Cloud computing risks & business adoption

Huda Qasim and Emad Abu-Shanab

International Journal of Emerging Sciences. 4.2 (June 2014): p52.

http://ijes.info/

Abstract:
Cloud computing is said to be the way forward, offering great facilitations for startup organizations with cost reduction and flexible and handy scalability. But along with these many advantages, the cloud computing environment suffers from many risks like: security, privacy, Service level agreements, and lack of standards. Many questions are raised in this regard like how serious are these threats? Should we forsake the cloud all together? Or are there ways around? This paper will explore the cloud computing environment, its architecture, nature and implementation. Also, risks associated with such environment will be explored. Finally, a proposed framework will be depicted to relate the type of business and the adoption options of diverse cloud computing environments. Finally, conclusions and future work are stated at the end.

Keywords: Cloud computing, Risks, business type, framework, typology, deployment model.

Full Text:

1 INTRODUCTION

In past, IT was considered an organizational asset; like money, time and labor. Today, things are changing. With less money, short period of time, and limited labor we can utilize an IT infrastructure through outsourcing such important asset. Businesses no longer need to acquire, and maintain an IT infrastructure. Businesses can benefit from the concept of cloud computing [1].

Technology, which was only a promising idea a few years ago, is now the fastest growing sector [2]. Cloud computing is a new paradigm that provides huge storage, and considerable reliability at an acceptable cost. It's a technology that changed a lot; starting by how software is priced, used, and produced, and how hardware is designed and utilized [3] as well as changing how business is done [4].

Adding scalability, flexibility, and connivance to organizations, Cloud computing is the commoditization of IT [1]. This new technology unarguably holds the promise of eliminating the need for expensive IT infrastructure by providing an IT architecture that is accessible online [5] with increased availability due to the high penetration of mobile technology and broadband Internet networks [6].

Despite its great potential, cloud computing faces significant issues in the business world, the mere idea of entrusting your data to another company sounds unacceptable to many [7]. It seems unrealistic to ignore the risks embedded in this approach [3]. Security challenges, and the ability to sustain an acceptable level of data integrity and privacy as data storage is outsourced, are few of many challenges that face this emerging technology [8].

Cloud computing is based on making data accessible to all authorized personnel regardless of their location via the Internet. The risks of this technology are not only the ones related to the cloud but also those that are inherited from the Internet itself. Although this technology deploys all security protocols and known measures, the central question remains: are these measures enough? Such question is important as we combine the vulnerability of the cloud with the value of our assets [5].

This conceptual paper will review the literature related to cloud computing in relation to its definition, characteristics, service models, and deployment models. The following section will go through the risks associated with cloud computing, as mentioned in literature. The following section of the paper will review some of the proposed solutions to limit the impact of these risks, and move forward with the technology. Finally, we will propose a framework that depicts the relationship between cloud computing environment and business type/sector.

2 INTRODUCTION TO CLOUD COMPUTING

Cloud computing is defined as "an information technology-based business model, provided as a service over the Internet, where both hardware and software computing services are delivered on-demand to customers in a self-service fashion, independent of device and location within high levels of quality, in a dynamically scalable, rapidly provisioned, shared and virtualized way and with minimal service provider interaction." [9, p.171]. This definition is a result of analyzing 36 definitions of cloud computing, which combines the technical aspect of the technology as well as its business prospective.

Other researchers defined cloud computing as a convenient model that allows for ubiquitous, on-demand network access to a sharable pool of computing resources (e.g., networks, servers, storage, applications, and services) that can be easily used with minimal management effort or vendors interaction [10]. It's a term used to refer to accessing resources (software applications, storage, and processing power) over the Internet, it has helped businesses to improve capabilities and add capacity without the need to install new software, train employees to use it, and worry about its maintenance [7].

The main characteristics of cloud computing are the following: Scalability of infrastructure; new capabilities can be added or dropped on need bases without the need to set up and modify infrastructure or set up new applications. Broad network access: network availability and network access, with standard mechanisms through the heterogeneous platforms (e.g., mobile phones, laptops, and PDAs). Location independence: clouds are location independent in some sense; there is practically no importance what so ever to the vendor's location. Reliability: reliability is improved with the use of redundant sites, which makes cloud computing suitable for business continuity and disaster recovery. Finally, Economies and cost effectiveness: Clouds regardless of the deployment model are much cheaper [11].

There are four service models for cloud computing [11] [12] [13] [14]:

1. Software as a Service (SaaS): which Offers application as a service on Internet, making collaborate access of software and data easier than ever, where organizations or individuals pay per use.

2. Platform as a Service (PaaS): Used by developers for developing new applications. Allow them to launching new application for minimal expenses.

3. Infrastructure as a Service (IaaS): Providers Provide the features on demand utility, organizations pay fraction of the cost on the contrary to acquiring the infrastructure, small portions of cloud are provided for free [15].

4. Desktop as a service (DaaS): Virtual Desktop Infrastructure where a third party can host desktop services, data storage, security and backup managed by service provider.

Another typology of cloud computing is distilled from the literature where four deployment models were proposed. The models depended on the status of organization and the cloud use [10] [16] [17]:

* Private cloud: The cloud infrastructure is only dedicated to a single organization use or its business units, where the cloud is not open for public use. This type of cloud may be owned by the organization itself or operated and managed by a third party.

* Community cloud: The cloud infrastructure is dedicated for the use of a specific community of consumers of a particular organization that have high security standards compliance considerations. Similar to the private cloud community, clouds can be managed and operated by the organization itself or a third party or somewhere in between.

* Public cloud: The cloud infrastructure is open for the use by the general public, business, and academic institutions. Also, organizations or governments may own, manage and operate this type of cloud, or some combination of the previous ones.

* Hybrid cloud: This cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community, or public).

3 RISKS OF CLOUD COMPUTING

This new technology has the power of changing a lot when it comes to how things are done in the business world. Along with its simplistic scalable nature, cloud computing does not eliminate the need to maintain in-house infrastructure, but it resolves all support related issues. Despite of all its advantages, cloud computing has many shortcomings that need to be taken into consideration before decision makers in an organization hasten into believing that cloud computing is the answer to all their prayers [18].

3.1 Security Risks

Ranked as number one in a survey of the most worrying threats in cloud computing [4] security threats are a major concern as we come to recognize the gap between what service providers claim and what customers want/acquire. There is continuous pressure exercised over cloud vendors to provide better protection for their clients' information assets, and on key industry players to come up with standards in this domain [19]. Surveying the literature, the following security threats are summarized [16] [20] [7] [14] [21]:

* The increased attacks: where ever businesses turn, hackers will follow. A number of threats could be faced in the cloud starting by denial of services due to DoS attacks; as experts even claim that both the risk and the expected damage are mitigated in the cloud paradigm.

* Side channel attacks: this could be done by placing a virtual machine close to the cloud to compromise the cloud, and use it to launch attacks.

* Authentication attacks: Authentication methods whether it's something you are, or something you have, or something you know, it has always been a weak point in hosted and virtual services and is usually very easy to attack .

* Man-in-the-middle cryptographic attacks: as the attacker places him/here self in the middle of two users, to intercept their communication .

* Inside-job: These types of attacks are carried out from the inside when someone who has the knowledge about the system manipulates the cloud or its content.

* Browser Security: This is an Internet inherited threat to have the credentials of the client intercepted as they connect to the browser .

* Cloud Malware Injection Attack (CMIA): the Cloud malware injection attack is when the attacker injects malicious software to the cloud to damage a spiteful service, application into the cloud.

* Flooding attacks: Attacker attacks the cloud system openly, the attacker keeps making request to the cloud, when the attacker has made so many request, he consumes the cloud resources, making it incapable of handling customer request

3.2 Legal risks

Due to the lack of uniform governmental regulation, and the absence of standard service level agreements (will be discussed later), client organizations are at high risk of not being able to protect their own resources. The number of enforcement actions challenging companies for data security practices filed at the Federal Trade Committee (FTC) has seen a dramatic rise due to the increase use of cloud computer services. This sizable adoption creates legal liabilities based mainly on security liabilities; when the vendor fails to provide adequate security for customer data/information, and making it vulnerable for hackers' attacks and damage [22].

Investigative support is another legally related issue; when illegal activities occur (even if it was internal), the investigation process is both difficult and expensive, and given the co-located data logs of multiple clients in cloud computing, the investigation becomes impossible [23] [7].

3.3 Privacy risks

Privacy issues range from the immature perception of technology to the absence of regulations in this regard. For further understanding of the issue we must first distinguish between domestic clouds and trans-border clouds, where the first operates within one jurisdiction and the later operates in several jurisdictions. Such environment adds more privacy and security risks to this technology.

In domestic clouds we are concerned whether the data is carried out and used appropriately, when and why it is accessed, how long will it be kept, and whether the owner is informed of any transactions [19]. On the other hand, in the transborder cloud, we worry about the cloud operator, its location, and any third party using it. Bearing in mind that what applies in one jurisdiction may not apply in the other. Other privacy issues include:

1. Access control: the fact that the data/applications of the organization are controlled by the vendor means that the vendors' personnel will have access to it [2].

2. Internal segmentation: the vendor's cloud is not dedicated to one organization, if not properly structured; there will be risks of data disclosure by other organizations with which the client organization shares the cloud. A comprehensive review of the privacy risk associated with data disclosure is discussed in the work of [24].

3. Data ownership: quite frequently the cloud vendor claims ownership of the data, and the right to disseminate and reuse it as well [25].

4. Subcontractors: it's not unusual to find out that your cloud vendor is actually another cloud vendor customer; this multilayer service provider's model complicates privacy even further, and who's legally responsible for privacy, security and compliance [26].

3.4 Service issues and risks

Service degradation and maturity: not all vendors are able to provide 24/7 support, any outage could result in great losses especially for businesses. The reliability of the cloud is one of the major concerns, and is a priority (Dhar, 2012). All services provided via the cloud involve Internet connection, which can suffer from congestion and outage (Mosher, 2011).

Service level agreement and lack of standards: The deficiency in standards concerning the control and communication for application in the vendors cloud is a major concern in the IT industry now [27]. There is a clear need to provide a new SLA methodology in the context of cloud computing [28].

The need for a new methodology stems from the fact that there are several attributes of the dynamic cloud architecture that must be considered in a comprehensive model of cloud computing SLA. Task related attributes that were handled internally (inside the

organization) prior to the cloud era, are now being handled by a vendor, they must be taken into account as the agreement between the consumer and the vendor is set. The tasks range from authentication and identity verification to encryption, backup and disasters recovery, as well as financial penalties in cases of poor performance [29].

3.5 Espionage Risk

Spying is one of the major concerns when it comes to cloud use; in April 2010 Google released a report, where it claims that many governments around the world have requested the privilege of accessing private information and censoring applications. The truth is that governmental overreach of private information is not a new threat, but it was augmented by cloud computing [30].

4 CLOUD COMPUTING AND BUSINESS

All the risks mentioned above where not enough to drive businesses away from the cloud concept. Clearly most of the organizations operating in cloud era look at this technology as an opportunity that needs not to be wasted. According to the CompTIA 4th Annual Research Report 2013, 90% of companies use some form of cloud computing.

Since forsaking the cloud to avoid its risks sounds out of question, then it's reasonable to look for ways to minimize the risks as we move forward. The bottom line is that many applications are general purpose ones, therefore, economically it makes much sense to try to find a provider for these applications [31].

Cloud computing is diffusing its way into the business world. As businesses are looking forward to bypassing the need to pay for expensive infrastructure, the perceived ease of use and connivance, as well as a common believe that cloud security and privacy are improving, are the main drivers for cloud adoption [6]. The previously mentioned report [32] proclaimed that the most important benefits that adopters have experienced as they used the cloud are the following (we report here the top five with their corresponding percentage of importance by reported by respondents): Ability to cut cost (43%), Better option for multiple reasons (42%), modernization of legacy IT (40%), reduce capital expenditure (38%), and add new capabilities of features (38%).

4.1 Risk mitigation options

Making the decision: Before an organization makes a decision as critical as moving to the cloud, the management is responsible for setting out the strategy and defining the organization's critical functions. To help decide whether cloud computing is a viable option or not, some organizations will find that cloud computing is not an option due to the sensitivity of their operation. Others might see some room for the adoption of this technology; these organizations have to assess their options in terms of service model, deployment model and service provider. They also need to have a realistic assessment of the associated risks [23].

Risk management is deemed vital in these situations; it's part of the activities that the organization needs to perform if it chooses to deploy this technology. It's a generic process with well-known guideline that organizations perform to treat risks embedded in their activities and to try to obtain and sustain their benefits [3]. Once the organization's managers give the green light for such deployment, a cloud usage policy must be created. The policy provides a clear view of what activities can be outsourced to the cloud vendor, and the risk management activities needed. Practically there are four ways to deal with cloud computing risks:

1. Risk avoidance: The organization may choose to forsake the cloud technology altogether, or implement a private cloud deployment model.

2. Risk reduction: The organization may try to reduce the risk associated with the technology either by reducing its likelihood, impact, or both.

3. Sharing: The organization may choose to share the risk of the technology by assuring its data or applications.

4. Acceptance: In some cases organizations, accept the risk and move along especially if they cannot work their ways around it [33].

Risk monitoring: regardless of how the organization have chosen to deal with the risk, it's important to monitor the situation, and to assess the impact of risk awareness or the actions taken, if new risks have emerged or the existing ones have changed [3].

4.2 Choosing the Deployment Model

As discussed previously, and due to many security and privacy challenges, there isn't a one unique solution for cloud use. Financial organizations would mostly use a private cloud to store their critical information, data or applications. On the other hand, organizations with high transactions and less sensitive, less valuable data, use public clouds for their data [30]. The choice is not only based on the sensitivity of the client organization data and activities, but the characteristics of each deployment model needs to be considered as well. It should be known that public clouds are highly structured and automated with little room for SLA negotiations. On the other hand, public clouds have security standards that are acceptable to many but of course aren't acceptable to all. Economy wise the public cloud is more feasible because the organization only pays for what it uses [34].

One of the solutions to deal with the low security in clouds is the adoption of an integrated security dynamic model, which differs from one transaction to another. Subashini & Kavitha suggested a framework that relates the type of cloud (public, private/community or hybrid) to the infrastructure issues (management, ownership, location, and access/consumption) [5]. The framework proposed infers that data should be stored and accessed based on metadata, which will make the data valueless for any intruder. After all, an organization must categorize its data based on its value and vulnerability to exposure, and then build its own integrated customized security measures. While the common security measures may be sufficient for some types of data, others require different measures [35].

Finally, organizations may try to take the best of both words; the privacy and data control of the private cloud and the economy of the public cloud [34]. All they do is to classify the data to understand the level of its sensitivity. As organizations cannot control the data once in the cloud, they can control what data to but on the cloud; these organizations are recommended to use the hybrid model [33].

4.3 Negotiating a service level agreement

After the vendor has been chosen, the client organization needs to negotiate a service level agreement with the vendor. A good contract needs to specify the location of data storage, and jurisdiction on the cloud storage. Because of the lack of universal standards, policies, and security regulation, the organization needs to be aware that different jurisdictions have different levels of privacy and security regulations in terms of their strength, based on which organization decision should be made [30].

Availability is one of the most important things to be included in the service level agreement with penalty clues if the agreed upon level of availability was not met [23]. Some kind of insurance policy, that bounds the vendor for the expenses of data recovery incurred from failure, needs to be created [36]. The client organization has to limit the access of the data stored on the cloud to a small number of oversight privileged administrative team, with a long term commitment with the client organization. Organizations need also to make sure that the data will be stored in an encrypted form, ask who implemented the encryption, and who has access to the key [23].

The SLA need to specify where the backup data is it be stored, its maintenance (Turner, 2013), the service provider should insure recovery in cases of total disasters, even if the organization cannot know where will the backup data be stored, they should be assured of complete restoration, and must be informed of how long it would take [23]. The service level agreement should include conditions about the vendors' internal auditing process, and what are his standards [37], the service provider should also agree to a third party periodic auditing [23].

5 A PROPOSED FRAMEWORK

This work tried to explore the environment of cloud computing, its risks and some solutions proposed in the literature. The option of adopting cloud computing is not an easy one, it involves huge risks, but still provides substantial benefits and synergies. Based on

the previous review of business environment, we concluded to the following framework shown in Figure 1.

The proposed framework relates the type of business (institution) to the cloud computing deployment model: the framework, Cloud Computing Business-Deployment Fit Model.

Based on the reviewed literature, it's safe to conclude that governmental institutions (with greater concerns as to where the service provider's jurisdiction) are most likely to create their own private cloud. Such option allows for better control, better security, and more reliance. An example case is the government of Japan which announced that by the year 2015 the country will have a private cloud that consolidates all governments IT systems, for better efficiency and less cost [38].

As for financial institutions, the idea of cloud computing seems to defy the principles on which these institutions where founded. Due to the flexibility, high scalability and the low cost made possible by the cloud technology, banks and other financial institutions are easing their way to a new era of business. They are very much like governmental institutions and pretty much for the same reasons; financial institutions are most likely to adopt single tenant private cloud deployment model [39]. For better exploitation of this technology, both governmental and financial institutions may use public clouds for non-core activities in a hybrid cloud deployment model [38] [39].

While public clouds are less demanding in terms of cost (with using the pay as you go payment model), the freedom of service for businesses, and the management services offered by the service providers, make public clouds well suited for small and medium size businesses [40].

6 CONCLUSION AND FUTURE WORK

Cloud computing is a relatively new technology that provides many benefits to businesses across the world. There are many issues that this technology presents, security and the elevated chances of attacks, privacy concerns as to who has access to the client organizations data or applications, who owns them and who has control over them, the lack of standards and legislations, the difficulties of negotiating a service level agreement, are all among the most pressing issues of this technology.

Despite of the significant risks associated with cloud computing, business adoption of this technology is exponentially escalating. Proving in a way that the advantages clouds provide are of great importance and outweigh the risks. By attentive management, organizations can limit the impact of cloud computing risks, assessing the risks associated with the technology, making an educated choice of deployment model, and negotiating service level agreement, are all important steps to reduce the risks of cloud computing.

This paper proposed an initial framework (Cloud Computing Business-Deployment Fit Model) that relates the institution type to the cloud computing deployment model. The model is a proposition for researchers to build on and expand to understand better the needs of organizations and the proper application of cloud computing.

Evidently, standards and best practices regarding cloud computing is an under researched topic that needs further investigation. These standards and best practices should enlighten businesses of how to make the best of cloud computing, without exposing their organizations to potentially destructive risks. Future research need to balance the choice between control and cost, between security and convenience, and between privacy and expansion.

Finally, there is a pressing need to present a comprehensive model that combines the adoption of cloud computing as well as the risk mitigation methodology that needs to be implemented; this model should serve as a guide to organizations especially small size and medium size organizations in the deployment of the cloud computing technology.

7 REFERENCES

[1] Rabai, L., Jouini, M., Aissa, A., & Mili, A. "A cybersecurity model in cloud computing environments". Computer and Information Sciences, 2013, 25, 63-75.

[2] Sabahi, F. "Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges". International Journal on Advances in ICT for Emerging Regions, 2011, 4 (2), 12-23.

[3] Fito, O. & Guitart, J. "Business-driven Management of Infrastructure-level Risks in Cloud Providers". Future Generation Computer Systems, 2013, 32, 41-53 (2014).

[4] Nicho, M., & Hendy, M. "Dimensions Of Security Threats In Cloud Computing: A Case Study". Review of Business Information Systems, 2013, 17 (4), 160-170.

[5] Subashini, N., & Kavitha, V. "A survey on security issues in service delivery models of cloud computing". Journal of Network and Computer Applications, 2011, 34, 1-11.

[6] Gupta, P., Seetharaman, A., & Raj, J. R. "The usage and adoption of cloud computing by small and medium businesses". International Journal of Information Management, 2013, 33 (4), 861- 874.

[7] Kuyoro, O., Ibikunle, F., & Awodel, O. "Cloud Computing Security Issues and Challenges". International Journal of Computer Networks (IJCN), 2011, 3 (5), 247-255.

[8] Mishra, B., & Mishra, V. "Implement Cloud Computing Model For Business Information System Security". International Journal of Current Research, 2012, 4 (11), 121-125.

[9] Madhavaiah, C., Bashir, I., & Shafi, S. "Defining Cloud Computing in Business". The Journal of Business Perspective, 2012, 16 (3), 163-173.

[10] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. Retrieved December 5, 2013, from Computer Security Division. U.S. Department of Commerce: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[11] Zissis, D., & Lekkas, D. "Addressing cloud computing security issues". Future Generation Computer Systems, 2012 28, 583-592.

[12] Kumar, A. "World of Cloud Computing & Security". International Journal of Cloud Computing and Services Science, 2012, 1 (2), 53-58.

[13] Madhavi, K. V., Tamilkodi, R., & Sudha, K. J. "Cloud Computing: Security threats and Counter Measures". International Journal of Research in Computer and Communication technology, IJRCCT, 2012, 1(4), pp. 125-128.

[14] Kumar, S., & Goudar, R. H. "Cloud Computing--Research Issues, Challenges, Architecture, Platforms and Applications: A Survey". International Journal of Future Computer and Communication, 2012, Vol. 1(4), pp. 356-360.

[15] Sharon, Y. "Move into the Cloud, shall we?" Library Hi Tech News, 2012, 29 (1), 4 7.

[16] Qaisar, S., & Khawaja, "Cloud Computing: Network/Security Threats and Counter Measures". Interdisciplinary Journal of Contemporary Research in Business, 2012, 9 (3), 1323-1329.

[17] Sharma, M., Bansal, H., & Sharma, A. K. "Cloud Computing: Different Approach & Security Challenge". International Journal of Soft Computing and Engineering (IJSCE), 2012, Vol. 2(1), pp. 421-424 .

[18] Hosseini, A. K., Greenwood, D., & Sommerville, I. "Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS".

IEEE 3rd International Conference on Cloud Computing, 2010, 3, pp. 450-457. Miami, FL.

[19] Svantesson, D., & Clarke, R. "Privacy and consumer risks in cloud computing." Computer law& security review, 2010, 26, 391-397.

[20] SeungHwan, J., Gelogo, Y., & Park, B. "Next Generation Cloud Computing Issues and Solutions". International Journal of Control and Automation, 2012, 5 (1), 63-70.

[21] Parekh, D. H., & Sridaran, R. "An Analysis of Security Challenges in Cloud Computing." (IJACSA) International Journal of Advanced Computer Science and Applications, 2013, Vol. 4(1), pp. 38-46.

[22] Wittow, M., & Buller, D. "Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime". Journal of internet law, 2010, 14 (1), 5-15.

[23] Heiser, J., & Nicolett, M. (2008). Assessing the Security Risks of Cloud Computing. Retrieved December 10.2013, from Gartner group: https://www.gartner.com/doc/685308

[24] Sinjilawi, Y., AL-Nabhan, M. & Abu-Shanab, E. "Addressing Security and Privacy Issues in Cloud Computing". Journal of Emerging Technologies in Web Intelligence, Vol. 6(2), May 2014, pp. 192-199

[25] Katzan, H. "On The Privacy of Cloud Computing". International Journal of Management & Information Systems, 2010, 14 (2), 1-12.

[26] Mosher, R. "Cloud Computing Risks". Information Systems Security Association ISSA Journal, 2011, 4 (1), 34-38.

[27] Dhar, S. "From outsourcing to Cloud computing: evolution of IT services". Management Research Review, 2012, 35 (8), 664-675.

[28] Pankesh, P., Ajith, R., & Amit, S. (2009). Service Level Agreement in Cloud Computing. Computing Cloud Workshops. A publication of Wright State University, Accessed from the Internet in 2013 from: http://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=1077&context=knoe sis

[29] Cochran, M., & Witman, P. "Governance And Service Level Agreemnet Issues In A Cloud Computing Environment". Journal of Information Technology Management, 2011, 22 (2), 41-55.

[30] Kshetri, N. "Privacy and security issues in cloud computing: The role of institutions and institutional evolution". Telecommunications Policy, 2013, 37, 372-386.

[31] Marston, S., Zhi, L., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. "Cloud computing: the business perspective". Decision Support Systems, 2011, 51 (3), 176-189.

[32] CompTIA 4th Annual Research Report. "Retrieved December 7, 2013, from Cloud Computing Trends 2013": Accessed from the Internet from http://clikcloud.com/ccone/cloud-computing-trends-2013-comptia-4th-annualresearch-report/#respond

[33] Warren, C., Eugene, L., & Heidi, P. (2012). Enterprise Risk Management for Cloud Computing. Retrieved December 2, 2013, from The Committee of Sponsoring Organizations of the Treadway Commission: http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf.

[34] Claybrook, b. (2011). Differences explained: Private vs. public vs. hybrid cloud computing. Retrieved November 24, 2013, From Search Cloud Computing.com EGuide:http://docs.media.bitpipe.com/io 10x/io_100433/item_419065/HPIntel sCloud Computing_SO%23034437_E-Guide_052611.pdf.

[35] Bhadauria, R., & Sanyal, S. "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques". International Journal of Computer Applications, 2012, Vol. 47(18), pp. 47-66.

[36] Turner, S. "Benefits and risks of cloud computing". Journal of Technology Research, 2013, 4 (1), 1-7.

[37] Gatewood, B. (2009). Cloud Computing Information Horizon: How to Avoid the Storm. Retrieved November 11, 2013, from Information Management:http://content.arma.org/IMM/Libraries/JulyAug_2009_PDFs/IMM_0709_clouds_on_info_horizon.sflb.ashx

[38] Craig, R., Frazier, J., Jacknis, N., Murphy, S., Purcell, C., Spencer, P., et al. "Cloud Computing in the Public SectonPublic Manager's Guide to Evaluating and Adopting Cloud Computing". Cisco Internet Business Solutions Group (IBSG), San Jose, CA, USA, 2009.

[39] Fratilab, L., Zotaa, R., & Constantinescua, R. "An Analysis of the Romanian Internet Banking Market from the Perspective of Cloud Computing Services". Procedia Economics and Finance, 2013, 6, 770-775.

[40] Parsi, K., & Laharika, M. (2013). A Comparative Study of Different Deployment Models in a Cloud. International Journal of Advanced Research in Computer Science and Software Engineering, 3 (5), 512-515.

Huda Qasim (1) & Emad Abu-Shanab (2)

(1,2) MIS Department, IT College, Yarmouk University, Irbid, Jordan

(1) hudaqassem123@gmail.com & (2) abushanab@yu.edu.jo

Figure 1: Cloud Computing Business-Deployment Fit Model (Proposed by the authors) Type of Institution Cloud Computing Deployment Model Private Hybrid Public Governmental Institutions [check] [check] [x] Financial Institutions [check] [check] [x] Small/Medium-Size Businesses [x] [check] [check]

Qasim, Huda^Abu-Shanab, Emad

Source Citation (MLA 7th Edition)
Qasim, Huda, and Emad Abu-Shanab. "Cloud computing risks & business adoption." *International Journal of Emerging Sciences* 4.2 (2014): 52+. *Academic OneFile*. Web. 24 Mar. 2016.

URL
https://proxy.library.carleton.ca/login?url=http://go.galegroup.com/ps/i.do?id=GALE%7CA379200284&v=2.1&u=ocul_carleton&it=r&p=AONE&sw=w&asid=08765ce60c8959716ca92b24898c4cf4

Gale Document Number: GALE|A379200284