Survey: Risk Assessment for Cloud Computing

Drissi S.
Computer Lab and Renewable Energy Systems (CLRES)
University Hassan II Aïn Chock. ENSEM
Casablanca, Morocco

Houmani H. and Medromi H.
Computer Lab and Renewable Energy Systems (CLRES)
University Hassan II Aïn Chock. ENSEM
Casablanca, Morocco

***Abstract*—with the increase in the growth of cloud computing and the changes in technology that have resulted a new ways for cloud providers to deliver their services to cloud consumers, the cloud consumers should be aware of the risks and vulnerabilities present in the current cloud computing environment. An information security risk assessment is designed specifically for that task. *However, there is lack of structured risk assessment approach to do it*. This paper aims to survey existing knowledge regarding risk assessment for cloud computing and analyze existing use cases from cloud computing to identify the level of risk assessment realization in state of art systems and emerging challenges for future research.**

Keywords—cloud computing; risk; risk assessment approach; survey; cloud consumers

I. Introduction

With the advancement in cloud technologies and increasing number of cloud users, businesses also need to keep up with the existing technology to provide real business solutions [1]. In addition, predictions for growth indicate massive developments and implementations of cloud computing services, including that the cloud computing services market is likely to reach between $150 billion in 2014 [29-30] and $222.5 billion in 2015 [31]. From the business perspective, cloud computing becomes one of the key technologies that provide real promise to business with real advantages in term of cost and computational power [2]. In spite of the advancement in cloud technologies and increasing number of cloud users, Cloud computing being a novel technology introduces new security risks [22] that need to be assessed and mitigated. consequently, assessment of security risks [17] is essential , the traditional technical method of risk assessment which centers on the assets should give way to the business focused on the specific nature of cloud computing and on the changes in technology that have resulted a new ways for cloud providers to deliver their services to cloud consumers.

The major contributions of this survey can be summarized as follows:

a) We investigate the existing knowledge regarding risk assessment for cloud computing.

b) Further, we also present a risk assessment requirement that can be used by a prospective cloud consumers to assess the risk in cloud computing.

The rest of the paper is organized as follows: Cloud computing and concepts of risk assessment are summarized in Section 2. In Section 3, we are investigated the major paradigms of risk assessment in cloud computing. New researches requirements for risk assessment in cloud computing environment are discussed in Section 4. Finally, the survey concludes with the open challenges of risk assessment in cloud computing environment in Section 5.

II. Fundamental Concepts

A. Cloud computing

In literature, there are many definitions for cloud computing. The National Institute of Standards and Technology(NIST) [4] defines cloud computing as ‘‘a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction’’. European Community for Software and Software Services (ECSS) [5] explains it as the delivery of computational resources from a location other than your current one.

Cloud can be categorized into three delivery models classified according to their uses; Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). Cloud Software as a Service (SaaS) which deliver software over the Internet (e.g. Salesforce CRM, Google Docs, etc), Cloud Platform as a Service which mainly offer virtualized execution environments to host Cloud services (e.g. Microsoft Azure, Force and Google App engine) and Cloud Infrastructure as a Service which provide virtualized computing resources as a service (e.g. Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydive and Rackspace Cloud).

Four deployment models have been identified for cloud architecture solutions: Private cloud: a cloud platform is operated for specific organization, Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns, Public cloud: a cloud platform available to public users to register and uses the available infrastructure. Hybrid cloud: a private cloud that can composite two or more clouds (private, community or public).

B. Risk assessment

“Risk in itself is not bad, risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity” [28].

Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives. According to the introduction to ISO 31000 2009, the term risk management also refers to the architecture that is used to manage risk [6]. Risk assessment is one step in the process of risk management.

Risk assessment is the process of identifying the security risks to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact. The main objective of risk assessment is to define appropriate controls for reducing or eliminating those risks.

Generally there are four steps of risk assessment. The four steps are as follow [7]:

1) Threat Identification

This first step identifies all potential threats to the system. It allows identifying the potential threat sources and develops a list of a threat statement that is potential threat sources that are applicable to the system.

2) Vulnerability Identification

In the second step, the goal of vulnerability identification is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

3) Risk Determination

In the third step, the purpose of risk determination is to assess the level of risk to the system.

4) Control Recommendation

In the fourth step, the goal is to purpose some controls that could mitigate or eliminate the identified risks, as appropriate to the system organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the system.

Risk analysis methods are generally divided into qualitative analysis and quantitative analysis:

Quantitative Risk Methodologies**:** Although there are many well-developed industries that use quantitative risk, it is not commonly used in information technology. In fact, it is very rare indeed. However, risk methodologies can be partially quantitative and partially qualitative. It is the position of this author however to categorize all of the major methodologies as essentially qualitative because none of them can produce ALEs that can credibly be used to measure specific costs versus benefits as quantitative risk analysis should. They instead provide a more general sense of cost versus benefit despite sometimes having aspects which are predominantly quantitative, such as incident statistics [20].

Qualitative Risk Assessments**:** approach describes likelihood of consequences in detail. This approach is used in events where it is difficult to express numerical measure of risk. It is, for example, the occurrence without adequate information and numerical data. Such analysis can be used as an initial assessment to recognize risk [34]. The following are some of the major risk assessment methodologies available today:

· EBIOS [8]
· OCTAVE [9]
· MEHARI [10]

Some are publicly available (e.g. OCTAVE), while others are restricted to members of organizations that are collaborating to create and updated them (e.g. SPRINT). The following are brief descriptions of each of these methodologies.

The method to assess risks is generally composed of the four following steps: thread identification, vulnerability identification, risk determination and control recommendation. These four steps of risk assessment are based on practical experiences in security assessment. These steps come from best practices that have been applied by many organizations for security assessment (e.g. EBIOS, MEHARI and OCTAVE).

The EBIOS [8] (Expression of Needs and Identification of Security Objectives) is a method for assessing and treating risks, which aims to determine the security actions to implement and also expressions safety.

OCTAVE [9] (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a method of assessment of vulnerabilities and threats on the basis of the operating assets of the company.

MEHARI [10] is a risk assessment method in the context of the security of information systems; this method is designed to meet the needs of each company.

These tools have not been designed specifically for cloud environments. In traditional IT environments, everyone in the business has to go to the IT department to obtain IT related services. However, for cloud computing, the risk assessment become more complex, there are several issues that are likely emerged. Among them is the question of multi-tenancy that means the data may be located at several geographically distributed nodes in the cloud and the control over where the processes actually run and where the data reside.

Existing risk assessment methods and standards (ISO/IEC 27001, ISO/IEC 27005, and EBIOS) are generally focused on structuring the different steps and activities to be performed. Their added value also depends on the knowledge bases of risks [24], [25], [26] and security requirements [24], [26] they require. They are the input to the activities performed. The methodological aspects are thus generally rigorous because, they build on a well defined process and structure to be followed.

III. Literature Review

A. Risk assessment for conventional system

Risk assessment has been discussed by many researches in different area. In [38], a risk assessment method has been discussed for Smartphone; this method describes a method for risk assessment that is tailored for Smartphone. The method does not treat this kind of device as a single entity. Instead, it identifies Smartphone assets and provides a detailed list of specific applicable threats. For threats that use application permissions as the attack vector, risk triplets are facilitated.

The triplets associate assets to threats and permission combinations. Then, risk is assessed as a combination of asset impact and threat likelihood. The method utilizes user input, with respect to impact valuation, coupled with statistics for threat likelihood calculation.

In [36], this paper proposes a method for a probabilistic model driven risk assessment on security requirements. The security requirements and their causal relationships are represented using MEBN (Multi-Entities Bayesian Networks) logic that constructs an explicit formal risk assessment model that supports evidence-driven arguments.

Several quantitative risk assessment methods exist. In [35], they propose a SAEM method which is a cost-benefit analysis process for analyzing security design decisions based on the comparison of a “threat index”. However, it is based on some impractical assumptions. In [23] they propose security ontology for organizing knowledge on threats, safeguards, and assets. This work constructs classification for each of these groups and creates a method for quantitative risk analysis, using its own framework. The work does not use known standards or guidelines as an input for its evaluation model, so desired mechanisms and countermeasures have to be defined in the process of risk analysis. Quantitative risk-based requirements are reasoning in [21] uses PACT as a “filter” arranged in series to find out a proportion of likelihood or the impact of risk factor. However, it lacks the ability to represent the impacts among multiple risk factors. The SSRAM model in [3] provides a prioritization that helps in determining how the risks identified will be addressed in different phases of software development. However, it lacks a baseline for systematically identifying potential risks and reasoning about their relationships and interactions in a real operational environment.

In [37], a novel approach is proposed, in which Analytic Hierarchy Process (AHP) and Particles Swarm Optimization (PSO) can be combined with some changes, is presented. The method consists of; firstly, the analytic hierarchy structure of the risk assessment is constructed and the method of PSO comprehensive judgment is improved according to the actual condition of the information security. Secondly, the risk degree put forward is PSO estimation of the risk probability, the risk impact severity and risk uncontrollability. Finally, it gives examples to prove that this method Multi Objectives Programming Methodology (MOPM) can be well applied to security risk assessment and provides reasonable data for constituting the risk control strategy of the information systems security.

B. *Risk assessment for cloud computing*

In recent years, the principles and practices of risk assessment/management were introduced into the world of utility computing such as Grid and Clouds either as a general methodology [40][41][42][16][43][46] or a focus on a specific type of risk, such as security [45] and SLA fulfillment [44][13].

European Network and Information Security Agency (ENISA) released cloud computing Risk Assessment report, in which ENISA pointed out the advantages and security risks in cloud computing, provided some feasible recommendations and designed a set of assurance criteria to assess the risk of adoptions cloud services [11] [12]. In [13], a quantitative risk and impact assessment framework based on NIST- FIPS-199 [33] (QUIRC) is presented to assess the security risks associated six key categories of security objectives (SO) (i.e., confidentiality, integrity, availability, multi- party trust, mutual audit ability and usability) in a Cloud computing platform. The quantitative definition of risk is proposed as a product of the probability of a security compromise, i.e., an occurring threat event, and its potential impact or consequence. The overall platform security risk for the given application under a given SO category would be the average over the cumulative, weighted sum of n threats which map to that SO category. In addition, a weight that represents the relative importance of a given SO to a particular organization and/or business vertical is also necessary and their sum always adds up to 1. This framework adopts a wide band Delphi method [14], using rankings based on expert opinion about the likelihood and consequence of threats, as a scientific means to collect the information necessary for assessing security risks. The advantage of this quantitative approach of risk assessment is that it enables cloud providers, cloud consumers and regulation agencies the ability to comparatively assess the relative robustness of different Cloud vendor offerings and approaches in a defensible manner. However, the challenge and difficulty of applying this approach is the meticulous collection of historical data for threat events probability calculation, which requires data input from those to be assessed Cloud computing platforms and their vendors. Similar efforts were carried out in [48].

In [15], a risk analysis approach from the perspective of a cloud user is presented to analyze the data security risks before putting his confidential data into a cloud computing environment. The main objectives of this work are to help service providers to ensure their customers about the data security and the approach can also be used by cloud service users to perform risk analysis before putting their critical data in a security sensitive cloud. This approach is based on trust matrix. There is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments. The approach suggested in this paper is a first step towards analyzing data security risks. This approach is easily adaptable for automation of risk analysis. In [16], a Semi-quantitative BLO-driven Cloud Risk Assessment (SEBCRA) approach that is aware of the Business-Level Objectives (BLOs) of a given Cloud organization is presented. The approach is designed for a Cloud Service Provider (CSP) to improve the achievement of a BLO, i.e., profit maximization, by managing, assessing, and treating Cloud risks. The core concept on which this approach is based is that “Risk Level Estimation for each BLO is proportional to the probability of a given risk and its impact on the BLO in question”. Once risk has been assessed, the Risk Treatment sub-process defines potential risk-aware actions, controls, and policies to conduct an appropriate risk mitigation strategies, such as, avoid the risk, by eliminating its cause(s), reduce the risk by taking steps to cut down its probability, its impact, or both, accept the risk and its related consequences or transfer or delegate the risk to external organizations. In an exemplary experimentation, the risk assessment approach demonstrates that it enables a CSP to maximize its profit by transferring risks of provisioning its private Cloud to third-party providers of Cloud infrastructures. This risk assessment approach can be extended to tackle scenarios where multiple BLOs are defined by a CSP and also work as an autonomic risk-aware scheduler, which will be based on business-driven policies and heuristics that help the CSP to improve its reliability.

In [17], a cloud-based risk assessment as a service is proposed as a promising alternative. Cloud computing introduces several characteristics that challenge the effectiveness of current assessment approaches. In particular, the on-demand, automated, multi-tenant nature of cloud computing is at odds with the static, human process-oriented nature of the systems for which typical assessments were designed. However, the autonomic risk assessment is far away from the light, because the risk assessment is hard task to do. In [18], a framework called SecAgreement (SecAg) is presented, that extends the current SLA negotiation standard, WS-Agreement, to allow security metrics to be expressed on service description terms and service level objectives. The framework enables cloud service providers to include security in their SLA offerings, increasing the likelihood that their services will be used. We define and exemplify a cloud service matchmaking algorithm to assess and rank SecAg enhanced WS-Agreements by their risk, allowing organizations to quantify risk, identify any policy compliance gaps that might exist, and as a result select the cloud services that best meet their security needs.

In [27], they present a methodology for performing security risk assessment for cloud computing architectures in deferent stages (deployment and operation) basing on rules of Bayesian dependencies. The main objective of this paper is to prove how to calculate the relative risk (RR) after cloud adoption (RR=1 do nothing, RR<1 accept risk, RR>1 apply mitigation).

In [32], this paper sums up 8 kinds of threats to security principles, and lists the corresponding factors. Combing with collaborative and virtualization of cloud computing technology and so on, adopting the theory of AHP and introducing the correlation coefficient to analyze the multiple objective decisions, the paper proposes a new information security risk assessment model based on AHP in cloud computing environment. Thus, the objective of this paper is to get the security risk assessment strategies of the information system in the cloud computing environment.

IV. Synthesis and Discussion

Most of the current work is for helping cloud consumers assessing their risk before putting their critical data in a security sensitive cloud. All of these researches have laid a solid foundation for cloud computing. However, they barely established a complete risk assessment approach in consideration of the specific and complex characteristics of cloud computing environment. There were neither a complete qualitative or quantitative risk assessment method for cloud computing. Therefore, there is a need of new risk assessment approach for cloud consumers to check the effectiveness of the current security controls that protect an organization's assets.

TABLE I. RISK ASSESSMENT LIMITATIONS FOR CLOUD COMPUTING

Research paper	**Characteristics**	
	Stakeholders	***Limitations***
[13]	Cloud providers and cloud consumers	The challenge and difficulty of applying this approach is the precise collection of historical data for threat events probability calculation, which requires data input from those to be assessed Cloud Computing platforms and their vendors. Risk assessment during service construction, deployment, operation, and during admission control and internal operations is virtually nonexistent. There is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments. This framework doesn't cover risks during all the stages of the lifecycle of the service when it exists on the cloud [27].
[15]	Cloud providers and cloud consumers	There is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments.
[17]	Cloud environment	This work has not implemented such a service but rather offer it as a paradigm to be pursued. Automating risk assessment for cloud computing is far from lights to be established, because the risk assessment needs always judgments of experts to succeed
[18]	Cloud providers and cloud consumers	This framework can be used just to compare between cloud providers to select the best one basing on calculation of risk factor of each one
EBIOS [8] MEHARI [9] OCTAVE [10]		These methods don't include the specific characteristics of cloud computing Using these methods needs more time and more money due to the complex nature of cloud computing These methods are potentially cumbersome and contain several steps to validate
[16]	Cloud providers	There is a lack of complete model or method of risk assessment in cloud computing environment

From this study of current risk assessment for cloud computing, it is clear that at present there is a lack of risk assessment approaches for cloud consumers. A proper risk assessment approach will be of great help to both the service providers and the cloud consumers. With such an approach, the cloud consumers can check the effectiveness of the current security controls that protect an organization's assets and the service providers can maximize and win the trust of their cloud consumers if the level of risk is not high. Also the cloud consumers can perform the risk assessment to be aware of the risks and vulnerabilities present in the current cloud computing.

VI. Conclusion and Futur Work

After survey the literature of risk assessment regarding cloud computing, most of the current works is for helping cloud consumers assessing their risk before putting their critical data in a security sensitive cloud. Therefore, the most obvious finding to emerge from this study is that, there is a need of specific risk assessment approach. At present, there is a lack of structured method that can be used for risk assessment regarding cloud consumers to assess their resources putting outside in order to maximize the trust between the cloud consumers and cloud providers and also the effectiveness of the security system established.

As future work, we will develop a new risk assessment approach, which can take into account the complex nature of cloud computing environment.

References

[1] Vivek Kundra. (2011, july) Seeking Alpha. [Online]. Available: http://seekingalpha.com/article/283444-cutting-government-spending-with-cloud-computing

[2] Rehan Saleem, “What’s New About Cloud Computing Security?,” 2011

[3] Mkpong-Ruffin, I., Umphress, D., Hamilton, J. and Gilbert, J. Quantitative software security risk assessment model , *ACM workshop on Quality of protection*, Alexandria, Virginia, USA, 2007.

[4] Mell P, Grance T. Perspectives on cloud computing and standards. National Institute of Standards and Technology (NIST). Information Technology Laboratory; 2009.

[5] CSS, White paper on software and service architectures, Infrastructures and Engineering – Action Paper on the area for the future EU competitiveness Volume 2: Background information, Version 1.3, retrieved:15.08.2010,http://www.euecss.eu/contents/documentation/volume%20two_ECSS%20White%20Paper.pdf

[6] R. Farrell, “Securing the cloud-governance, risk and compliance issues reign supreme,” *Information Security Journal: A Global Perspective*, vol. 19, pp. 310–319, 2010.

[7] ISO 31000:2009, Risk management—Principles and guidelines

[8] EBIOS, Central Directorate for Information Systems Security, Version 2010 website. [Online]. Available: http://www.ssi.gouv.fr.

[9] Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), Carnegie Mellon - Software Engineering Institute, Juin 1999.

[10] Method Harmonized Risk Analysis (MEHARI) Principles and mechanisms CLUSIF, Issue 3, October 2004.

[11] Catteddu, D., Hogben, G.: ENISA Cloud Computing Risk Assessment. ENISA (2009)

[12] Catteddu, D., Hogben, G.: Cloud Computing Information Assurance Framework. ENISA (2009)

[13] P. Saripalli and B. Walters, QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security , In the Proceedings of the IEEE 3rd International Conference on Cloud Computing, pp. 280-288, 2010

[14] H. A. Linstone, The Delphi Method: Techniques and Applications. Addison-Wesley, 1975.

[15] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, Vasudeva Varma, “Towards Analyzing Data Security Risks in Cloud Computing Environments”, International Conference on Information Systems, Technology, and Management (ICISTM 2010), Bangkok, Thailand

[16] J. Oriol Fitó, Mario Ma_as and Jordi Guitart, Towards Business driven Risk Management for Cloud Computing, pp. 238-241, Proceedings of 2010 Int. Conf. on Network and Service Management

[17] Burton S. Kaliski Jr. and Wayne Pauley “Toward Risk Assessment as a Service in Cloud Environments,” *EMC Corporation, Hopkinton, MA*, USA 2010

[18] M. Hale, and R. Gamble, “SecAgreement: Advancing Security Risk Calculations in Cloud Services,” *8th IEEE World Congress on Services*, 2012.

[19] Heiser, J., Nicolett, M.: Assessing the Security Risks of Cloud Computing. Gartner (2008)

[20] Vishal Visintine, “An Introduction to Information Risk Assessment”, GSEC Practical ,Version 1.4b, August 8, 2003

[21] Feather, M. and Cornford, S. Quantitative risk-based requirements reasoning. *Requirements Engineering, 8* (4),pp. 248-265.

[22] Cloud Security Alliance (CSA): Top threats to cloud computing, version 1.0. http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (March 2010)

[23] Ekelhart, Fenz, Klemen and Weippl, Security Ontologies: Improving Quantitative Risk Analysis, (2007), 156a.

[24] DCSSI (2004). EBIOS – Expression of Needs and Identification of Security Objectives. http://www.ssi.gouv.fr/en/condence/ebiospresentation.html, France.

[25] ISO/IEC 27005 (2008). Information technology -Security techniques - Information security risk management. International Organization for Standardization, Geneva.

[26] ISO/IEC 27001 (2005). Information technology -Security techniques - Information security management systems - Requirements. International Organization for Standardization, Geneva.

[27] Afnan Ullah K, Manuel O, Mariam K, Ming J, Karim D.“Security risks and their management in Cloud Computing”. 2012 IEEE 4th International Conference on Cloud Computing Technology and Science

[28] Van Scoy, Roger L. Software Development Risk: Opportunity, Not Problem

[29] Deloitte. Executive Forum - Cloud Computing: risks, mitigation strategies, and the role of Internal Audit. Available: http://www.deloitte.com

[30] C. Pettey and B. Tudor. *Gartner says worldwide cloud services market to surpass $68 billion in 2010* Available: http://www.gartner.com/it/page.jsp?id=1389313

[31] Press Office. (2010, 31 August 2010). *Cloud Computing Services - New Market Report Published*. Available: http://www.companiesandmarkets.com/r.ashx?id=41AETZYHJ289173&prk=ecb8413c602cb89051067456b636c7b9

[32] Peiyu L., Dong L., 2011. “The New risk assessment model for information system in Cloud Computing environment”, Procedia Engineering 15, pp. 3200 – 3204

[33] NIST, “Standards for Security Categorization of Federal Information and Information Systems. *FIPS-199*,” <csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199.pdf>, Accessed Dec 2010.

[34] Harms-Ringdahl, L. (2001) Safety analysis: Principles and practice in occupational safety. CRC Press.

[35] Butler, S.A., Security Attribute Evaluation Method: A Cost-Benefit Approach, (2002), 232.

[36] Z. Xuan, N. Wuwong , et al., “Information security risk management framework for the Cloud Computing environments,” in 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), 2010, pp. 1328-1334.

[37] Gamal A. Awad, Elrasheed I. Sultan Noraziah Ahmad, N. Ithnan, “Multi-objectives model to process security risk assessment based on AHP-PSO” ,Modern Applied Science Vol. 5, No. 3; June 2011

[38] Theoharidou, M., Mylonas, A., Gritzalis, D.: A risk assessment method for smartphones. In: Proc. of 27th IFIP Information Security and Privacy Conference, pp. 428-440 (2012)

[39] X. Zhang, N. Wuwong, H. Li and X. Zhang, Information security risk management framework for the Cloud Computing environments,pp. 1328-1334,Proceedings of the 10th IEEE Int. Conference on Computer and Information Technology, 2010

[40] A. Morali and R. J. Wieringa, Risk-based confidentiality requirements specification for outsourced IT systems, pp. 199-208, Proceedings of the 18th IEEE International Requirements Engineering Conference, 2010, DOI 10.1109/RE.2010.30

[41] C. S. Yeo and R. Buyya, Integrated risk analysis for a commercial computing service in utility Computing, Journal of Grid Computing, Vol 7,No.1,pp.1-24,ISSN:1570-7873,Springer,Germany,March 2009

[42] Min Luo, Liang-Jie Zhang and Fengyun Lei, An Insurance Model for Guaranteeing Service Assurance, Integrity and QoS in Cloud Computing, pp. 584-591, Proceedings of 2010 IEEE International Conference on Web Services, DOI 10.1109/ICWS.2010.113

[43] A. Juan Ferrer, F. Hernandez, J. Tordsson, E. Elmroth, C. Zsigri, R. Sirvent, J. Guitart, R.M. Badia, K. Djemame, W. Ziegler, T. Dimitrakos, S.K. Nair, G. Kousiouris, K. Konstanteli, T. Varvarigou, B. Hudzia, A. Kipp, S. Wesner, M. Corrales, N. Forgo, T. Sharif, and C. Sheridan, OPTIMIS: a Holistic Approach to Cloud Service Provisioning, Future Generation Computer Systems, 2011,DOI: 10.1016/j.future.2011.05.022

[44] K. Djemame, I. Gourlay, J. Padgett, K. Voss, and O. Kao, Risk management in Grids, In R. Buyya and K. Bubendorfer, eds, Market-Oriented Grid and Utility Computing, pp. 335–353. Wiley, 2009

[45] J. A. Zachman, A Framework for information systems architecture,IBM Systems Journal, Vol 26. No 3, 1987