2010 Sixth International Conference on Networking and Services

SLA Perspective in Security Management for Cloud Computing

Shirlei Aparecida de Chaves, Carlos Becker Westphall and Flavio Rodrigo Lamin
Network and Management Laboratory - LRG
Federal University of Santa Catarina, Florianópolis – Santa Catarina – Brazil
{shirlei, westphal, lamin}@inf.ufsc.br

***Abstract*— One of the network and services management problems is security, either in preventing attacks and using computational mechanisms to protect data and systems or in administrative matters, which involves not just what needs to be protected, but also what security service levels will be delivered. This paper explores Service Level Agreements for Security or just Sec-SLAs. Is tried to provide an overview on the subject, the difficulties faced during the security metrics definition process and the Sec-SLA monitoring, as well as an analysis on the Sec-SLA role in new paradigms like cloud computing.**

Keywords - network and security management; security metrics; security service level agreement; cloud computing security

I. Introduction

Control systems and data security are important in any computer system. This demand can be covered by creating new devices or techniques and by making some adjustments in traditional ways of storing and controlling systems and data. In this sense, this paper studies Security Service Level Agreements or just Sec-SLAs not as a brand new technique, but as a new design for the traditional Service Level Agreements or SLAs. Instead of considering traditional service levels like network throughput or delay, for example, it considers just service levels related to security.

The present paper explores Sec-SLAs and discusses some aspects of defining security metrics. Although the subject was already largely studied, new paradigms like cloud computing bring a new view on it, either in the management of services field, as in the establishment of what are the main security aspects to be covered. In this sense, a four-step process is presented to be used when specifying Sec-SLAs for cloud computing as also are presented some security metrics suitable for cloud computing environments.

Given this introduction, the remaining of this paper is organized as follows. In Section 2, related work is analyzed. In Section 3, what is a Sec-SLA is presented in more details. In Section 4, a brief discussion on defining security metrics is presented. In Section 5, some directions on how to generate Sec-SLAS for services being migrated to the cloud are analyzed and discussed. In Section 6, we try to contribute to the discussion, by analyzing issues related to how secure an infrastructure to manage these contracts should be. In Section 7, the conclusion and future work are presented.

II. Related Work

Sec-SLAs and security metrics were studied by [1][2][3][4][5]. In [3], the term Sec-SLA is analyzed considering the question: "how to accurately delineate security in a SLA context?" As a result, [3] builds three steps to be followed while developing Sec-SLA metrics:

a) Policy Analysis: any data available in the enterprise that could give support to create Sec-SLAs can be evaluated in this step. It could be data related to guidance's and policies, for example.

b) Architecture Analysis: in the previous step, a set of preliminary service level agreement categories was obtained. Now, when possible, these categories are applied in an architecture analysis activity. The objective is to analyze the customer's infrastructure and to find the requirements that could be met directly into elements like web servers and firewalls. This analysis also helps to formulate the questions to be used in the next step.

c) Interviews: to collect on what are the security concerns in the user's point of view.

After these steps, the results can be processed, in order to check if the categories obtained can be used as final categories or if some of then can be grouped. The refined list of categories can be used in the Sec-SLA.

In [5], whose work has its basis on [3], there is a contribution to the writing of Sec-SLAs, by defining and validating metrics to be used in such contracts. In order to obtain the security metrics, [5] applied the steps proposed in [3], using as working scenario the network of the Department of Informatics and Statistics, at the Federal University of Santa Catarina (INE-UFSC). In [1], the metrics obtained in [5], are restructured in order to be aligned with International Security Standards.

However, establishing a Sec-SLA is not sufficient. Monitoring the Sec-SLA is fundamentally important too. According to [5] it is also complex, "because the agent-manager approach normally used in the monitoring of other kinds of SLA, does not fit easily to every security characteristic". However, this issue remains uncovered in [3] and [5]. In [2], the monitoring problem is focused through a definition of a security service level agreement monitoring and controlling architecture, called Sec-Mon.

III. What is a Sec-SLA?

The SLA as it is commonly known, is usually defined as in

978-0-7695-3969-0/10 $26.00 © 2010 IEEE
DOI 10.1109/ICNS.2010.36

IEEE computer society

[10]: "(…) *a formal negotiated agreement between two parties. It is a contract that exists between the Service Provider (SP) and the Customer. It is designed to create a common understanding about service quality, priorities, responsibilities, etc.*"

According to the above definition service level is a key concept. But what is a service in the context of a SLA? In this case, the answer is: it depends on the SLA. In [11], is pointed that "*although these contracts usually cover the services telecommunications carriers provide to corporate customers, they can also include the services a company's IT (Information Technology) department provides to other business units within the organization*." In [12], the concept of service is used as in ITIL[1]: one or more IT systems that enable a business process. The authors in [12], emphasize that we should take into account that an IT system is a combination of hardware, software, skills, process and people. In this paper, we use the same concept of service as in [12].

Considering the importance of computer systems security, its intricate characteristics and the growing of outsourcing scenarios, including the outsourcing of security services, security service levels need to be agreed in a separate Service Level Agreement. Thus, a Sec-SLA is a specific SLA that deals with metrics related to security instead of the traditional telecommunication metrics such as throughput, delay, packet loss and other similar metrics.

The service level security requirements or demands, like indicated in [13], are later converted in a set of mechanisms, including cryptography, data packet filtering, redundancy of hardware and software, etc.

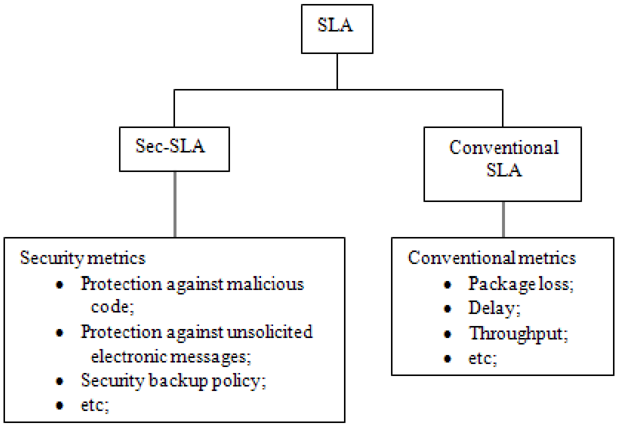

Figure 1. Sec-SLA X Conventional SLA

In Figure 1, the differences between a Sec-SLA and a conventional SLA are summarized. In the next section we work the concept of security metrics and the difficulties faced during their definition.

IV. DEFINING SECURITY METRICS

The definition of the term metric is a little vague, especially when referring to IT area. This vagueness, as said in [6], is due to the fact that the term is used in several situations, related to a variety of properties, varying from a service performance to a process maturity. In [7], is also pointed that this vagueness is challenging when designing proper security metrics. Several authors agree that being quantifiable and measurable are essential metric attributes [4][5] [6][7][14].

When designing security metrics, this challenge is a main concern too. The definition of a security that can be quantifiable and can be expressed in a service level is a hurdle to be overcome. This concern, indicated in other points of the present paper, was one of the main questions in [3][5]. Much research is being done to facilitate the process of designing such metrics, like in [1][6][7][8][9].

In [1], a step further is given, aligning the security metrics obtained in [4], to met international security information standards, like ISO/IEC 17799:2005 (now known as ISO/IEC 27002). The concern with international standards is especially important if we consider that many of the organizations that could implement a Sec-SLA could also be in some certification process.

In Table I, some metrics, as seen in [5], are transcript to provide a better overview on possible security metrics.

TABLE I. SECURITY METRICS EXAMPLES [5]

Metric	Description
Password Management	Presents, for example, how often passwords should be changed, password format.
Backup policies	Presents how often backups are made, how is stored and for how long.
Repair time	How long it takes to the IT team put the system on in a failure situation.

V. SEC-SLAS IN THE CLOUD

Changes occurred in the traditional distributed computing paradigm lead to the need of enforcements in the traditional SLAs. The more recent is the notion of "computing in the cloud". The popular term for this new computing model is cloud computing. There is no clear consensus on what exactly cloud computing is, but several authors, like [14][15] and [16], outline the fact that it is a new distributed computing and business paradigm, that provides computing power, software and storage and even a distributed data center infrastructure on demand, delivered over the Internet. The key words in the previous definition are *on demand*. Services delivered in such conditions demand considerable effort in the process of defining security service levels.

The definition of security metrics, as well as its monitoring, has to be done on demand as well. The negotiation of the SLA will have to be agile, in order to not affect the hiring of services, as one of the greatest appeals of cloud computing is to allow unexpected demands to be met more quickly.

The security problem in cloud computing raises many questions, especially from customers, who need to understand the risks associated when migrating services to the cloud, as well as to know what are the ways available to ensure that the

[1] ITIL: Information Technology Infrastructure Library

security of such data will be maintained.

Several recent work in cloud computing cites the importance of negotiating SLAs. For instance, The Cloud Security Alliance [17], whose formal debut was made at RSA Conference 2009 releasing a white paper entitled *Security Guidance for Critical Areas of Focus in Cloud Computing*, points the fact that more consideration should be given to the content of the SLA, considering its 'auditability' [17]. In [18], is pointed that to become a viable alternative to the enterprise, cloud computing infrastructures need to provide stable service level for business process. It is also pointed that "in cloud computing environments SLAs are typically provided for basic platform services (e.g., system uptime, network throughput) [18]." The same characteristic was already indicated in a previous topic in the present paper and is the motivation for having the security service levels treated in a separated SLA, that we call Sec-SLA.

Due to its nature, cloud computing has several types of uses, i.e., one might be computing in the cloud when creating a datasheet in Google Docs, as well as when hiring a server in a data center to any enterprise purpose. Some cloud computing categorization was done, trying to differentiate these use possibilities, according to the main objectives of use. The categories more indicated in cloud computing related work are the three following, reproduced in this section like the definition given in [19].

A. Infrastructure as a Service (IaaS)

Products in this case "deliver a full computer infrastructure via the Internet [19]."

B. Platform as a Service (PaaS)

In this case, is offered "a full or partial application development environment that users can access and utilize online, even in collaboration with others [19]."

C. Software as a Service (SaaS).

In this case, is provided "a complete, turnkey application—including complex programs such as those for CRM or enterprise-resource management via the Internet [19]."

The steps proposed in [3] are suitable as an approach to derive security service levels for services being migrated to the cloud. Even considering the fact that the Sec-SLA generation and negotiation should be dynamic, as mentioned earlier in this paper, in a scenario where the organization intends to move services or process to the cloud, a first analysis aiming to discover the organization security needs relating to these services or process will have to be done. If the organization already has these security requisites well known and documented, the analysis could jump to a refinement, considering particularities of the cloud computing category to be used. Below is described these steps, considering a scenario of services or process being migrated to a cloud provider.

A. Policy Analysis

In this phase, will be analyzed the available documentation in the organization and maybe in the field where the organization has its activities, like customers' contracts, national regulations, internal policies and so on.

Intended results:

- An initial list of security service categories for the Sec-SLA. This step must be done by the organization, because it is a particular survey, i.e., although some generalization is possible, each organization has its particularities related to security needs.

B. Architecture Analysis

Considering that cloud computing has many categories of use and each category has its own particularities, the organization should know, at least in a first moment, which type is intended. The definition of what category is more suitable for the organizations needs is done in another phase and is not on the scope of the present work. With the preliminary security service categories collected in the policy analysis step, in the architecture analysis phase will be analyzed which of these categories could be directly mapped to the category of cloud computing intended. It would be also possible to analyze security mechanisms owned by the organization that could be migrated to the cloud as well (identity management, for example).

Documents that could be helpful in this phase are any available diagrams like network maps, software architecture diagrams, process diagrams, etc.

Intended results: a refined list of security categories for the Sec-SLA, as well as questions to be made in the interview phase.

C. Interviews

In this phase, interviews with people related to the services that will be migrated to the cloud will be made. The questioning will be driven to specific questions about topics of the SLA to be generated. Many of the questions were already formulated in the previous step, the architecture analysis, aiming to collect more details on specific topics.

D. Negotiation

If there is a negotiation in place with some cloud computing provider, in this phase the security service levels will be negotiated. If there is not, it will be necessary to check with the possible providers which of them offers support for negotiating security service levels. If the list of security service levels built in the previous steps is mandatory, providers that do not offer security service level negotiation will be eliminated. As pointed in [17], many cloud providers include service level agreements in their online contracts, already defining how the services will be delivered, what makes it potentially non-negotiable.

In a research previously made by us, a list of the main customer' security concerns were collected. These concerns are summarized in Table II.

TABLE II. MAIN CUSTOMER' SECURITY CONCERNS RELATED TO CLOUD COMPUTING

Customers' security concern	Motivation
Vulnerability to attack / data breaches	Critical business information and IT resources are outside the customers firewall.
Standard security practices / regulatory compliance	If the cloud provider has some sort of security certification or external audits.
Conformance to state or national data-storage / privacy laws	In the cloud, data can be anywhere, being important to know and to follow the local regulations.
Privileged user access	The personnel control will not be made just by the customer. Other users, from the cloud provider, may have access to the customer's data.
Data segregation	In a cloud, the environment is shared, resulting in the need of strong schemes to separate users' data.
Recovery	The provider capacity of restoring the entire system and how long it would take.
Investigative support	If it will be possible to investigate inappropriate or illegal activities.
Long-term viability	If the data will be available and in a format that will allow being imported to a substitute application, in the case of the cloud provider goes broke or is acquired by another provider.

Table II could be an initial guide if the customer does not know from where to start the investigation, as it well summarize general security problems of cloud computing.

Is worth to remember that SLAs main focus is characteristics related to the quality of service being delivered. However, giving some aspects already pointed, like the location of resources (that could be in any country), some legal aspects should be addressed in the Sec-SLA. In this sense, an interchange of expertise is needed. Actually, some research is already being done by the legal area. A recent seminar, entitled "Cloud Computing: Managing the Legal Risks"[2], aimed to address the current and emerging legal risks for business using cloud computing. Probably one of the most important aspects in this matter is about jurisdiction. The customer needs to obey the laws of its own country, as also the laws of the country where its data is being stored. A big question in this subject is: what if we have a conflict of law?

Another important aspect to be considered is that, despite of being a contract of virtual services, those services will be deployed and maintained in a physical location. Knowing how secure such facility is could be vital for business. Special attention should be paid to disaster recovery plans and physical access controls. In most of cases the customer may not be able to personally check such cloud provider controls, but they should be covered in some part of the contract.

In Table III, considering the Recovery concern mentioned in Table II, is made a list of what could be possible security metrics for service levels of a category that was called *Backup Planning*. The minimum level acceptable is shown in the table as level 3 (three) and the maximum level as 1 (one).

TABLE III. SECURITY METRICS FOR BACKUP PLANNING

Security Metric	**Service Level**		
Backup Planning	***1 (max)***	***2***	***3 (min)***
Backup frequency	Hourly	Twice a day	Daily
Backup location	A dedicated backup server, replicated.	A dedicated backup server	The backup should be done by the client
Backup format	Any chosen by the client	A specific open format agreed by both	Any open format
Backup restore time	30 minutes	1 hour	2 hours

VI. MONITORING THE SEC-SLA

Having the customer reached an agreement with the cloud provider, through a Sec-SLA, there is another important step: to monitor if the security metrics are being met.

In Figure 2, is shown a general overview of the architecture proposed by [2] for monitoring and controlling Sec-SLAs, called Sec-Mon.

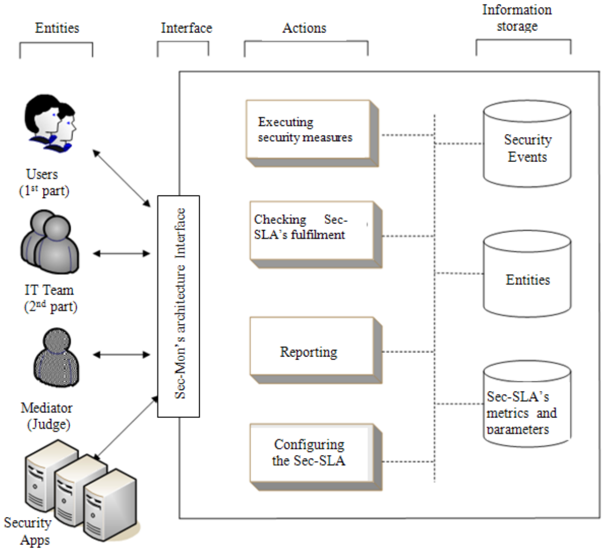

Figure 2. Sec-Mon's architecture general overview [2].

A. *Sec-Mon architecture security aspects*

Architectures like Sec-Mon [2] represent a contribution in the search for ways to monitor and control a Sec-SLA. However, it is necessary to secure the architecture itself, because even when used in an intracompany environment, it can be a weak point in the Sec-SLA monitoring process.

When deployed, the architecture will involve not just software and hardware devices, but also people and process, all of them fail and misuse-prone (intentional or not). Thus, this architecture has to be analyzed against to some security principles, like for example, integrity, privacy, availability,

[2] More details available at http://www.straffordpub.com/products/cloud-computing-managing-the-legal-risks-2009-12-09

authenticity and non-repudiation.

In Table IV, we summarize an analysis of this architecture according to each security principle indicated in the previous section, considering the main issues that should be addressed in each one.

TABLE IV. SEC-MON ARCHITECTURE ANALYSES ACCORDING TO SOME SECURITY PRINCIPLES

Security Principle	Why	Main issues
Integrity	Considering specially the legal aspect of a Sec-SLA, it is essential that all the data involved, like metrics and collected data to analyze the service conformance to these metrics are not compromised.	What are the assurances on keeping the validity of data?
Privacy	When it comes to security, privacy is always an important issue.	Which data should be private in the architecture? How is protected the privacy of individually identifiable information?
Availability	Availability is also crucial to guarantee the access to the data already collected to analyses, as also to collect new ones.	How is guaranteed the architecture availability?
Authenticity	All the security metrics and collected data need to be inserted in the architecture by someone authorized to.	How are the users authenticated and their access controlled?
Non-repudiation	Every known user of the system should have their actions traceable to them and not be able to refuse their authoring.	Are the users of the architecture able to deny their actions?

Finalizing the monitoring section, one more question is needed:

- Who will be responsible for this monitoring? The customer? The cloud provider? A third party?

VII. CONCLUSION AND FUTURE WORK

A Sec-SLA is a formal negotiated document that defines in, specially, a quantitative way what service levels will be delivered from the provider to the customer. In other words, the Sec-SLA deals with the “what”, not the “how”. However, by defining good security metrics (in the terms defined in section IV), the “how” could be better visualized. Usually the IT team faces lots of options in technological solutions and having a clear and documented understanding of what are the security requirements certainly would help. One of the main advantages of a Sec-SLA, beyond the legal one, is the possibility of a better understanding of how security is being accomplished.

It was also possible to notice that many research is being done focusing on the security metric subject. Fortunately, security metrics are of great concern in more areas than network and services management and much of the effort done to improve their definition and measurability is useful in a Sec-SLA context.

Proposed architectures like Sec-Mon represent an important subsidy in the search for ways to monitoring and controlling the Sec-SLA. The general overview shown in Figure 2 is conceptual, i.e., the Sec-Mon architecture is independent of a specific technology and even that in the moment of its construction was not considered the cloud computing paradigm, it could easily be adapted to provide means of being deployed in a cloud environment.

Finalizing, a research to pre-design security metrics according to the cloud computing category, aiming to help the need for dynamic negotiation of Sec-SLAs in the cloud is in place. It is a great challenge because the paradigm is still evolving, as well as the understanding of what are the security challenges that it brings.

REFERENCES

[1] P. R. Barbosa, R. R. Righi and D. L. Kreutz, “Defining Metrics to Sec-SLA Agreements in Conformance to International Security Standards,” in: XXXIII Latin American Informatics Conference, San José, Costa Rica, 2007, v. 1. pp. 36-47. *Original in Portuguese.*

[2] R. R. Righi, D. L. Kreutz and C. B. Westphall, “Sec-Mon: An Architecture for Monitoring and Controlling Security Service Level Agreements”, in: XI Workshop on Managing and Operating Networks and Services, pp. 73-84. SBC Press, Porto Alegre (2006). *Original in Portuguese.*

[3] R. R. Henning, "Security service level agreements: quantifiable security for the enterprise?" in *NSPW '99: Proceedings of the 1999 workshop on New security paradigms*. New York, NY, USA: ACM, 2000, pp. 54-60. [Online]. Available: http://dx.doi.org/10.1145/335169.335194

[4] C. Irvine and T. Levin, "Quality of security service," in *NSPW '00: Proceedings of the 2000 workshop on New security paradigms*. New York, NY, USA: ACM, 2000, pp. 91-99. [Online]. Available: http://dx.doi.org/10.1145/366173.366195

[5] R. R. Righi, F.R. Pelissari and C.B. Westphall, “Sec-SLA: Specification and Validation of Metrics to Security Service Level Agreements”, in: IV Workshop on Computer System Security, pp. 199–210. SBC Press, Porto Alegre , 2004. *Original in Portuguese.*

[6] I. Kocsis, G. Csertán, P. L. Pásztor and A. Pataricza, "Dependability and security metrics in controlling infrastructure," in *SECURWARE '08: Proceedings of the 2008 Second International Conference on Emerging Security Information, Systems and Technologies*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 368-374. [Online]. Available: http://dx.doi.org/10.1109/SECURWARE.2008.62

[7] U. Premaratne, J. Samarabandu, T. Sidhu, B. Beresh and J.-C. Tan, "Application of security metrics in auditing computer network security: A case study," in 4th International Conference on Information and Automation for Sustainability,February 2009, pp. 200-205. [Online]. Available: http://dx.doi.org/10.1109/ICIAFS.2008.4783996

[8] R. Savola, "Towards a security metrics taxonomy for the information and communication technology industry," in *ICSEA '07: Proceedings of the International Conference on Software Engineering Advances*. Washington, DC, USA: IEEE Computer Society, 2007, p. 60. [Online]. Available: http://dx.doi.org/10.1109/ICSEA.2007.79

[9] R. J. Robles, Y.-S. Jeong, J. H. Park and T.-h. Kim, "Strategy for it security in e-enterprise environment," in 2008 International Symposium on Ubiquitous Multimedia Computing, October 2008, pp. 214-217. [Online]. Available: http://dx.doi.org/10.1109/UMC.2008.50

[10] “Service Level Agreement / Quality of Service Overview”, TM Forum. [Online]. Available: http://www.tmforum.org/browse.aspx?catID=2016&linkID=29209. Last access: Dec. 05, 2009.

[11] N. J. Muller, "Managing service level agreements," *Int. J. Netw. Manag.*, vol. 9, no. 3, pp. 155-166, 1999. [Online]. Available:

http://dx.doi.org/10.1002/(SICI)1099-1190(199905/06)9:3%3C155::AID-NEM317%3E3.3.CO;2-D

[12] I. L. Magalhães and W. B. Pinheiro, "IT Services Management in Pratics: An Approach based on ITIL", Novatec, São Paulo, 2007. *Original in Portuguese*

[13] G. C. M. Moura and L.P. Gaspary, "A Proposal for Measuring the Complexity of Security", in 8th Brazilian Symposium on Information and Computer System Security. Gramado, Brazil, 2008. *Original in Portuguese*.

[14] T. Heyman, R. Scandariato, C. Huygens and W. Joosen, "Using security patterns to combine security metrics," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, May 2008, pp. 1156-1163. [Online]. Available: http://dx.doi.org/10.1109/ARES.2008.54

[15] L. Mei, W. K. Chan and T. H. Tse, "A tale of clouds: Paradigm comparisons and some thoughts on research issues," in *APSCC '08: Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 464-469. [Online]. Available: http://dx.doi.org/10.1109/APSCC.2008.168

[16] I. Foster, Y. Zhao, I. Raicu and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE '08*, 2008, pp. 1-10. [Online]. Available: http://dx.doi.org/10.1109/GCE.2008.4738445

[17] "Security guidance for critical areas of focus in cloud computing," Cloud Security Alliance, Tech. Rep., April 2009. [Online]. Available: http://www.cloudsecurityalliance.org/guidance/csaguide.pdf .Last access: Dec. 05, 2009.

[18] V. Stantchev and C. Schröpfer, "Negotiating and enforcing qos and slas in grid and cloud computing," in *GPC '09: Proceedings of the 4th International Conference on Advances in Grid and Pervasive Computing*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 25-35. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-01671-4_3

[19] N. Leavitt, "Is cloud computing really ready for prime time?" *Computer*, vol. 42, no. 1, pp. 15-20, January 2009. [Online]. Available: http://dx.doi.org/10.1109/MC.2009.20.