Security Criteria in Deciding on Migration of Systems to the Cloud

Rafael Gómez[1], David G. Rosado[2], Daniel Mellado[1] and Eduardo Fernández-Medina[2]

[1]Spanish Tax Agency, Madrid, Spain

[2]GSyA Research Group, University of Castilla-La Mancha,
Dept. of Information Systems and Technologies, Ciudad Real, Spain

Abstract. Cloud computing is setting trend in IT world. As it evolves, providers and clients claim their concern about their pros and cons. Some proposals have been made on the methodologies to assess criteria for benefits and risks of the different cloud models. How these proposals deal with security issues (that most IT executives point out as their top concern)? In this paper we go into the issue of how we can incorporate security requirements to a decision making process for whether to migrate legacy systems to the cloud and how to do it. From systems in control of the firms' data centers to systems working partially, if not totally out of their control.

1 Introduction

Mell & Grance propose in [20] the most widespread definition for the ultimate utility model in the IT field: the cloud computing. They describe cloud computing as "*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*."

Some like Jansen & Grance say that cloud might be "at odds with traditional security models and controls" [15] and, for IT executives, security is a top concern when they are asked about the major deterrents for adoption of the cloud model [8, 10]. So it's still today [23] (see *fig. 1*).

But, is this concern really undermining the final decision when we face in the other plate of the balance the promise of huge savings? How can we model and calibrate the pros and cons of the whole migrating process of a business? After all, security criteria are probably some of the most difficult to size of all criteria in the decision process.

There are authors who see the cloud not as a threat but an opportunity to improve the security of many legacy systems. Winkler says in [25] that the migration to the cloud "gives us hope that we can regain control over gaps and issues that stem from poorly integrated or after-thought security." Also, Buyya et al. point out in [4] that

Gómez R., G. Rosado D., Mellado D. and Fernández-Medina E..
Security Criteria in Deciding on Migration of Systems to the Cloud.
DOI: 10.5220/0004099600930100
In *Proceedings of the 9th International Workshop on Security in Information Systems* (WOSIS-2012), pages 93-100
ISBN: 978-989-8565-15-0

security can be guaranteed more easily over grids and clusters.

According to a research carried out by MeriTalk among 166 US Federal IT executives 47% of the existing federal IT applications are based on legacy technologies that need modernization [24]. The overall federal budget to maintain this kind of systems can be estimated around the $35.7B, somewhat around 40% of the overall federal budget for IT (this percentage when applied to the whole world IT annual budget stands out up to $1.45T). According to Gartner, modernization technologies for legacy is the fourth in the list of IT executives' priorities [11].

In this paper we present a preliminary research of some of the efforts that have been made in the field and the concrete references that we have found regarding issues like the impact of the security criteria in the migration of legacy systems to the cloud. It is meant to be only the first step into a full research aiming the problem and how it is presented to private and public organizations, what issues they regard as important, and how they incorporate security criteria on their decisions.

The paper is structured in seven sections. The first one is this introduction. Section two presents a definition on the decision problem. Sections three and four present two related issues: the current state on multi-criteria analysis and the current research on the legacy systems migration. In section six gives out some related works. Last, in section seven we present our conclusions and future work.

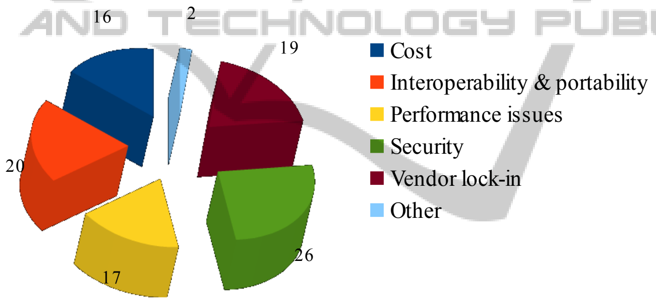

Fig. 1. Top concerns surrounding cloud computing.
(source The Open Group Cloud Computing Survey 2011)

2 Problem Definition

An organization that plans migrating its legacy systems to the cloud must face several challenges: to reduce or keep the overall provision costs while ensuring the functional levels and enhancing or maintaining some other requirements like scalability, security and privacy, and response when a lack of availability event comes about.

Decision Makers: Most of the times, the leading decision makers are the non IT executives (i.e. those in the functional areas) and also those who are responsible of the IT area. Usually all of them work together since there are common interests though each one might have different concerns about the migration goals.

Goals: In any case, the goal of the decision is not unique and, frequently, they are conflicting goals. Every project of migration of a system to the cloud (whether or not is legacy) aims one or more of these:

- To reduce the cost associated to the normal work of the system.
- To improve the flexibility of the system to cope with peak times.
- To improve the system availability.
- To ease the sustainable growth of the system.
- To improve the intrinsic security of the system.
- To prepare the organization for a (may be partial) outsourcing of IT function.

Uncertainty and Risks: On the other hand, we must be prepared to accept that either decision (migrate it or not, and which systems are to migrate, and which model we choose) have some uncertainties that we must manage. For instance, the main uncertainty usually comes from the financial side. A sustained growth of the organization might justify investments and service costs of traditional data centres, but if a recession strikes, maintaining oversized systems may impose an excessive cost impossible to reduce with traditional models. Another uncertainty we find is the question on how technology evolves and the lower costs that the evolution brings.

Impact of Time: A legacy migration (valuable for the organization) is not a long term project, but its effects are long term and must be planned carefully. First, because the main driver of the change usually is cost savings (like other outsourcing processes). Nevertheless, once the decision is made, the utility model will be there for good. In other words: if the driver is cost savings, the opportunity window may be not always the same. Furthermore, any outsourcing process implies a cultural change that needs some time to mature (before and after the project kick off).

Roles: Though there are two clearly identified roles (service providers and clients), the truth is that there are many others that participate and/or are affected by the decision: Public Administrations, other companies and people. For instance, when a European citizen entitles to a EU company to keep their personal data, but when the company places its data in the cloud, the preservation of the rights is not clear.

Decision Variables: The first decision variable in this kind of decision making problem is whether migrating the legacy is viable, either in its entirety or some subsystems, or it's better to keep the system just as it is.

If the migration is proposed, another decision variable is which service and deployment models we choose for implementing the decision. The service models that we usually find in literature are: software as a service (SaaS), platform as a service (PaaS) and infrastructure as as service (IaaS). Deployment models usually proposed are: public cloud, community cloud, managed cloud, hybrid cloud and private cloud. Each of the service models and deployment models has different characteristics of technical implications, cost, scalability, security, propriety, location, etc. and solutions proposed may be different for each subsystem.

Finally, a third decision variable is what is service level that the company wants to agree with the cloud service provider for each of the clauses in the service level agreement (SLA). It can be anticipated that the provider will charge differently for each service level agreed in the SLA (availability, unattended management, monitoring, etc.). This variable is, furthermore, quite complex because can imply different combinations and/or technical developments.

Table 1. Deployment models.

	Managed by	Property of infrastructure	Infrastructure located in	Accessible and used by
Public cloud	3rd Party provider	3rd Party provider	Out of premises	Non trusted
Community cloud	3rd Party provider	3rd Party provider / Community	In premises / Out of premises	Trusted
Managed cloud	3rd Party provider	3rd Party provider	In premises	Trusted
Private cloud	Organization / 3rd Party provider	Organization / 3rd Party provider	In premises	Trusted
Hybrid cloud	Organization & 3rd Party provider	Organization & 3rd Party provider	In premises & out of premises	Trusted & Non trusted

3 Multi-criteria

The first thing we can see when we look at the problem is the fact that we do not face a situation in which a single goal can be optimized. We have several goals, some of them conflicting each other, some of them difficult to quantify (therefore to optimize).

Some of the goals (i.e. reducing the maintenance costs and improving the system availability) are easy to measure, but are at odds with each other. Others, like improving intrinsic security are hard to measure.

Some works, like [19], have presented into quantifying some aspects of security. But, when the main driver for the change is economical, the best path is to quantify security in terms of its economic impact.

Formally, a MCDA problem can be expressed as:

$$max\{g_1(a), g_2(a), \ldots, g_k(a) \quad / \quad a \in A\} \qquad (3.1)$$

Where A is a finite set of possible alternatives $\{a_1, a_2, \ldots, a_n\}$ and $\{g_1(.), g_2(.), \ldots, g_k(.)\}$ a set of evaluation criteria.

Rarely an MCDA problem includes an alternative that optimizes all the criteria at once. Furthermore, the solution is not only dependent on all input parameters in (3.1), but on the beliefs of decision maker. The best solution is a compromise between the given data and the preferences expressed by the decision makers.

In [12] Guitouni & Martel presented a methodology for a MCDA process consisting in the non lineal recursive iteration with four steps: 1) structure the problem, 2) model the preferences, 3) calculate the preference model, and 4) make recommendations. The goal of the methodology was being able deal with all the aspects of a decision problem in which a satisfactory solution is the new paradigm.

4 Legacy Systems Migration

The problem of low quality software from the perspective of maintainability and adaptability of the systems is not new. Actually, this has been the core issue of the whole practice of software engineering for many years. Whenever a new technology appears, the products and services that were developed with the previous technologies become legacy. For a given technology, the word ‘legacy’ is quite ambivalent: for the owner of the system or for non IT executives ‘legacy systems’ are valuable assets, whereas for the software practitioner of the IT executive they are a source of risks.

There are many definitions for ‘legacy system’, but probably the most extended in the software engineering field are found in [22]: a system becomes legacy when “*significantly resist modification and evolution regardless of the technology from which it is built.*” Some point out that legacy systems actually have a social part and include, not only hardware and software, but processes and people. Another common characteristic of this kind of systems is that they are classified as critical to business.

As for the methodology to evolve legacy systems we can find a framework in [3], where Bisbal et al. classify the evolution of legacy from wrapping technologies to overall redevelopment of the deprecated system, being common the mixed. Properly speaking, migration is in between wrapping and redevelopment. In [22], Seacord et al. also offers an approximation to modernizing driven by risk.

Nevertheless, most of the works we have found have one thing in common: they are not specifically adapted to a given technology (that is, they have not been tailored). There is little work on how to migrate to service oriented architectures (SOA), work that should draw our attention since cloud computing actually is an specific form of provision for this kind of architectures. In [13], Heckel et al., justify the lack of work in the field of SOA since it’s an area for which concern for reengineering is quite recent. Actually, if we set our focus into the more specific issue of cloud computing, references are even less.

5 Security Criteria for Cloud Environments

It’s not surprising that there are plenty of research on security criteria for cloud computing or SOA, either generic ones or quite specific.

Jansen & Grance’s report [15] is probably the most noticeable set of criteria and specific issues related to cloud computing. In it, it is made a detailed description on the criteria and issues related to privacy and security, identifying the pros and cons of the model set up against its traditional counterpart, and the main points to cover.

They identify some positive aspects of the cloud model: specialization of the technical people, greater uniformity leads to a greater security and eases automation, resources availability, platform scalability, uniformity, robustness of the backup and recovery policies. They also give some negative aspects (i.e. a greater system complexity from the global perspective or the the loss of direct control either on the logical or the physical items).

Since cloud computing steams from a set of different technologies like SOA, Web 2.0 and computing as an utility, many of the issues related to privacy and security were already known. They are only viewed from a new perspective.

Jansen & Grance divide their security criteria in nine sections: security governance, rules and standards compliance, trust building, security architecture, identity and access management, software isolation, data protection, system’s availability and incident response. For each of these sections, they make specific recommendations.

Two other basic references for cloud security are [5] and [6] from the Cloud

Security Alliance (CSA). CSA presents its guide following three views and fifteen of security: architecture, governance and operation. Each of the domains represent, to our decision problem, a set of restrictions to our model that should be evaluated for each of the legacy piece we have to deal with.

As we can see, none of this threats looks directly linked with the migration of legacy. Nevertheless, the overall impression is that legacy migration does pose some specific security questions.

6 Related works

There are plenty of works presenting decision models of some sort related to cloud migration. One of them even presents a case. But most are not multi-criteria, and nearly all focus solely on the aspect of expected economic savings.

Probably the most interesting one we have found is presented in [16, 17] which studies specifically the use of decision support tools. Khajeh-Hosseini et al. present in [17] two methods supported by tools to asses on the decision process on who is the best provider and technology solution for cloud computing: though costs modeling, and benefits and risks analysis. Costs modeling is presented as an extension to the UML deployment diagram by means of allowing the modeler to incorporate items like virtual machines or virtual storage, or an unspecific node, or remote applications or data. In its risks/benefits analysis mode, [16] presents a more deep analysis regarding the benefits and risks and taking into account diverse factors with an overall decision outcome as a weighted sum of the risks and the benefits. Both, pros and cons, are catalogued intro categories: technical, organizational, legal, security and financial.

Though it's not specific to MCDA, another interesting work is Schryen's one in [21]. In it, it's presented a model based on fuzzy logic applied to the problem of investing in security measures for distributed system models. Shryen proposes a process that starting from a formal specification language for modeling security conditions and its transformation into logical predicates, he defines some fuzzy sets and a decision model based on those sets.

Another paper worth mentioning is Huang's et al. [14]. In it, they use models like DEMATEL, ANP and Grey Relational Analisys to address the analytical decision process of baking services cloud migration.

There are other articles published on the issue of decision making for cloud migration, some of them are closer to our problem (security), others less close: Andrezejak, Kondo & Ji [1], Bibi, Katsaros & Bozanis [2], Chen & Sion [7], Fedriksson & Agustsson [9], and Künsemöller & Kark [18]. We haven't considered them since, though they are related with MCDA techniques and cloud migration, they do not deal with the migration concept in the sense that we talk about here.

7 Conclusions and Future Work

From the works we have seen up to now, we conclude that though there are quite a few papers on the issue of MDCA applied to cloud computing decisions, there is nothing specifically designed to address the problem of legacy system migration, and, though some of them point out to security concerns none of them handles the security issues as factors modeled in a quantitative manner integrated with the overall decision model, but as constraints that must be ensured.

For that reason, we are working to develop an overall model to help the practitioners to integrate security into de decision of migrating legacy systems to the cloud with a MCDA perspective.

Given that any proposed model should take into account the actual beliefs and preferences of the actual practitioners, we have developed a questionnaire to help us to understand which are the true concerns of the IT decision makers who must face a project to migrate part of their systems to the cloud, and how much security is a real concern and how the value it against economic restrictions like costs.

The questionnaire will look into other issues like the anticipated and the actual issues regarding the migration process, and the result of the projects (if they are already finished).

We will feed this questionnaire to several IT executives and further refine our model so that it can be used to future aid into the decision problem after modeling the beliefs and preferences of the decision maker.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557) and ORIGIN (IDI-2010043(1-5), financed by the Centre for Industrial Technological Development (CDTI) and the FEDER, MAGO-PEGASO (TIN2009-13718-C02-01) awarded by the Spanish Ministry for Science and Technology and SERENIDAD (PEII11-0327-7035) and SISTEMAS (PII2I09-0150-3135) financed by the Council of Education and Science of the Castilla-La Mancha Regional Government.

References

1. Andrzejak, A., D. Kondo, and S. Ji. Decision Model for Cloud Computing under SLA Constraints. in IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), 2010. 2010.
2. Bibi, S., D. Katsaros, and P. Bozanis. Application Development. Fly to the Clouds or Stay in-House. in 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 2010.
3. Bisbal, J., D. Lawless, B. Wu, and J. Grimson, Legacy Information Systems: Issues and Directions. IEEE Software, 1999. 16(5): p. 103-111.
4. Buyya, R., C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 2009. 25(6): p. 599-616.
5. CSA, Security Guidance for Critical Areas of Focus in Cloud Computing. 2009, Cloud Security Alliance.
6. CSA, Top Threats to Cloud Computing. 2010, Cloud Security Alliance.
7. Chen, Y. and R. Sion. To Cloud Or Not To Cloud? Musings On Costs and Viability. in 2nd

ACM Symposium on Cloud Computing SOCC 2011. 2011.

8. Christiansen, C. A., C. J. Kolodgy, S. Hudson, and G. Pintal, Identity and Access Management for Approaching Clouds, in IDC White Paper. 2010.
9. Fredriksson, J. and K. Augustsson, Cloud Service Analysis Choosing between an on-premise resource and a cloud computing service. 2011, Chalmers University of Technology, University of Gothenburg.
10. Gens, F. IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. 2008; Available from: http://blogs.idc.com/ie/?p=210.
11. Gomolski, B., Gartner Perspective on IT Spending 2010. 2010, The Gartner Group.
12. Guitouni, A. and J. M. Martel, Tentative guidelines to help choosing an appropriate MCDA method. European Journal of Operational Research, 1998. 109(2): p. 501-521.
13. Heckel, R., R. Correia, C. M. P. Matos, M. El-Ramly, G. Koutsoukos, and L. F. Andrade, Architectural Transformations: From Legacy to Three-Tier and Services. Software Evolution, 2008: p. 139-170.
14. Huang, C.-Y., W.-C. Tzeng, G.-H. Tzeng, and M.-C. Yuan, Derivations of Information Technology Strategies for Enabling the Cloud Based Banking Service by a Hybrid MADM Framework. Smart Innovation, Systems and Technologies, 2011. 10: p. 123-134.
15. Jansen, W. and T. Grance, Guidelines on Security and Privacy in Cloud Computing. 2011, NIST.
16. Khajeh-Hosseini, A., D. Greenwodd, and I. Sommerville. Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. in IEEE 3rd Int. Conf. on Cloud Computing (CLOUD 2010). 2010.
17. Khajeh-Hosseini, A., I. Sommerville, J. Bogaerts, and T. P. Decision Support Tools for Cloud Migration in the Enterprise. in IEEE 4th Int. Conf. on Cloud Computing (CLOUD 2011). 2011.
18. Künsemöller, J. and H. Kark. A Game-Theoretical Approach to the Benefits of Cloud Computing. in 8th Intl. Workshop on Economics of Grids, Clouds, Systems, and Services (Gecon2011). 2011.
19. Madan, B. B., K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, A method for modeling and quantifying the security attributes of intrusion tolerant systems. Performance Evaluation, 2004. 56 p. 167–186.
20. Mell, P. and T. Grance, The NIST Definition of Cloud Computing 2011, NIST.
21. Schryen, G. A Fuzzy Model for IT Security Investments. in Sicherheit 2010. 2011.
22. Seacord, R., D. Plakosh, and G. Lewis, Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices. 1st ed. Addison-Wesley Professional. 2003.
23. The Open Group, The Open Group Cloud Computing Survey. 2011, The Open Group
24. Tobin, M. and B. Bass, Federal Application Modernization Road Trip: Express Lane or Detour Ahead? 2011, Meritalk.
25. Winkler, V. J. R., Introduction to Cloud Computing and Security, in Securing the Cloud. Cloud Computing Security. Techniques and Tactics., E. Syngress, Editor. 2011. p. 25.