(IJRST) 2017, Vol. No. 7, Issue No. I, Jan-Mar e-ISSN: 2249-0604, p-ISSN: 2454-180X

RELATIONSHIP AND CLOUD FACTORS AFFECTING GOVERNMENT CONFIDENCE IN THE PUBLIC CLOUD

***Waleed Alghanim, **Dr. Feng Chen**

**PhD candidate, School of Computer Science and Informatics, De Montfort University, UK*

***Senior Lecturer, Software Technology Research Laboratory, De Montfort University, UK*

ABSTRACT

Despite the advances in public cloud and the associated advantages governments are still reluctant to deploy sensitive data and critical systems into the public cloud. The advantages of scalability and cost are attractive for governments and the current direction for governments is to place more of their data and systems in the public cloud towards a more comprehensive government cloud solution. However, there are major concerns related to the public cloud that are especially significant to governments which include governance over data and systems, compliance and security and privacy. If these concerns are answered governments will perceive less risk and be more confident to deploy to the public cloud. Beside the technical solution of improving security, one of the solutions to this concern is an effective relationship between government and cloud service provider. This study investigates the relationship factors between government and cloud service provider and the associated cloud factor concerns to find out how they affect confidence in the public cloud, towards providing further insight into government reluctance to place sensitive data and critical systems in the public cloud. The research framework identifies the relationship factors which include risk, trust, collaboration, negotiation and reputation and identifies which cloud related factors, which include governance, compliance, security and privacy and performance and offering, are affected by these relationship factors. The study builds on previous studies that address relationship factors or cloud factors in isolation where this study considers them together as factors for the willingness to adopt the public cloud. This is achieved through a questionnaire with government officials involved in cloud adoption policy. The results reveal that although governments feel their general relationship with service providers is not a concern, there are concerns about cloud factors that are of particular relevance to government.

Keywords—public cloud, government, relationship, confidence

INTRODUCTION

The public cloud has numerous potential benefits for government which include scalability and cost effectiveness. However, in comparison to the private sector, governments have been much slow in the uptake of the public cloud and prefer to opt for private solutions. There are a number of reasons that are attributed to this reluctance by government to adopt the public cloud and they include security and privacy concerns, compliance and governance. Although these are concerns that can be associated with any organisation, they are particularly a concern for government because of the responsibility they have to the privacy and security of citizen data and sensitive. There are two main approaches as solutions to the problem of government reluctance and they include a technological solution whereby improvement in technology can serve to alleviate security fears, and the

relationship solution, whereby an improved SLA agreement achieved through an improved relationship between cloud service provider and government will increase government confidence in the public cloud.

This study is concerned with the relationship factors that affect public confidence to adopt the public cloud where thay are considered with cloud related factors. Many studies that consider this issue do not offer a full picture

LITERATURE REVIEW

A. *Government in the cloud benefits and challenges*

There are a number of benefits of the cloud for government which include data storage which resolves government's problems of storing large amounts of data, cost and scalability (Bo, 2013).

There are equally a number of challenges for government in the cloud. Such challenges include a lack of established standards and a limited number of cloud providers who can meet government needs which include legal and regulatory requirements (Diez and Silva, 2013). More general challenges include security, privacy, performance and reliability issues as well as concerns about the law and national and international regulatory framework. Aziz et al. (2013) say that although the cloud has many benefits, one of them being cost savings, there are risks associated with the technology and its implementation. Zwattendorfer et al. (2013) say that challenges include security and privacy concerns with sensitive data in the cloud, compliance, interoperability and portability, identity and access management and auditing. Tripathi and Parihar (2011) present technical, economic and social challenges, where technical challenges include the transfer of legacy systems, economic challenges are mainly related to return on investment and weighing up the costs against the benefits and social challenges are related to usage, accessibility and acceptance.

B. *Security and Privacy*

Security and privacy issues, are 'show-stoppers' for the adoption of the cloud (Ghani and Suri, 2011). Security is one of the most significant issues when it comes to the adoption of the cloud by e-government and has been the main reason for reluctance for adoption by government. Government data contains highly sensitive data about citizens. Clouds are susceptible to hacking, not only for data that is stored but also for data that is transmitted (Bhatt, 2012). Spiga et al. (2014) said threats to security is the main barrier for full adoption of cloud computing despite the benefits of the cloud, this is especially the case for public administrations because security is more critical, therefore, there needs to be consideration of security and privacy laws in development of the delivery model. Ahmed and Hossain (2014) say that unless security is consistent and robust there will be little credibility in the advantages that cloud computing has to offer. Y (2013) brings attention to a number of security issues that exist in the cloud which include consideration of privacy, security, compensation for loss of data and liability.

Specifically, the problem is that sensitive data is placed in the cloud with no knowledge of location and there is a lack of transparency about the mechanisms that the cloud service provider uses for

securing data and applications (Brohi and Bamiah, 2011). Liang (2012) says that there is a need for better and more comprehensive cooperation between technology vendors and world governments to create unified global rules for a safer government cloud.

Security is essential in the government sector and has to be provided on several layers, these include the network, applications and the data security (Zwattendorfer et al., 2013). Similarly, Hashizume et al. (2013) say that cloud computing is a new computing model and there is uncertainty about security at different levels which include the host, the network, data and applications, for the latter there is a concern of how application security is moved to the cloud.

Security concerns are related to risk areas which include dependency on a 'public' internet, data storage, multi-tenancy, lack of control (governance) and therefore, traditional security measures which include authentication, authorization and identity are now not enough for clouds (Hashizume et al. 2013).

C. *Governance*

In addition to the aforementioned challenges of cloud adoption by government, there is also the impact on IT governance (Haag and Eckhardt, 2014). This refers to governments losing physical control over their data (Nycz and Polkowski, 2015). The lack of control of cloud services and not knowing how cloud systems are managed by the cloud providers is a cause for concern, and that the owner of the data, the cloud provider, is the custodian and thus has to meet the data owner's security requirements (Diez and Silva, 2013).

The main difference between normal IT systems and cloud computing in terms of security is governance, in that the organisation loses control over assets and information, this means that the collaboration between the cloud provider and the customer is essential in order to reduce the threats associated with loss of governance by the customer (Rebollo et al., 2012). This is especially the case in the public cloud where users should have the ability to control their data (Abbadi and Alawneh, 2012).

The public sector will face challenges in relation to governance when they adopt cloud computing, governance here is referred to as that related to compliance with legal and policy constraints and internal and external auditing requirements (Craig et al., 2009). The problem of governance is made worse by geographical dispersion and associated problems include enforcement difficulties, increased monitoring costs and ensuring rights when data is stored overseas (Craig et al. 2009).

IT governance is something that is considered when addressing the factors that have an influence on adoption of the cloud. Borgman et al. (2016) say that IT governance structures within an organisation moderate the technological, environmental and organisational factors as factors that influence adoption of the cloud. It is important to note that IT governance here refers to IT governance within the organisation.

As an example of these concerns, Mreea and Munasinghe (2016) refer to the Singapore government's cloud initiative where a private cloud is to be implemented because security and governance requirements cannot be met by the public cloud.

D. ***Compliance***

An important consideration for governments is that they are bound by laws that govern the protection of data, especially sensitive data related to its citizens. Problems arise in cloud computing because the servers can be located in different geographical jurisdictions which have their own data protection laws. Therefore, an important concern for government in the cloud is achieving compliance with national and international regulatory and legal frameworks (Diez and Silva, 2013).

Legal issues related to data protection are the most important in the area of cloud computing and therefore, before planning any technical details for implementation it is important to consider the legal requirements (Diez and Silva, 2013), this is especially the case in the EU where public organisations are not allowed to send data out of the EU, due to the EU Data Protection Directive (Hashemi, 2013) and the US where the Patriot Act allows the government to seize data for investigation purposes.

Unfortunately, the role of service providers regarding the compliance obligations of their clients is not well defined or understood by the service providers (Hon et al., 2012). There is the accusation that during consideration and negation of terms, which are often standard, there was little consideration by the cloud provider of the legal and regulatory obligations of the user and that the user had compliance responsibilities to regulators (Hon et al., 2012).

Haag and Eckhardt (2014) say that within public organisations there is uncertainty when it comes to jurisdiction and compliance at a global level because the nature of cloud services being cross-border and distributed which instill in governments an attitude of wait and see. In relation to this idea, it is technically it is difficult to verify that data is processed where it is claimed by the provider and often providers can be misleading (Hon et al., 2012). However, although there may be uncertainty about data being outside of Europe, providers often provide assurance that data will not be located in the United States due to the Patriot Act.

E. ***Relationship Factors***

Trust and risk perception are key relationship factors that have an effect on government willingness to adopt the public cloud. Establishing trust is key to establishing a successful cloud computing environment (Ahmed and Hossain, 2014).

Critical infrastructure services and organisations will not place their critical applications in the public cloud without being assured of trustworthiness of the different elements of the cloud (Abbadi and Alawneh, 2012). Similarly, there is concern about placing sensitive data in the cloud and that trust is the solution to enhance security and is an important way to improve reliability (Gholami and Arani, 2015).

Burda and Teutberg (2014) present a model that considers user's perception of risk and trust in addition to the antecedents of trust, they found that trust can mitigate uncertainty and actually reduce risk perception, and that risk perception is one of the main inhibitors of cloud adoption.

The relationship between the user and the service provider and the ongoing assessment by the user and the decision whether or not to continue with the provider, is affected by uncertainty of the cloud provider where quality is difficult to assess (Huntgeburth, 2015).

RESEARCH FRAMEWORK

The study is based on the idea that in order to fully understand why governments are reluctant to adopt the public cloud it is important to understand not only concerns related to cloud factors, but also the relationship factors that may also have an effect. Importantly, the approach of this research is to consider relationship and cloud factors together because to consider them in isolation does not offer a complete picture of the reasons for government reluctance. To provide an example, it would not be suffice for those interested in improving the relationship between cloud service provider and government to merely understand that government do not trust the cloud provider, but rather to says that this lack of trust manifests itself in relation to security or compliance. The study also identifies the different detailed aspects of cloud factors, referred to as sub cloud factors to further identify which aspects of the cloud are there relationship issues.

Cloud factors and relationship factors were examined and considered as critical success factors for adoption of the public cloud by government. These were derived from a review of the literature and models and frameworks for cloud adoption and trust and risk theories.

The research method, a questionnaire, was developed based on this research framework where questions were developed within domains which included trust, risk perception, negotiation, collaboration and reputation within which questions were related to the cloud factors of governance, compliance, security and privacy and performance and offering.

METHODOLOGY

The study adopted a quantitative methodology which included the use of questionnaires. Based on the research framework where a number of relationship and cloud critical success factors were identified, the questionnaire comprised of questions that addressed relationship factors in relation to cloud and cloud sub factors, on a five-point Likert scale of agreement.

Example of question structure:

Relationship CSF: ability to specify requirements

Main question: You are able to specify your requirements in relation to the following:

Cloud CSF: Governance

Sub Cloud CSFs:

- Knowledge and control over data, processes and applications
- Surety of other cloud tenants
- Knowledge and control over third party (CP) issues
- Clarity of roles and responsibilities / accountability (government and CSP)
- Dynamic SLA (towards mitigating risks, adapting to changing requirements)
- Control and knowledge of CSP employees
- Auditing and measuring of CSP
- Collaboration
- Governance during migration to the cloud

Purposive sampling was used to identify government employees in Saudi Arabia from various government ministries and department. The criteria were that these employees were involved in the process of cloud adoption or were influential in the decision-making process and thus, held middle management or senior positions in government. In total, there were 80 respondents to the questionnaire. Statistical analysis was conducted using SPSS.

RESULTS

In reference to trust, there was generally a high level of agreement that the government trusted the cloud service provider (CSP), however, where the respondents were asked if they trusted the CSP in relation to governance there was a high level of disagreement with this idea. Within governance there was a wide variation in the level of agreement, however, for sub cloud factors that would be a particular concern for government there was a low level of trust, these included control and knowledge over CSP employees and third party providers, surety over other cloud tenants and the ability to have a dynamic service level agreement (SLA) to suit government needs. Compliance is a particular concern for government and it was found they did trust the CSP in this area, again there was a wide variation within the sub cloud factors and for those factors that would be a particular concern for government, such as confidence about location of data and confidence regarding jurisdiction, there was a low level of trust. For the remainder of the cloud factors which included security and privacy and performance and offering similar patterns were noted. Generally, there was agreement that they trust the CSP but distrust arose in the sub cloud factors that would have a particular relevance to government such as security about CSP employees, security of third parties and tailored security solutions. For the risk domain, there was a close correlation with trust whereby a high level of trust correlated with a low perception of risk, and where there was a perception of risk it was in relation to government-specific concerns as is the case with trust.

Government felt that they had the ability and confidence to specify their requirements but this was met with a low confidence in the CSP's ability to understand those requirements. Again, the lower confidence in the CSP was related to areas that are of particular concern for government, this was especially the case for customisable service agreements and the extent of knowledge and control that the government had over CSP employees and processes. This lead to a lack of confidence during the

negation phase between government and CSP. Similar findings were noted for collaboration, where the government felt that they could collaborate generally and in areas such as security, but in specific areas that would be a concern for government such as governance over data and knowledge of data location there was lack of confidence.

DISCUSSION

This study viewed the issue of reluctance of government to adopt the cloud in consideration of both the cloud factors and the relationship factors with the CSP. To understand the cloud related concerns in isolation does not show how such concerns manifest in the relationship, and to consider relationship factors in isolation does not identify which aspects of the cloud are affected in that relationship. Moreover, the study offered a more in-depth investigation into the specific areas of the cloud. In consideration of this idea the study offers a more comprehensive understanding of the reasons for reluctance to adopt the public cloud.

One of the main issues with public cloud services is that they are standardised and only standardised SLAs are offered. The results of this study have shown that such standardisation of services is exactly the problem for government, this was evidenced by the fact that where government had concern was in relation to cloud factors that would be a particular concern for government such as control and knowledge of CSP employees, data location and customisable services. These cloud concerns are directly related to governance where it is a requirement of government that they have a certain level of control over data and systems in the cloud in order to be compliant to domestic and international legal and regulatory requirements.

REFERENCES

[1] Abbadi, I. and Alawneh, M. (2012). A framework for establishing trust in the Cloud. Computers & Electrical Engineering, 38(5), pp.1073-1087.

[2] Ahmed, M. and Ashraf Hossain, M. (2014). Cloud Computing and Security Issues in the Cloud. International Journal of Network Security & Its Applications, 6(1), pp.25-36.

[3] Aprna Tripathi, Bhawana Parihar. E-governance Challenges and Cloud Benefits. IEEE International Conference on Computer Science and Automation Engineering (CSAE). 2011

[4] Bo, L. (2013). Study on Massive E-govemment Data Cloud Storage Scheme Based on Radoop. *re*. 1 (1), 434 - 437.

[5] Borgman, H.P., Bahli, B., Heier, H., and Schewski, F.: 'Cloudrise: exploring cloud computing adoption and governance with the TOE framework', (IEEE, 2013, edn.), pp. 4425-4435.

[6] Brohi, S.N. and Bamiah, M.A. 2011. "Challenges and Benefits for Adoption the Paradigm of Cloud Computing", International Journal of Advanced Engineering Sciences and Technology, 8(2), pp. 286-290.

[7] Burda, D. and Teuteberg, F. (2014). The role of trust and risk perceptions in cloud archiving — Results from an empirical study. The Journal of High Technology Management Research, 25(2), pp.172-187.

[8] Craig, R., Frazier, J., Jacknis, N., Murphy, S., Purcell, C., Spencer, P., and Stanley, J.: 'Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing', White Paper. Cisco Internet Business Solutions Group, 2009.

[9] O. Diez, A. Silva. "Govcloud: Using Cloud Computing in Public Organizations." Technology and Society Magazine, IEEE 32.1 (2013): 66-72.

[10] Gholami, A. and Arani, M. (2015). A Trust Model Based on Quality of Service in Cloud Computing Environment. International Journal of Database Theory and Application, 8(5), pp.161-170.

[11] Haag, S., & Eckhardt, A. (2014). Organizational cloud service adoption: A scientometric and content-based literature analysis. Journal of Business Economics, 84(3), pp. 407-440.

[12] Hashemi, S. (2013). Cloud Computing Technology for Egovernment ARCHITECTURE. *International Journal in Foundations of Computer Science & Technology*. 3 (6), 15 - 23.

[13] Hashizume, K. Rosado, D. Fernandez-Medina, E. Fernandez, E. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*. 4 (5), 1 - 13.

[14] Hon, W., Millard, C. and Walden, I. (n.d.). Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now. SSRN Electronic Journal.

[15] Liang, J. (2012). Government Cloud: Enhancing Efficiency of E-Government and Providing Better Public Services. *2012 International Joint Conference on Service Sciences IEEE*. 261 - 265.

[16] Luna, J. Ghani, H. germanus, D. Suri, N. (2011). A Security Metrics Framework for The Cloud. *Conference Paper*. 1 (1), 1 - 6.

[17] Mreea, M. Munasinghe, K. Sharma, D. (2016). A Strategic Decision Value Model for Cloud Computing in Saudi Arabia's Public Sector. *IEEE*. 1 (1), 26 - 29.

[18] M. Nycz, Z. Polkowski. (2015). Cloud Computing In Government Units.2015 Fifth International Conference on Advanced Computing & Communication Technologies. 513 - 520.

[19] Rebollo, O. Mellado, D. Fernández-Medina, E. (2012). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *Journal of Universal Computer Science*. 18 (6), 798 - 815.

[20] Spiga, Daniele, Enrico Fattibene, Matteo Manzali, Davide Salomoni, Valerio Venturi, Paolo Veronesi, Livio Fanò et al. (2014) "A Cloud-based solution for Public Administrations."

[21] Trenz, Manuel; Huntgeburth, Jan C.; and Veit, Daniel J., "The Role Of Uncertainty In Cloud Computing Continuance: Antecedents, Mitigators, And Consequences" (2013). ECIS 2013 Completed Research. Paper 147.

[22] Y, A.. (2013). Security Issues in Cloud Computing - A Review. International Journal of Thesis Projects and Dissertations. 1 (1), 1 - 6.

[23] B. Zwattendorfer, K. Stranacher, A. Tauber, P. Reichstädter - "Cloud Computing in E-Government across Europe - A Comparison", Technology-Enabled Innovation for Democracy, Government and Governance Lecture Notes in Computer Science Volume 8061, 2013, pp. 181-195.