Security Risk factors that influence Cloud Computing Adoption in Saudi Arabia Government Agencies

Madini O. Alassafi, Abdulrahman Alharthi, Robert J Walters and Gary B Wills
School of Electronics and Computer Science
University of Southampton
Southampton, United Kingdom
{moa2g15, aaa2g14, rjw1, gbw}@soton.ac.uk

Abstract— **Cloud computing technologies play a substantial role in public organizations and private sector companies since it reduces the cost of using information technology services and allows users to access the service anytime and everywhere, whilst only paying for what they use. In developing countries, such as Saudi Arabia, the cloud computing is still not widely adopted, compared to countries in the west. In order to promote the adoption of cloud computing, it is important to recognize that an important and specific issue related to cloud computing is the potential and perceived security risks posed by implementing such technology. Therefore, the aim of this research is to investigate the security risk factors that influence organization to adopt cloud computing in a Saudi Arabia context. This research proposed a framework for the successful adoption of cloud computing, focused on risks when implementing security in the cloud system.**

Keywords- cloud computing; cloud adoption; cloud security risks; security benefits.

I. INTRODUCTION

Cloud computing is a term used to define distributed computing associated through a network to afford utility services to the end user [1]. The cloud allows users to access the service anytime and everywhere, and only pay for what they use. Cloud computing is a way of delivering computing resources based on different technologies such as cluster computing, distributed systems and web based services. It has become an attractive opportunity for enterprises as it meets their IT demand and their infrastructure.

On other hand, there are also disadvantages to using cloud computing that must be considered. The risks of adopting cloud computing have been categorized into different levels such as cost, security, governance, legal–compliance and performance concerns [2]. In the cloud, the customer may not have the kind of control over their data or the performance of the applications that they have with traditional Information and communication technologies (ICT) or the ability to audit or change the processes and policies under which users must work.

The security of the cloud, and associated privacy concerns, give many organizations pause as they think through their particular cloud computing concerns. Security concerns including physical security and simple access to facilities and equipment, as well as logical security, industry compliance requirements, auditability, and more [3]. Although the adoption of cloud computing services can provide many advantages for the government agencies, few European countries have developed governmental cloud strategy plans [4]. Furthermore, the security risks have potential influence on the acceptance of cloud computing in most of the world. One of the main problems notable by big government organizations is the amount of spent on the IT infrastructure. For example, "*the Saudi Arabia government agencies spent around 4 million GBP in 2010 and it is predicted that the total spending for the year subsequent might have increased by 10.2% compared to 2010*" [5]. This indicate that in Saudi Arabia, there is negative potential attitude toward adopting and implementing advanced technologies. Some studies have been conducted in investigate the influence of the social and management aspects that facilitate or pose challenge on the cloud adoption in Saudi Arabia [5].

As result of the literature, there is inadequate efforts to know the factors that influence acceptance or rejection of cloud computing services due to security risks [4]. According to ICorps Technologies, by 2020 it is expected that the cloud computing market will exceed $270 billion. This forecast implies that the cloud computing industry is on the rise and the number of cloud users around the world is increasing. The increase in use of cloud computing technology is due to its low initial investment, lower maintenance cost and very high computations power [6].

As cloud computing providers have several security controls that overcome the ability of any government or private organization, there is a low marker of using cloud in Saudi Arabia due to the security risks [7]. In order to understand the security risks associated with cloud computing adoption, this study will investigate the Saudi government agencies attitude toward security risk cloud in adoption investigating the perceived influence of cloud computing security benefits and how these security risks and benefits can affect the decision making process toward cloud adoption.

II. LITERATURE REIVEW

A. Overview of Cloud Computing Adoption

Every organization has some ideas, which are to be streamlined to achieve big profits. To implement these ideas, every organization can benefit from Information & Technology (IT) at every stage. Therefore, there is need to develop IT applications for specific use. Developing an IT application, require data centers with servers and storage devices, uninterrupted power supply, cooling systems, complicated software and experts to run those systems [8]. The process of developing an IT application involves development, staging and production environment. When we develop many applications for an organization, the investment cost will be very high. Apart from the infrastructure, the organization need the software's to be updated all the time [9].

Governments around the world are dynamically into cloud computing as a wealth of growing efficiency and reducing cost [10]. Cloud adoption in general is a considered move by organizations to reducing cost, mitigating risk and realizing scalability of data base capabilities. The growth in computing lies in Cloud Computing technology, where the main objectives is reducing IT costs while increasing productivity, availability, reliability and flexibility and reducing the response times [5]

The report of National Institute of Standards and Technology (NIST) titled "The NIST Definition of Cloud Computing" provides the following definition for cloud computing: " *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction*" [11].

B. *Cloud Adoption Benefits*

The most significant benefits of cloud adoption are (Pay as you go pricing model, Scalability, Availability, Low maintenance and Easy implementation). Moreover, the cloud adoption has many benefits for organizations and the one of the most benefit is that, the cloud be able to decrease costs and saving money for the companies and small or large enterprises due to the cloud adoption is offering an outsourcing model that lets them to get resources and pay as they use of services. For example, the money that company spends on to run their system, instead of building up in-house IT infrastructure as a principle expenditure. Furthermore, the maintenance of IT resources and the upgrades are achieved by a third party, which endorse organizations to allocation responsibility and saving money [12].

III. THE PROPOSED FRAMEWORK

The proposed framework is intended to investigate the security risk factors that influence the adoption of cloud computing in Saudi Arabian context. This framework proposed the successful adoption of cloud computing focused on risks when implementing security in the cloud system. The proposed framework is consists of three categories:

- The first is Social Factors category, which has three components: trust, privacy and security culture.
- The second is Cloud Security Risks category, which comprises of cloud technology security risks such as malicious insider, insecure interfaces and shared technology.
- The third category is Perceived Cloud Security Benefits that includes well-known cloud security features such as smart scalable security mechanism, centralized auditing, and standardized security policies interfaces.

The framework factors were identified by critically reviewing studies found in the literature together, with factors from the industrial standards within the context of Saudi Arabia. The framework's categories and factors are illustrated in Fig. 1.

A. *Perceived Cloud Security Risk Factors*

The perceived cloud security risk factors describes cloud security risk factors, which are related to the nature of the cloud security and set of known security risks that highlighted by the security organization industries and research studies of the cloud technology and identifies the factors that affect an organization's decision to adopt this technology.

- **Insecure interfaces and application programing interfaces:** consumers manage and react with cloud services out of interfaces and APIs. Providers have to guarantee that security is inserted and considered at their service models. However, the users should understand and be aware of security risks in the use [13].
- **Share technology risk:** infrastructure as a service is constructed on shared infrastructure that is frequently not considered to accommodate a multi-tenant architecture such as CPU caches and GPUs.
- **Account or service hijacking**: according to CSA, the service traffic hijacking was recognized as the third highest cloud computing security risk. It is regularly with stolen identifications and it considered the strong two factors authentication techniques [14].
- **Malicious insiders:** a risk to an organization, because it is a current or previous operate provider, or other one who had authorized access to an organization's system or have access to potential sensitive data. However, it is important for the government organizations to understand what providers are doing to identify and protect beside the malicious insider risk [13].
- **Compliance with regulations** according to Gartner compliance with regulation is one of the important risk factors that the government should be aware of it before adopting the cloud even when it is held through a service provider. Compliance with regulation is an effective factor that can make a secure reluctant transferring to the cloud computing. This risk derives from the fact, which there are no governmental regulations or directions that can support the firm in the event of a data breach. The lack of IT standards is a big problematic may hinder the adoption decisions of cloud computing [15].

- **Data ownership (governance) and accountability**: this factor is critical security risk that the government organization requirements to be carefully think through and qualify since the organization logically and actually defends the data it owns [16].

- **Service data integration/protection:** every organization must be sure for their own data is protected since it is moving between the end user and the cloud data center. However, the risk is bigger for organizations which using a cloud computing model because unsecured data is more liable to interception when it transmission [17].

- **Data leakage**: according to CPNI, it is weakness of security access rights to more than domains and weakness of physical transport system for cloud data and backups.

B. Social Factors

Social factors are related to the Saudi organization security behavior and attitude toward the usage of cloud computing in term of security in cloud adoption perspective.

- **Trust:** mentions to support on another entity, the belief that this entity will function as expected Trust in the cloud computing with difficulty consists on trusting the service itself and the provider to supply a trusted level of authentication, confidentiality, and integrity related to the service and stored the data [3].

- **Security culture:** security culture can support most of organizational effectiveness in a way that information security can be normal part in daily activities of all employee. Security cultures help the execution of information security policies and work out to the organization. Security culture covers social, cultural, and ethical scale to develop the security pertinent behavior of the organizational organs and keep it to be a subculture of organizational culture [18].

- **Privacy:** confidentiality of data that give access to only licensed users. Privacy considered the major concern to any organization that willing cloud computing because really cannot have completely control to the information that stored on cloud-based servers [19].

C. Perceived Security Benefits

This category comprises of the perceived cloud computing security features that affect cloud adoption decision making in the organizations which highlighted by organization industries and research studies. According to European Network and Information Security Agency (ENISA), the cloud security features [20] are further elaborated below:

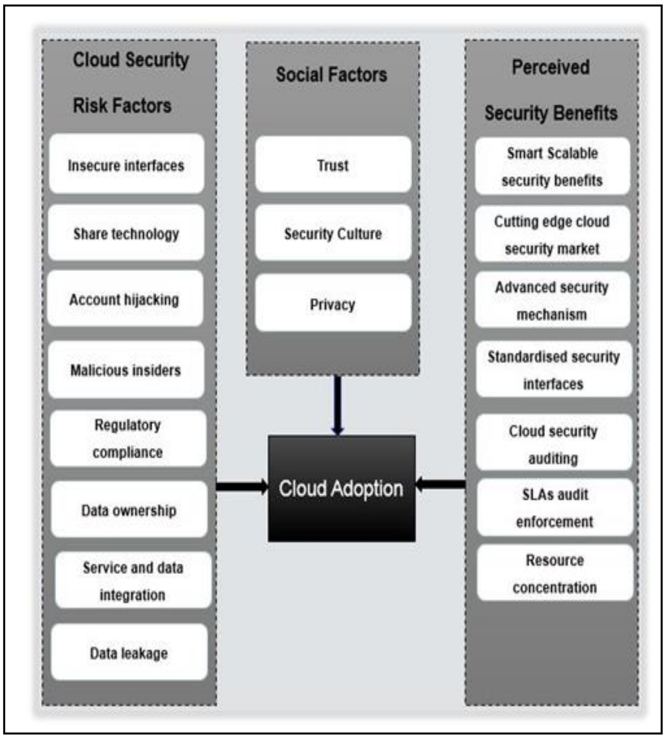

Figure 1. Cloud computing adoption Framework

- **Smart scalable security benefits:** this is defined as the ability to extend the security features to multiple locations, edges networks, timeless of response and threat management. The list of cloud resources that can be rapidly scaled on demand already includes, e.g., storage, CPU time, memory, web service requests and virtual machine instances, and the level of granular control over resource consumption is increasing as technologies mature.

- **Cutting edge cloud security market:** Cloud providers such as Amazon, Google are considered the two largest hardware and software provider in the world. Therefore, the cloud costumer can benefit up to date high standard security techniques in order to secure their assets.

- **Advanced security mechanism:** cloud provider can provide centralized security as service patches and updates for the customer, which is more efficient than traditional organization security capability.

- **Standardized security interfaces:** security management free interfaces can ease the consumer ability to change from provider to other providers in a short period and reduced cost.

- **Cloud security auditing:** auditing in the cloud can be better organized, via pay as you go for auditing and gathering audit log requirements.

- **Service level agreement (SLAs) audit enforcement:** cloud customer can benefit set of audit manage requirements and the provider should comply with those audit demands stated in the service level agreements (SLAs).

- **Resource concentration:** pool of security resources can be harnessed by costumers including access control, comprehensive security policy, patch and data management and maintenance processes.

IV. CONCLUSION

Cloud computing is the developing paradigm of distributing IT services to consumers as a utility service over the Internet. The great benefit of cloud computing is that the cloud offers resources to multiple users at any time in a dynamic way and according to users' needs. In addition, users only pay for the services that they need. However, regardless of the fact that the cloud offers some benefits for enterprises from flexibility to decreasing cost, moving an existing system to the cloud is not an easy task for the reason that there are a number of variant challenges in different domains such as legislations, technology, and management challenges. One of the most noticed challenge that face any government agency is cloud security risks.

To investigate the latter issue of cloud security risks, the study is to focus on the security risk factors that affect government agencies decision to adopt the cloud. This study is aimed to construct a framework to investigate the cloud security risks and the cloud security features that influence Cloud Computing adoption in Saudi Arabia. This is an ongoing research and future work will be focused on reviewing then validating the proposed framework.

REFERENCES

[1] R. Buyya, R. Buyya, C. S. Yeo, C. S. Yeo, S. Venugopal, S. Venugopal, J. Broberg, J. Broberg, I. Brandic, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Futur. Gener. Comput. Syst.*, vol. 25, no. JUNE, p. 17, 2009.

[2] P. Bannerman, "Cloud computing adoption risks: state of play," *Governance*, vol. 3, no. September, pp. 0–2, 2010.

[3] S. Pearson, "Privacy, Security and Trust in Cloud Computing," *Priv. Secur. Cloud Comput.*, pp. 3–42, 2013.

[4] G. Elena and C. W. Johnson, "F ACTORS INFLUENCING RISK ACCEPTANCE OF C LOUD COMPUTING SERVICES IN THE UK," vol. 5, no. 2, 2015.

[5] M. Alsanea and J. Barth, "Factors Affecting the Adoption of Cloud Computing in the Government Sector : A Case Study of Saudi Arabia," 2014.

[6] K. Kumar, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?," *Computer (Long. Beach. Calif).*, vol. 43, no. 4, pp. 51–56, 2010.

[7] F. Alharbi, A. Atkins, and C. Stanier, "Strategic Framework for Cloud Computing Decision-Making in Healthcare Sector in Saudi Arabia," *Seventh Int. Conf. eHealth, Telemedicine, Soc. Med.*, vol. 1, no. c, pp. 138–144, 2015.

[8] C. Loken, D. Gruner, L. Groer, R. Peltier, N. Bunn, M. Craig, T. Henriques, J. Dempsey, C.-H. Yu, J. Chen, L. J. Dursi, J. Chong, S. Northrup, J. Pinto, N. Knecht, and R. Van Zon, "SciNet: Lessons Learned from Building a Power-efficient Top-20 System and Data Centre," *J. Phys. Conf. Ser.*, vol. 256, no. 1, p. 012026, 2010.

[9] M. Miller, "Cloud Computing : Web-Based Applications That Change the Way You Work and Collaborate Online," *Que Publ.*, pp. 1–29, 2009.

[10] L. Badger, D. Bernstein, R. Bohn, F. De Vaulx, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, "US Government Cloud Computing Technology Roadmap Volume II Release 1 . 0 (Draft) Useful Information for Cloud Adopters," *Nist Spec. Publ.*, vol. II, p. 85, 2011.

[11] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Natl. Inst. Stand. Technol. Inf. Technol. Lab.*, vol. 145, p. 7, 2011.

[12] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.

[13] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," *Security*, no. February, pp. 1–14, 2013.

[14] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," *Security*, no. February, pp. 1–14, 2013.

[15] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing — The business perspective," *Decis. Support Syst.*, vol. 51, no. 1, pp. 176–189, 2011.

[16] P. S. Wooley, "Identifying Cloud Computing Security Risks," *Contin. Educ.*, vol. 1277, no. February, 2011.

[17] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Gov. Inf. Q.*, vol. 27, no. 3, pp. 245–253, Jul. 2010.

[18] M. Alnatheer and K. Nelson, "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," *Proc. 7th Aust. Inf. Secur. Manag. Conf. December 2009*, no. December, pp. 6–17, 2009.

[19] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," *2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci.*, pp. 693–702, 2010.

[20] Enisa, "Cloud Computing: Benefits, risks and recommendation for information security," no. December, 2009.