Return On Security Investment for Cloud Computing: a Customer Perspective

Carlos Alberto da Silva
Institute of Computing - Unicamp
Campinas, Brazil
beto@lasca.ic.unicamp.br

Paulo Licio de Geus
Institute of Computing - Unicamp
Campinas, Brazil
paulo@lasca.ic.unicamp.br

ABSTRACT

Cloud Computing has introduced a variety of models of service delivery and deployment for public clouds, hybrid and private, that changed enterprise computing. Several providers provide these services, and each uses different models and pricing solutions. One of the most complex tasks for IT governance team is to calculate the total cost of an IT service in relation to its potential return, and needs to consider the tangible and intangible benefits (security) with views over the short, medium and long term as well as contract termination costs. To evaluate the Return On Security Investment (ROSI) in Cloud Computing, this paper presents a new qualitative and quantitative approach for calculating the ROSI.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

General Terms

Security

Keywords

Cloud Computing Security; ROSI; Security Metrics

1. INTRODUCTION

Potential customers of cloud computing perceive a lack of transparency and a relative lack of control when compared to the traditional computing models[12]. In the industry these services are referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), respectively.

Such customers (or companies) decide to migrate part of their data, services or infrastructure to a cloud computing service provider (CSP) based on the following parameters: expected benefits, adoption costs, performance, flexibility, business opportunities and others[19, 18, 20]. In the current literature, it is unclear whether the CSP should provide security services or not, and what these services characteristics and varying levels of protection and costs involved should be.

The decision to migrate refers to a particular document: "Deployment Profile", which is defined in the context of this article to include four elements that will be evaluated: mobilized assets, types of cloud service, deployment models and a specific CSP. Due to the varying levels of customer controls for each profile, different security services are offered by the CSP. Increased protection on the side of the CSP should raise rates deployment and maintenance costs, while less protection means more control and client-side costs.

From a customer's perspective, this paper presents a new qualitative and quantitative approach to the security requirements in the process of migrating to cloud computing, and proposes the use of security metrics to analyze the benefits and costs of security for a given deployment profile. The ultimate goal is to properly assess whether the decision to migrate assets (e.g. data, services, applications, infrastructure etc.) to cloud computing is beneficial or not, both economically and security-wise. This means that the customer has to evaluate both the level of security provided by the CSP and the costs that such controls present. We assume that the CSP is cooperating and willing to reveal its offered security services through a portfolio of security metrics.

2. BASIC CONCEPTS

In this section, the concepts that will be used in this approach will be presented.

2.1 Security Metrics

A metric is a standard for measurements, and its value is the result of measuring something. A metric provides a numerical description of a particular feature of the items under investigation. The metric defines both what is being measured (the attribute) and how it is being measured (the unit of measurement)[15].

Measurement is the process of collecting metrics and establishing rules for interpretation of the results. Any restrictions or related controls are defined in the measurement process[21].

Each metric can return values such as: i) number - expressing an absolute value of a measured element; ii) percentage - expressing a measured component relative to the

total of the elements; iii) average - expressing a mean value of an element relative to a set of elements; iv) other quantifiable values.

Security metrics are a technique by which we monitor and compare the level of security and privacy, or privacy state (status), or the security record of a computing environment. The judicious use of security metrics promotes transparency, decision-making, predictability and proactive planning[14].

In this proposal, we use the methods and techniques presented by [9, 8, 7] to create the portfolios of security metrics to the security requirements of the cloud computing environment.

2.2 Return on Investment (ROI)

Return on Investment (ROI) is one of several financial indicators available to estimate the financial result of the company's investments (in this proposal: a possible client who hires a service from a CSP). This calculation takes into account the cost of an investment and its expected earnings, and provides an estimate of how favorable the investment will be. To calculate the ROI (simple ROI), the cost of an investment should be subtracted from the gain (return) of the investment, and the result divided by the cost of the investment; the result is expressed as a percentage or fee. In most cases, a rate greater than 0 (zero) means that the return is greater than the cost, then the investment can be considered beneficial (how beneficial depends on the objectives of the investment or corporate standards of the company)[11]:

$$\text{ROI} = \frac{(\text{Gain\_From\_Investment} - \text{Cost\_of\_Investment})}{\text{Cost\_of\_Investment}}$$

Where:

- Gain From Investment: the final value of the benefits;
- Cost of Investment: the initial value of the investment

Such values can be estimated or calculated.

2.3 Methodology for ROSI Calculation

There are many possible ways to estimate ROSI in a cloud computing environment, and no approach is suitable for all situations due to the measurable and non-measurable qualities. Selecting the best option for a particular case depends on many factors, including what the business drivers for migrating to the cloud are (revenue growth versus cost savings), the approach to prepare and evaluate the business cases (emphasis on tangible versus intangible QoS), and where the company is in the growth cycle/maturation of business (new business versus mature company).

3. CALCULATING ROSI

This section presents the definition of new economic indicators created by this approach to calculate the return on investment in security for the security requirements in a cloud computing environment.

3.1 ROSI_{a}

The financial indicator ROSI_{a} is the arithmetic difference between the value measured by the CSP for the security requirement "Deployment Profile" and the value expected by the customer, as follows:

$$\text{ROSI}_{\text{a}} = -(\text{Evaluated\_Metric} - \text{Expected\_Value})$$

Where:

- Evaluated_Metric: the value measured by the CSP for the security metric requirement, between 0 and 4;
- Expected_Value: the value expected by the client for the security requirement, between 0 and 4.

3.2 ROSI_{vi}

The financial indicator ROSI_{vi} is obtained by subtracting the expected value from the measured value for the given metric, as informed by the client, relative to the measured value, as follows:

$$\text{ROSI}_{\text{vi}} = \frac{(\text{Evaluated\_Metric} - \text{Expected\_Value})}{\text{Evaluated\_Metric}}$$

Where: Evaluated_Metric and Expected_Value to assume the value between 0 and 4.

3.3 ROSI_{vf}

The financial indicator ROSI_{vf} is obtained by subtracting the expected value from the measured value for the given metric, as informed by the client, relative to the expected value, as follows:

$$\text{ROSI}_{\text{vf}} = \frac{(\text{Evaluated\_Metric} - \text{Expected\_Value})}{\text{Expected\_Value}}$$

Where: Evaluated_Metric and Expected_Value to assume the value between 0 and 4.
The results for the previous indicators may fall into the following ranges:

- Positive: the CSP is ensuring greater security than the customer expects (beneficial to the client). Example: ROSI_{a} being 2.0 indicates that the Gain from Investment is 200 % above the cost of investment;
- Zero: the CSP has exactly the level of security that the customer wishes/requests;
- Negative: the CSP is presenting less security than the customer expects (prejudicial to the client). Example: ROSI_{a} being -1.0 indicates that the Gain from Investment is 100 % below the cost of investment.

3.4 Deployment Profile

The migration decision has to be implemented on the customer side. Essentially, the customer has to answer to the following question: "Are the security controls offered adequate and efficient from a security perspective?". The answer to this question must affect the decision to migrate to the cloud computing [20].

The process of creating the "Deployment Profile", where the customer chooses, from the portfolios of Infrastructure and Service security metrics, which security metrics to use and their expected values. Each expected value falls in the range [0, 1, 2, 3, 4], respectively corresponding to the expected security levels [Critical, High, Medium, Low, None].

3.5 Behavior Security Metrics

At this stage, we will analyze a sub-metric of Firewall, "Packet filtering" where their efficient is measured at the highest number of packets filtered by rules.

Using generic algorithm for time series analysis, the Figure 1 presents the packet filtering security metric was collected

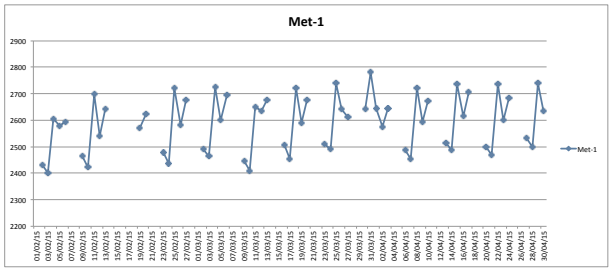

Figure 1: Packet filtering metric (collected)

and in the period: 01/02/2014 to 06/30/2015, in schedule of eleven consecutive hours.

The Figure 2 presents the metric applying filters in the time series, excluding: saturdays, sundays and holidays, and the normalized metric to the scale of values [0-4]. The function of normalization can be summarized for f(x), where x account the number of filtered packets, and assumes "2" for values greater/equal to 2,500 packets, and assumes "3" to values lower than 2,500 packets. Such parameters of normalization are defined for each security metrics.

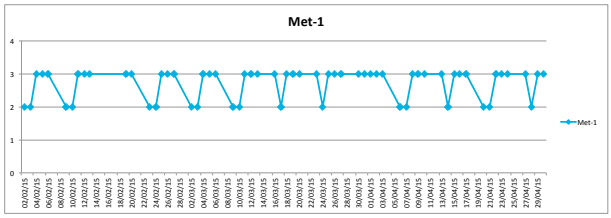

Figure 2: Packet filtering metric (normalized)

The Figure 3 presents the baseline prediction for the normalized metric to the scale of values [0-4] using the reference one week.

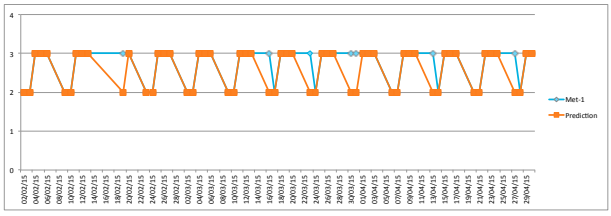

Figure 3: Packet filtering prediction

In the context of this work, we seek to identify the factors that produce the change of a value in the range of [0-4] for each security metric measured the cloud computing environment, summarized as follows: by Customer, at Provider, by Client/Provider, and and Dynamic System.

4. CASE SCENARIO

Let's consider a case scenario of customer John who considers whether to migrate assets (e.g. data, services, etc.) to a cloud deployment provided by CSP_X. CSP_X provides a private cloud deployment for John, while the available offered service is Software-as-a-Service (SaaS).

The customer chose in the range [0, 1, 2, 3, 4], respectively corresponding to the expected security levels to some security metrics (portfolio) to security requirements, and calculate the $ROSI_{a,vi,vf}$. The result of $ROSI_{a,vi,vf}$ should guide decision making about hiring or not the service SaaS offered by the CSP_X.

Table 1 shows the firewall security metrics from the infrastructure portfolio chosen by the customer, where: i) Identification (Id) singles out a metric from the portfolio; ii) Evaluated Metric (EM) is the value that the CSP_X is committed to meet via contract (measured by the CSP_X through a time series analysis); iii) Expected Value (EV) is the value expected by the client for the security requirement.

Table 2 shows the PostgreSQL database security metrics from the service portfolio chosen by the customer.

Figures 4 and 5 illustrate the behavior of the security metrics that make up the deployment profile values: i) Evaluated Metric (EM) is the value that the CSP_X is committed to comply via contract (blue lines); ii) Expected Value (EV) is the value expected by the customer from the CSP_X (black lines); iii) Average EM (Aveg-EM) is the arithmetic mean value of the metrics measured by the CSP_X (green lines). Figure 4 illustrates the firewall security metrics from the infrastructure portfolio and Figure 5 the PostgreSQL database security metrics from the service portfolio.

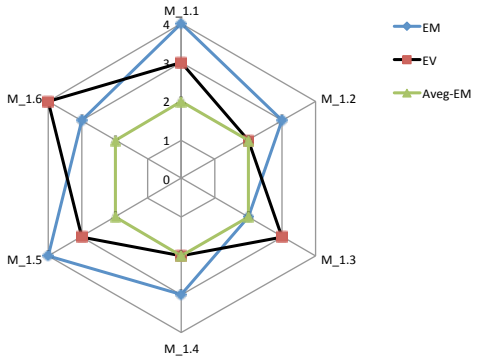

Figure 4: Firewall Metrics

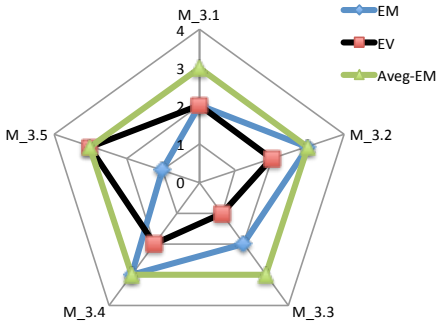

Figure 5: PostgreSQL Metrics

The red dots (expected values) that are above or equal to the blue dots (evaluated metrics) are the requirements that

are met by the CSP_X (beneficial to the client). Otherwise, the expected values that are below the evaluated metrics are the CSP_X requirements that do not meet the customer's security level (prejudicial to the client).

4.1 Results

The client should consider the behavior of each chosen security metric, in order to understand and evaluate all aspects involving the cloud migration decision. For instance, the client may reject some of the included security controls or replace them with equivalent ones, based on their benefit to the security cost or the result for $ROSI_{a,vi,vf}$.

Based on data from Table 1, the security metrics $M_{1.3}$ and $M_{1.6}$ indicates negative values for the return on security investment, i.e. these metrics are presenting security levels below what the customer expects (prejudicial to the client).

When analyzing the percentage of security requirements that have negative values for $ROSI_{a,vi,vf}$, we verify that 18% of them are prejudicial to the client (2 out of 11).

For security requirements that differ from the contract, the customer can choose one of the following:

- Accept the migration to the CSP_X based on the described Deployment Profile and the results for $ROSI_{a,vi,vf}$;
- Reject the migration to the cloud due to the results for $ROSI_{a,vi,vf}$ that are not satisfactory;
- Choose another Deployment Profile with new parameters: assets, models, types and controls;
- Choose another CSP_X that satisfies the given parameters.

Thus, the customer can identify which what security requirements are guaranteed by the CSP_X (beneficial to the client), and what not (prejudicial to the client).

Table 3 shows the necessary investment for firewall security metrics from the infrastructure portfolio chosen by the customer. The currency used in the example is irrelevant, so we consider the values as plain numbers (e.g. 30), where: Cost is the annual value for: install, configure, training, etc. and Investment is the necessary annual value to improve the security requirement provided by the CSP_X.
The CSP_X can use the $ROSI_a$ values to calculate the investment must do to meet the security requirements detrimental to the client, for example, metrics "1.3" and "1.6" need 100% investment to meet customer needs, i.e., double the amount invested in the process security controls.

5. RELATED WORK

For obtaining the ROSI, none of the existing approaches propose a set of metrics that focuses on security controls and applied computing platforms in the cloud. Some works on ROSI include targeted reviews based on cost [24, 22, 4, 23].

A comparative and quantitative analysis of the current taxonomy for cloud computing is presented by [13].

The following standards, tools, recommendations and references may be useful in the ROSI calculation process: Information Systems Audit and Control Association (ISACA) presents [1, 2]; Cloud Security Alliance (CSA) presents [5, 6]; National Institute of Standards and Technology (NIST) presents [3]; European Network and Information Security Agency (ENISA) presents [10, 11]; International Organization for Standardization (ISO) presents [16, 17]. None of the above surveys cover security oriented metrics, and neither are they specifically designed to assess the cloud computing controls offered by CSPs.

6. CONCLUSION AND FUTURE WORK

In this work, we proposed a new quantitative and qualitative methodology for obtaining the Return On Security Investment for a specific deployment profile through the use of security metrics. The proposal covers the services offered by the cloud computing providers from a client security perspective. Furthermore, this approach has the advantage of supporting a hierarchical decomposition and also presents a solution to deal with intangible costs and benefits, thereby allowing for distributed and scalability features.

As for future work, there is the need to automatically convert the client-approved document (Implementation Profile) to a Security-SLA, in order to formalize the security services according to the chosen requirements. One also needs to try and automate the analysis and configuration of value mapping (0–4) for each security metrics, which currently holds the model dependent on human intervention. Moreover, monitoring the Security SLA-based security metrics needs to be tackled more deeply, so that proper QoS over security requirements using $ROSI_{a,vi,vf}$ may be obtained, thus allowing for minimizing security violations of the Security-SLA. All these should contribute to a greater engagement to the cloud environment.

Acknowledgment

The authors would like to thank CAPES and Fundect (Process #23/200.308/2009) for his financial support.

7. REFERENCES

[1] I. S. Audit and C. A. (ISACA). It control objectives for cloud computing: Controls and assurance in the cloud. Technical report, 2014.

[2] I. S. Audit and C. A. (ISACA). Security considerations for cloud computing. Technical report, 2014.

[3] L. Badger, T. Grance, R. Patt-Corner, and J. Voas. Cloud computing synopsis and recommendations. Technical report, National Institute of Standards and Technology, May 2012.

[4] V. Chang, G. Wills, R. J. Walters, and W. Currie. Towards a structured cloud roi: The university of southampton cost-saving and user satisfaction case studies. *Sustainable ICTs and Management Systems for Green Computing*, pages 179–200, 2012.

[5] C. S. A. (CSA). Security guidance for critical areas of focus in cloud computing v2.1. Technical report, 2014.

[6] C. S. A. (CSA). Security, trust & assurance registry (star). Technical report, 2014.

[7] C. A. da Silva and P. L. de Geus. An approach for security-sla in cloud computing environments. *Proceedings of the IEEE Latin-America Conference on Communications (LatinCOM'14)*, pages 1–6, 2014.

[8] C. A. da Silva and P. L. de Geus. Arquitetura de monitoramento para security-sla em nuvem computacional do tipo saas. *Proceedings of the XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG'14)*, 2014.

Table 1: Deployment Profile (Portfolio of Infrastructure metrics)

Id	Description	EM	EV	$ROSI_a$	$ROSI_{vi}$	$ROSI_{vf}$
1.	**Firewall**					
1.1	Average time vulnerabilities are patched	4	3	1	0,20	0,25
1.2	Security event records	3	2	1	0,25	0,33
1.3	Application Software Security Threat Level	2	3	-1	-0,33	-0,25
1.4	Packet filtering	3	2	1	0,25	0,33
1.5	Mean time between failures	4	3	1	0,20	0,25
1.6	Mean time between maintenance	3	4	-1	-0,25	-0,20

Table 2: Deployment Profile (Portfolio of metrics for a Service)

Id	Description	EM	EV	$ROSI_a$	$ROSI_{vi}$	$ROSI_{vf}$
3.	**PostgreSQL Database**					
3.1	Default TCP port	2	2	0	0	0
3.2	Default user service account	3	2	1	0,25	0,33
3.3	Insecure user account	2	1	1	0,33	0,50
3.4	Mean time to verify latest security patches	3	2	1	0,25	0,33
3.5	SQL injection	4	3	1	0,20	0,25

Table 3: Necessary Investment (Portfolio of Infrastructure metrics)

Id	Description	$ROSI_a$	Cost	Investment
1.	**Firewall**			
1.3	Application Software Security Threat Level	-1	8,000	16,000
1.6	Mean time between maintenance	-1	5,000	10,000

[9] C. A. da Silva, A. S. Ferreira, and P. L. de Geus. A methodology for management of cloud computing using security criteria. *Proceedings of the IEEE Latin American Conference on Cloud Computing and Communications (LatinCloud'12)*, pages 49–54, 2012.

[10] ENISA. Cloud computing: Benefits, risks and recommendations for information security. Technical report, European Network and Information Security Agency (ENISA), November 2009.

[11] ENISA. Introduction to return on security investiment. Technical report, European Network and Information Security Agency (ENISA), December 2012.

[12] I. Foster, Y. Zhao, I. Raicu, and S. Lu. Cloud computing and grid computing 360-degree compared. *Grid Computing Environments Workshop (GCE'08)*, pages 1–10, 2008.

[13] N. Gonzalez, C. Miers, F. Redigolo, M. Simplicio, T. Carvalho, M. Naslund, and M. Pourzandi. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, SpringerOpen Journal*, 11(1), 2012.

[14] L. Hayden. *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*. McGraw-Hill Osborne, 2010.

[15] D. S. Herrmann. *Complete guide to security and privacy metrics*. Auerbach Publications, 2007. ISBN: 0-8493-5402-1.

[16] ISO/IEC-27017:2014. Information technology - security techniques - code of practice for information security controls based on iso/iec 27002 for cloud services (draft). Technical report, 2014.

[17] ISO/IEC-27018:2014. Information technology - security techniques - code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors. Technical report, 2014.

[18] B. Johnson and Y. Qu. A holistic model for making cloud migration decision: A consideration of security, architecture and business economics. *10th International Symposion on Parallel and Distributed Processing with Applications*, pages 435–441, 2012.

[19] M. Kantarcioglu, A. Bensoussan, and S. C. Hoe. Impact of security risks on cloud computing adoption. *49th Annual Allerton Conference on Communication, Control, and Computing*, pages 670–674, 2011.

[20] B. Martens and F. Teuteberg. Decision-making in cloud computing environments: A cost and risk based approach. *Information Systems Frontiers*, 14(4):871–893, 2012.

[21] S. C. Payne. A guide to security metrics. Technical report, SANS Institute, July 2006.

[22] L. B. A. Rabai, M. Jouini, M. Nafati, A. B. Aissa, and A. Mili. An economic model of security threats for cloud computing systems. *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec'12)*, pages 100–105, 2012.

[23] W. Sonnenreich, J. Albanese, and B. Stout. Return on security investment (rosi) - a practical quantitative model. *Journal of Research and Practice in Information Technology*, pages 55–66, 2006.

[24] N. Tsalis, M. Theoharidou, and D. Gritzalis. Return on security investment for cloud platforms. *IEEE International Conference on Cloud Computing Technology and Science*, pages 132–137, 2013.