Proc. of the Third Intl. Conf. on Advances in Information Processing and Communication Technology - IPCT 2015

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-20

Building Government Confidence in the Public Cloud Through Improved SLAs

Waleed Alghanim, Feng Chen

***Abstract*— Increasingly governments are using cloud technology to host data and services. However, there is reluctance to place sensitive data in public clouds because of security and privacy concerns. These concerns are related to governance in the public cloud and compliance with laws. When sensitive data is stored in a public cloud, governments lose a certain amount of control. There are two suggested solutions to this problem. Firstly, the use of technology, e.g. encryption; however, this will cancel many benefits associated with the public cloud making it no longer a viable option. Secondly, through the relationship between the government as a customer and the cloud provider; this involves the service level agreements (SLA) which are often standard. Unfortunately, the standards, frameworks and certification schemes that include guidance on the governance of this relationship do not consider the specific needs of government in public cloud use and difficult to customize. Although there is willingness by governments to use the public cloud for sensitive data, unless above issues are resolved, advancement in this area will be slow. Through critical analysis of existing standards, this study proposes a new approach to the governance of the government-cloud provider relationship towards increasing confidence in placing sensitive data in the public cloud. The study focuses on standards that already consider the public cloud and sensitive data such as the Cloud control Matrix and CSA Guidance.**

***Keywords*—e-government, public cloud, sensitive data, SLA**

I. Introduction

Governments are reluctant to use the public cloud for deploying sensitive data. E-government services make a government lose the control over the information technology resources used in the cloud. This loss of control, or governance, means that it is difficult for governments to ensure security of data and systems to a standard that is required by their own laws.

Waleed Alghanim / PhD Candidate
School of Computer Science and Informatics / De Montfort University
UK

Feng Chen /Senior Lecturer
Software Technology Research Laboratory / De Montfort University
UK

Because of the nature of the public cloud it is often the case that contracts between the government and the cloud service provider are often standard and non-negotiable, one of the downsides of the public cloud in relation to its benefits associated with economies of scale. Although there are negotiable contracts available that are necessary for governments to gain the required level of control and oversight that is required by law, the ability to negotiate the relationship in order to mitigate the risks is unlikely enough to allow sensitive data and mission critical applications into the public cloud.

Inevitably, the future of e-government will have to take advantage of the benefits of the public cloud which include economies of scale, however, there needs to be balance between the specific needs of government. This paper proposes that this can be achieved through effective negotiation between governments and cloud providers through improving the standards that are designed to govern this relationship.

II. Literature

A. *E-government in the Cloud*

Aziz et al. (2013) focus on the challenges of adopting cloud technology for E-government and say that the adoption of the cloud by government has many benefits, one of them being cost savings, however, they bring attention to the fact the due to the technology itself there are also risks and importantly that the success of the implementation of this technology depends on how well the government deals with the challenges. Bhatt (2012) also considers the advantages, limitations, problems and solutions of cloud computing for E-government and the emerging future trends. Bo (2013) approaches the issue of e-government in the cloud from the angle of data storage and says that a cloud solution solves the problems that governments have with storing large amounts of data.

Moreover, there are a number of challenges when deploying the cloud for the government sector. Zwattendorfer et al. (2013) say that these 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 (2012) present technical and economic challenges. Under the technical challenges they talk about legacy systems, some of which can be written in to the new cloud computing environment but for some that could be too expensive and thus a key factor is the interoperability between existing software and hardware platforms. The economical challenge is mainly related to return on investment and weighing up the costs against the benefits.

Proc. of the Third Intl. Conf. on Advances in Information Processing and Communication Technology - IPCT 2015

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-20

Diez and Silva (2013) also look at the impacts and benefits of cloud computing for the public sector and an interesting question that is raised by these authors is why few public organizations have adopted cloud computing, which has been successful and widely accepted by other types of organization? Zwattendorfer et al. (2013) say that the challenges of governments adopting the cloud include security and privacy concerns with sensitive data in the cloud, compliance, interoperability and portability, identity and access management and auditing.

B. *Sensitive Data in the Public Cloud*

The present study is concerned with government adoption of the cloud by governments through placing sensitive data in the public cloud and their reluctance to do so. Bhatt (2012) says that sensitive data should be kept in corporate (private) clouds and non-sensitive data can reside in public clouds. Similarly, during analysis of the benefits of cloud computing for e-government in general, and the benefits that it can help developing countries to leapfrog, Khan et al., (2011) suggest that critical and sensitive government information is stored in a government private cloud and for general services where government has less control over their provision, the public cloud solution is recommended. Moreover, Lecklider (2014) says that for government agencies in the US, such as the Department of Defense, there are some data that is too sensitive and will never be put in a commercial cloud. This issue is also a concern for Diez and Silva (2013) who says that there needs to be careful consideration about what services can be migrated to the cloud, and there are certain services that cannot be migrated. Diez and Silva (2013) note that personally identifiable information is at risk especially in the public cloud, a suggestion is to anonymize the data before moving to the cloud.

The reason for such concerns is obvious; e-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). 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)

III. Governance

Another major issue is the fact that opting for the public cloud means that governments lose control over their data. Nycz and Polkowski (2015) acknowledge that there is a governance issue that the main problem with cloud computing is the lack of physical control of the data. Due to the nature of the public cloud, that is provided by a third party provider and hosted on a third party platform, there is a loss of governance ability of the owner of the data, unlike private clouds where the physical infrastructure is under the direct control of IT departments.

With a private cloud the hardware and physical infrastructure are located under the control of the government, there are no other parties involved and they can secure the servers with a firewall. However, with a public cloud most of this control is lost. There are other parties involved which include the cloud provider (CP) and the cloud service provider (SP) and the cloud is shared by multiple tenants and there are also employees of the CP and SP to be considered. Furthermore, security is a service that is provided by the SP and therefore, mostly in their control. Although the user owns the information, it is processed on an infrastructure that is owned by the CP and this is particularly a problem for critical applications because of the transnational nature of the cloud where there could be loss of control (Ahmad and Janczewski, 2011).

The European Union Agency for Network and Information Security (ENISA) Security & Resilience in Governmental Clouds report says that it is challenging for public bodies to manage their security requirements in traditional IT environments and this problem is made worse in cloud environments because they have to understand that there is a shift in the balance of accountability and responsibility for functions such as governance and control of IT and data operations (ENISA 2011). Thus there has been a shift to indirect governance and control over IT infrastructure and data; this is especially the case with public cloud computing, although these issues can be overcome by effective negotiation with the cloud provider (ENISA, 2011)

There are three main parties involved in public cloud computing, namely; the cloud provider, the cloud service provider and the cloud customer which will change the level and type of governance that a government has. One of the main issues related to security is that each of the three parties has their own security requirements which may in fact conflict with each other, in other words each stakeholder has different security requirements that they want to impose on the same service (Almorsy, 2011).

Therefore, there is a need for effective negotiation between the parties if governments want to regain or retain governance over data and systems. It is one of the premises of the study that this can only be achieved if all of the areas where governance is relevant are identified. This identification takes place using the various standards that govern the relationship, for example, responsibilities and access rights of third-party cloud provider personnel or the management of data in the cloud. More governance will lead to more confidence but this will only be possible when the standards consider governance in the specific situation of governments using the public cloud to deploy sensitive data.

IV. SLA Relationship

All of these issues lead to a decrease in the type and level of governance that governments have over the cloud and the associated assets. In reference to the governance issues, the change towards indirect governance and control over IT infrastructure and data through the use of the public cloud presents a significant challenge. However, some of these issues can be overcome by negotiation.

The reluctance of governments to place sensitive data in the public cloud is something that has been addressed by

Proc. of the Third Intl. Conf. on Advances in Information Processing and Communication Technology - IPCT 2015

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-20

ENISA in 2015. ENISA say that there are two possible solutions to the problem of this reluctance, which is based on security and privacy concerns, the first is encryption as a technical solution, and the second is to improve the relationship between the public cloud provider and the government as a customer through improving the Service Level Agreement (SLA). Therefore, there is a need to address the issues that affect this relationship, specifically in this case the standards that govern the negotiation between customer and provider.

There are a number of issues related to security and privacy that can be addressed through the SLA relationship. These issues include the transfer of responsibility and the control over assets as well as system components to a third party, the lack of a direct point of contact to discuss the allocation of duties for both parties, greater coordination in terms of security-related compliance to law and regulation, the lack of insight and control over security and privacy and the allocation of responsibility. All such issues are only made aware to governments through the various standards, and this paper proposes that the root cause of lack of confidence in the public cloud is the weakness of these standards in informing that relationship.

V. Standards, Certification and Frameworks

This study proposes that an improvement in the SLA relationship will increase government's confidence in placing sensitive data in the public cloud. When a government or government department engages with a cloud provider during negotiation, it does so using an accepted standard, framework or certification scheme.

The main problem is however, that many of the standards, certification and frameworks do not consider the specific and unique needs of government placing sensitive data in the public cloud. They are not suitable for the government use in this case.

The Cloud Security Alliance (CSA) is an organization that has put forward a number of standards to ensure security in the cloud which includes governing the relationship between the customer and the cloud provider. CSA has developed a Cloud Control Matrix (CCM) which is cross referenced with other standards and frameworks. The CCM is also used as a basis for other standards provided by the CSA. A criticism of the CCM is that it is aimed at different types of organization and cloud computing generally.

The Consensus Assessment Initiative Questionnaire (CAIQ v3.0.1) includes questions that a cloud consumer, or even a cloud auditor, can ask a cloud provider. The questions are 'yes' or 'no' and they can be tailored to suit the requirements of the organization. The questions are based on the security controls found in the Cloud Control Matrix CCM.

CSA has provided CSA Guidance which although includes consideration of auditing and monitoring security across the cloud-based IT security supply chain, does not focus on the public cloud or government considerations and is very generic. In fact, CSA themselves claim that the CSA Guidance will not be suitable for all situations because there are many different cloud deployment options, specifically governments are faced with whether to use SaaS, PaaS or IaaS and public or private clouds. Because there are so many possibilities CSA claim that there is no list of security controls for one situation.

Another commonly accepted standard is NIST which although provides a catalogue of security and privacy controls for government information systems which are wide ranging, it covers all aspects of security and privacy in information systems generally and is not designed specifically for government use of the cloud.

ISO 27001 is the most widely used certification designed for information security management systems and specifies requirements for implementing such systems. ISO 27001 contains a set of high level security objectives also known as control objectives, this is accompanied by ISO 27002 which provides more detailed security measures also known as security controls. Unfortunately, of the limitations of ISO are that it focuses on the risks for an organization but does not consider whether or not an organization can be trusted to provide IT services as a product for customers, the scope of the certification can be chosen by the company, which means not all of their products may be covered and an organization is free to choose the control to be implemented and the risks the organization is willing to accept. Moreover, with the ISO 2700 cloud standards they only offer information of what needs to be done in order to be compliant, but they do not tell you how to do it, this is by their own admission and their security certifications do not cover all of the complexities of cloud computing (Almorsy et al, 2011).

In summary, there are concerns expressed by customers that there is a lack of trust by customers, specifically; these concerns are about the liability and accountability of providers in terms of security breaches and data protection. The problem is that these concerns are not addressed by existing standards, certification schemes and frameworks, and therefore, these need to be reconsidered to increase confidence in governments.

VI. Conclusion

In conclusion, the reluctance of governments to use the public cloud for hosting sensitive data in the public cloud stems from security and privacy concerns. The solution to this problem can be found in improving the relationship between the government and the cloud provider and this paper has proposed that in order to achieve this and increase confidence, there needs to be an improvement in the standards that govern this relationship or a new approach to such standards.

Future development on this idea will involve an identification of the unique and specific requirements of governments placing sensitive data in the public cloud followed by a critical analysis of the standards, frameworks and certification that govern this relationship towards increasing confidence. Already countries such as Estonia, a pioneer of e-government, are starting to consider a complete e-government solution that depends on the public cloud.

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-20

References

[1] M. Aziz, J. Abawajy, M. Chowdhury (2013). The Challenges of Cloud Technology Adoption in E-Government. *2013 International Conference on Advanced Computer Science Applications and Technologies*, 470 - 473.

[2] D. Bhatt, (2012). A Revolution in Information Technology - Cloud Computing. Walailak Journal. 9 (2), 107 - 113.

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

[4] A.Tripathi, B. Parihar. (2011). E-governance challenges and cloud benefits. IEEE. 351 - 354.

[5] 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

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

[7] F.Khan, B.Zhang, S.Khan, S.Chen. (2011). Technological Leap Frogging E-Government Through Cloud Computing.Proceedings of IEEE, 201 - 206.

[8] T.Lecklider. (2014). Good enough for government work. Cloud Computing, 18 - 19.

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

[10] R. Ahmad, L. Janczewski. (2011). Governance Life Cycle framework for Managing Security in Public Cloud: From User Perspective. 2011 IEEE 4th International Conference on Cloud Computing. 372 - 381.

[11] ENISA. (2011). Security & Resilience in Governmental Clouds - Making an informed decision. ENISA., 1 - 141.

[12] M. Almorsy, J. Grundy, A. Ibrahim. (2011). Collaboration-Based Cloud Computing Security Management Framework. 2011 IEEE 4th International Conference on Cloud Computing, 364 - 371.