ensuring that only the authenticated and authorized users have an access to the applications and related data repositories on the cloud [13]. A government, or an organization, that adopted cloud computing may be subjected to security breaches, application failures, or connection unavailability [13]. The possible security risks of governmental use of cloud computing are categorized to four categories. These categories are: access, availability, infrastructure, and integrity [14]. The top of security risks that are defined by ENISA [15] are loss of governance, lock-in, isolation failure, compliance risks, malicious insider, insecure or incomplete data deletion, data protection and management interface compromise. These risks are described as follows:

- **Loss of governance:** Cloud users relinquish control to the cloud provider on a number of issues which may affect security. This situation makes the organization dependent on the cooperation of the cloud provider to carry out activities, such as continuous monitoring and incident response. At the same time, the Services Level Agreement (SLA) may not offer a commitment to provide such services on the part of the cloud provider, thus it leaves a gap in security defenses.
- **Vendor Lock-in:** There is currently a little of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or back to in-house IT environment. This introduces a dependency on a particular cloud provider (CP) for service provision.
- **Isolation failure**: Multi-tenancy and shared resources are defining characteristics of cloud computing. A tenant may access to other tenants' virtual machines, network traffic, actual/residual data, or other resources.
- **Compliance risks:** Achieving certain certifications that comply to industry standard or regulatory requirements may be put at risk by migration to the cloud:
  - If the cloud computing provider cannot provide evidence of their own compliance with the relevant requirements (i.e. Noncompliance with regulations)
  - If the cloud computing provider does not permit audit by the cloud customer (CC).
- **Malicious insider:** Only employees with higher level of access can gain access to private data and service. In some cases where only the cloud service provider is responsible about security, the risk of insiders become massive especially with the cloud provider's inability in monitoring its employees. Besides they can cause greater damage, their impact appears on the confidentiality, integrity, and availability of all data. Insiders malicious can be current employee, a contractor, or business partner who can access the network or data for causing damage [16].
- **Insecure or incomplete data deletion:** When a request to delete a cloud resource is made an adequate data deletion may be impossible, either because extra copies of data are stored but are not available or because the disk to be destroyed also stores data from

other clients. In the case of multiple tenancies and the reuse of hardware resources, the data recovery tools cloud be used to recover deleted data.

- **Data protection**: Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer to check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way.
- **Management interface compromise:** Customer management interfaces of a public cloud provider are accessible through the Internet, and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities [15][16].

3.2 Performance Risks

In virtualization environment, multiple virtual machines can share CPUs and main memory. The performance unpredictability is caused by I/O interference between virtual machines and the scheduling of virtual machines [17]. Applications continue to become more data-intensive so data transfer rate will be increased across the cloud which produce data transfer bottleneck risks. Cloud provider overcapacity also affects the performance. If cloud provider resources capacity approaches 80% threshold and compromising some necessary services or performance, the cloud provider will most likely protect his own services and pass the degradation in service to their customers [14].

- **Performance Unpredictability:** Multiple tenants simultaneously requiring support, lower-priority organizations might not receive the required service level response from the cloud provider [11].
- **Data Transfer Bottlenecks:** Cloud computing may not be the correct selection for a cloud service consumer enterprise that located in geographical regions with underdeveloped Internet infrastructure, causing latency problems, for example (especially relevant in developing countries) [18]. Take in to account the use of sufficient Internet bandwidth before using cloud computing to prevent such risk.

3.3 Managerial Risks

The adoption of cloud computing affects internal management of the organizations i.e. management procedures, human recourses (culture, IT workforce resistance, change in administration roles) as well as affects the IT procurement procedures, converting from upfront expenditure to operational expenditure. The organization will face many risks related to IT organizational changes risk, third-party management and other risks as follows:

- **IT organizational changes:** Some IT staff who may be concerned about their job or may become redundant if cloud computing is adopted [11] [18].
- **Attenuation of Expertise:** Outsourced computing services to cloud provider can, over time, diminish the level of technical knowledge and expertise of the organization, since management and staff no longer needs to deal regularly with technical issues at a detailed level [19].
- **Unexpected costs:** Customer may get a high bill or over billed [12] because one of their websites become very popular, employees upload and store a lot of data, or attackers mount a DOS attack consuming all the resources [20]. The most reliable public CSPs are currently located in limited developed countries. Therefore, they may require payment in foreign currencies, and this will expose the cloud customer to additional foreign currency risk [18].

• **Cloud solution pricing predictability:** Many cloud providers offer a pay-as-you-go pricing model which makes calculating the cost of the cloud services appear simple. For example, can management predict whether the prices of cloud solutions will rise or fall in the future? How long will the current pricing of cloud services remain effective? Are caps on pricing increases stipulated in contracts? [11].

• **Captive renter:** In some cases, a CSP might recognize that the organization has become a captive renter once the internal technology staff has been disbanded and the CSP is solely supporting the important business processes, then annual price increases become more likely [11].

4. Conclusion and Future Work

Although, the change from traditional E-Government technologies into cloud based E-Government technologies brings many benefits, but it does not come free from challenges and risks. In this paper the risks of cloud based E-Government are reviewed and categorized into three main categories which are :

Security risks include: Loss of governance, Vendor Lock-in, Isolation failure, Isolation failure, Malicious insider, Insecure or incomplete data deletion, Data protection and Management interface compromise risk.

Performance risks include: Performance Unpredictability and Data Transfer Bottlenecks risk.

Managerial risks include: IT organizational changes, Attenuation of Expertise, Unexpected costs, Cloud solution pricing predictability and Captive renter risks.

5. References

1. Onwudebelu U. and Chukuka B., Will adoption of cloud computing put the enterprise at risk? Adaptive Science & Technology (ICAST), The 4th International Conference on, IEEE, pp 81-83, 2012.
2. Lee H. and Kim M., Implementing Cloud Computing in the Current IT Environments of Korean Government Agencies, International Journal of Software Engineering and Its Applications Vol. 7, No. 1, January, pp 149-160, 2013.
3. Buyya R, Yeo ., Venugopal S., Broberg J. and Brandic, I. “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility”. Future Generation Computer Systems 25, pp 599-616, 2009.
4. Akbari, M. Cloud Computing Adoption for SMEs: Challenges, Barriers and Outcomes (Masters Dissertation), Dublin Institute of Technology, 2013.
5. CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance Guidance Version 2.1 (2009).
6. Buyya R., Broberg J. and Goscinski A., Cloud Computing Principles and Paradigms. John Wiley & Sons. , 2011.
7. Grobauer B., Walloschek T. and Stöcker E., Understanding Cloud Computing Vulnerabilities, IEEE Cloud Computing, pp 14-20, May/June 2012.
8. Dermentzi e., Cloud computing in Egovernment, MSc dissertation, february 2013.
9. Palanisamy B. Top 10 Risks In The Cloud. March 2012, www.coalfire.com. Accessed on 29-09-2017.
10. J. O. Fit´o and J. Guitart, “Introducing Risk Management into Cloud, Computing,” Computer Architecture Department, Technical University of Catalonia, Tech, 2010.

11. C Horwath ,W Chan , E Leung , H Pili, Thought Leadership in ERM ,Enterprise Risk Management for Cloud Computing, Committee of Sponsoring Organizations of the Treadway Commission (COSO),USA, June 2012.
12. IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud ,ISBN 978-1-60420-185-7 ,United States of America.,2011.
13. K AlAjmi, Is Cloud Computing Appropriate for Government? International Conference on E-Learning, E-Business, Enterprise Information Systems,& E-Government, (pp. 169-175), April 2012.
14. Paquette S, Jaeger P T, Wilson S C. Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly; 2010;27(3):245–253.
15. Catteddu and G. Hogben, "Cloud Computing: benefits, risks and recommendations for information security,". European Network and Information Security Agency (ENISA), 2009.
16. N Ahmed, A Abraham , Modeling Security Risk Factors in a Cloud Computing Environment, Journal of Information Assurance and Security. Volume 8 (2013) pp. 279-289.
17. Armbrust, M; Fox, A; Griffith, R; Joseph, AD; Katz, RH; Konwinski, A; Lee, G; Patterson, DA;Rabkin, A; Stoica, I &Zaharia, M (2009), 'Above the Clouds: A Berkeley View of Cloud Computing'. Technical Report No. UCB/EECS-2009-28.
18. Z Enslin, Cloud computing adoption: Control objectives for information and related technology (COBIT) – mapped risks and risk mitigating controls, African Journal of Business Management Vol.6 (37), pp. 10185-10194, 19 September, 2012.
19. W. Jansen, and T. Grance, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology (NIST) Special Publication (800-144), 2011.
20. Dr. M.A.C. Dekker, DimitraLiveri, Cloud Security Guide for SMEs, Cloud computing security risks and opportunities for SMEs, ENISA, April 2015.
21. Karim Djemame et al. A Risk Assessment Framework for Cloud Computing, Cloud Computing, IEEE Transactions , July-Sept.2016.