2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing

A CLOUD ADOPTION RISK ASSESSMENT MODEL

Erdal Cayirci
Electrical and Computer Engineering Department
University of Stavanger
Stavanger, Norway
erdal.cayirci@uis.no

Alexandr Garaga, Anderson Santana de Oliveira
SAP Labs France
Mougins, France
{alexandr.garaga, anderson.santana.de.oliveira} @sap.com}

Yves Roudier
Network Security Team
Eurecom
Biot, France
yves.roudier@eurecom.fr

***Abstract*—Cloud Adoption Risk Assessment Model is designed for cloud customers to assess the risks that they face by selecting a specific cloud service provider. It is an expert system to evaluate various background information obtained from cloud customers, cloud service providers and other public external sources, and to analyze various risk scenarios. This would facilitate cloud customers in making informed decision to select the cloud service provider with the most preferable risk profile.**

Keywords—risk assessment;cloud computing;security

I. INTRODUCTION

Moving business processes to the cloud is associated with a change in the risk landscape to an organization [1]. Cloud Security Alliance (CSA) [9] has found that insufficient due diligence was among the top threats in cloud computing in 2013. This threat is linked to the fact that organizations which strive to adopt cloud computing often do not understand well the resulting risks.

Regulations related to data protection, financial reporting, etc. put certain requirements that should be complied with even when outsourcing business processes to 3rd parties, like cloud service providers (CSPs). For example, EU Data Protection Directive, in particular Article 29 Data Protection Working Party [10] recommends that all data controllers (usually corporate cloud customers) perform an impact assessment of moving personal data of their clients to the cloud.

However, most of the cloud customers, especially Small-Medium Businesses, may not have enough knowledge in performing such assessments at a good level, because they may not necessarily employ IT specialists and the lack of transparency is intrinsic to the operations of the CSPs. This makes difficult to choose an appropriate CSP based on cloud customer's security requirements, especially considering the abundance of similar cloud offerings [7].

This work proposes a methodology, cloud adoption risk assessment model (CARAM), to help in assessing the various risks to business, security and privacy that cloud customers face when moving to the cloud by leveraging information from cloud customers, CSPs and several public sources.

CARAM consists of the following tools that complement the various recommendations from European Network and Information Security Agency (ENISA) [1], and Cloud Security Alliance (CSA) for a complete risk assessment framework:

- A questionnaire for cloud customers
- A tool and an algorithm to classify the answers to Cloud Assessment Initiative Questionnaire (CAIQ) to discrete values
- A model that maps the answers to both questionnaires to risk values
- A multi-criteria decision approach with posterior articulation of cloud customer preferences for relative risk analysis

In Section II, we elaborate on the literature related to the risk assessment for adoption of cloud computing: we focus on the work carried out by ENISA and CSA because CARAM is based on them. In Section III, we introduce CARAM, and then a multi-criteria risk assessment approach with posterior articulation of the cloud customers. In Section IV, we outline some limitations of the approach. We conclude our paper in Section V.

II. RELATED WORK

International Organization for Standardization (ISO) published a standard on Risk Management [15], ISO 31000, and the joint publication by ISO and The International Electrotechnical Commission (IEC) complemented ISO 31000 with publication ISO/IEC 31010 [16] about risk assessment techniques. Both of these standards are generic. Information Technology (IT) Governance Institute and the Information Systems Audit and Control Association (ISACA) introduced COBIT in 1996, which provides a common language to communicate the goals, objectives and results of businesses. The latest version of COBIT is from 2013 and provides recommendations also on enterprise risk management [14]. COBIT is a generic framework for IT, and its adaptation to Cloud Computing has been made for selected cases [13].

In its recommendations on risk assessment for cloud computing [1], ENISA provides a list of relevant incident scenarios, assets and vulnerabilities. It suggests estimating the level of risk on the basis of likelihood of a risk scenario mapped against the estimated negative impact, which is the essence of the risk formulation by also many others in the literature [2], [3], [4], [5], [14], [16].

Although ENISA's recommendations are specific for cloud computing, it is a generic framework that does not provide an approach to map the specifics of CSPs and cloud service customers (CSC) to the 35 risk scenarios listed in the report [1]. In Section III we describe how to fine-tune this approach to estimate risk values based on known information about

978-1-4799-7881-6/14 $31.00 © 2014 IEEE
DOI

CSCs and CSPs. ENISA's framework can be categorized as a generic qualitative deductive risk assessment for cloud computing.

Another qualitative deductive scheme was published by "The Commission nationale de l'informatique et des libertés" (CNIL) or in English: The French National Commission on Informatics and Liberty [11] more recently. CNIL's methodology is similar to the ENISA's Framework with the following difference: It is a risk assessment focused on privacy risks in cloud computing. It also recommends measures to reduce the risks and assesses the residual privacy risks after the application of these measures. However, it is still generic and does not differentiate CSPs or CSCs.

Cloud Security Alliance Cloud Assessment Initiative Questionnaire (CAIQ) [6] is a questionnaire prepared for CSPs to document the implemented security measures. It is based on the Cloud Control Matrix (CCM) taxonomy of security controls [18] and is aimed to help CSCs understand the security coverage of specific cloud offerings. The questionnaires answered by many CSPs are publicly available in CSA Security, Trust and Assurance Registry (STAR) [7].

Luna et al. introduce in [19] Cloud Security Level Agreements (SecLA) and propose a methodology to benchmark SecLA of CSPs with respect to CSCs' requirements [17]. Both CSP SecLA provisions and user requirements are expressed using a special data structure: Quantitative Policy Trees, allowing expressing controls with different granularity: CCM control areas, control groups, and controls (corresponding to CAIQ answers). The authors demonstrate their approach using data on several CSPs from STAR, by calculating security levels for respective controls and control groups.

While similar in the intent CARAM is a model for risk assessment, while [17] proposes a ranking algorithm for matching CSC requirements vs. CSP provisions. In [17] CSCs need a certain level of security expertise to specify their requirements, while in CARAM this is not necessary: CSCs only need to specify acceptable risk levels for security, privacy and service categories, while still allowing a more fine grained specification. Another major difference is that [17] assumes the existence of a mapping from provisions to quantitative Local Security Levels to allow further analysis. Given a high number of potential CSPs and controls for each CSP creating this mapping would require significant manual work. In CARAM we propose a way to automatically construct such a mapping (see Section III.A).

Habib et al. propose a multi-faceted Trust Management system architecture for a cloud computing marketplace [21]. The system evaluates the trustworthiness of CSPs in terms of different SLA attributes assessed using information collected from multiple sources. This is done by evaluating opinions related to SLA attributes and aggregating them into a trust score for a CSP. The authors mention CAIQ answers as a source of information, however they do not specify how exactly the CSP trust score is computed from the answers, especially considering that the answers are in free text form.

Joint Risk and Trust Model (JRTM) [2] was developed by Accountability for Cloud and Other Future Internet Services Project (A4Cloud). JRTM is a quantitative and inductive risk assessment model that assesses the cloud service security and privacy risks for a specific CSP and CSC. It counts on a third party (i.e., a Trust as a Service Provider) to accumulate statistical data (i.e., evidence) on the trustworthiness of CSPs. These evidences include the number of security, privacy and service events that a CSP was subject to and the percentage of the events that the CSP recovered from before they become an incident (i.e., they impact on CSC).

CARAM, introduced in this paper, is a new model based on ENISA and CAIQ. It complements ENISA Cloud Risk Assessment by adapting it to specifics of CSPs and CSCs for a relative risk assessment.

III. RISK LEVELS COMPUTATION

ENISA [1] identified 35 incident scenarios that fall in one of the following four categories: policy and organizational, technical, legal and the other scenarios not specific to cloud computing (see Table 3). The likelihood of each of these scenarios and their business impact are determined in consultation with an expert group. The scale of probability and impact has five discrete classes between very low and very high. For example, the probability and impact of Incident Scenario P1 in "Policy and Organizational Scenarios" category (i.e., lock-in) are given as HIGH and MEDIUM relatively.

ENISA also provides a list of 53 vulnerabilities (i.e., 31 cloud specific and 22 not cloud specific vulnerabilities) and 23 classes of CSC assets that may be affected by the cloud adoption. Each of 35 incident scenarios is related with a subset of vulnerabilities and assets. For example, the Incident Scenario P1 is related to Vulnerabilities *V13 (*lack of standard technologies and solutions), *V31* (lack of completeness and transparency in terms of use), *V46 (*poor provider selection), *V47* (lack of supplier redundancy) and Assets *A1* (company reputation), *A5* (personal sensitive data), *A6* (personal data), *A7* (personal data critical), *A9* (service delivery – real time services), *A10* (service delivery).

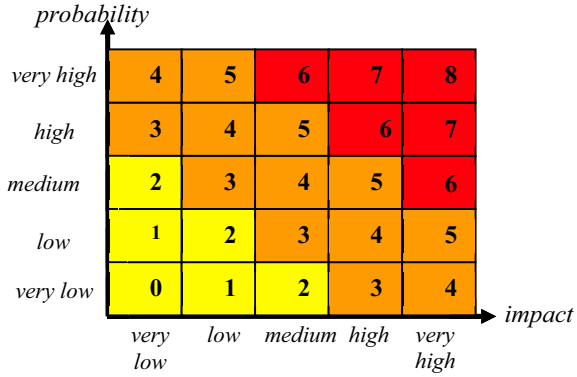

Figure 1: ENISA definition of risk levels.

The likelihood and business impact values that are determined by the experts are converted to the risk levels for each incident scenario based on a risk matrix with a scale between 0 and 8

as shown in Figure 1. Then, the risk levels are mapped to a qualitative scale as follows:

- Low risk: 0-2
- Medium: 3-5
- High: 6-8

Hence a cloud customer can assess the risk level related to an incident scenario qualitatively and understands what kind of vulnerabilities and assets are related to each scenario by examining [1]. These values represent educated guesses over a wide range of common cloud deployments and do not have a precise semantics. In practice, the risk levels are related to many factors such as the security controls that CSPs implement and the concerned assets of the specific users. Therefore, a generic value cannot be applied to all CSPs and CSCs. Although vulnerabilities and assets for each incident scenario are given by ENISA framework, it does not describe how those values can be adapted for a specific CSP and CSC pair. CARAM fills this gap. For that, first the qualitative scale used by ENISA as probability and impact values are mapped to a quantitative scale as follows:

- Very low → 1
- Low → 2
- Medium → 3
- High → 4
- Very high → 5

For example, probability P_I and impact I_I values for the first scenario (i.e., lock in) is HIGH and MEDIUM respectively. We map these values as follows: P_I=4 and I_I=3.

However, probability and impact of a risk scenario are very much dependent on the vulnerabilities and assets involved in. Therefore, these values cannot be the same for all CSPs and CSCs. CARAM adjusts the values from ENISA, taken as a baseline, considering additional information about the cloud service. For that, we use Equations 1 and 2:

$$\beta_i = P_i \times \vartheta_i \qquad (1)$$

$$\delta_i = I_i \times \alpha_i \qquad (2)$$

In Equation 1, for the risk scenario i, β_i is the adjusted probability, ϑ_i is the vulnerability index of a given CSP, δ_i is the adjusted impact and α_i is the asset index for a given CSC. Here we assume that probability and impact of an incident are proportional respectively to the number of non-addressed vulnerabilities by a CSP and the number of CSC assets related to risk scenario i. Note that vulnerability index of a CSP is the same for all CSCs and the asset index of a CSC is the same for all CSPs. Vulnerability and asset indices are calculated as given in Equations 3 and 4 respectively, where v_{ki} is 1 if vulnerability k is in the list of vulnerabilities [1] for risk scenario i, and 0 otherwise. Similarly, a_{ki} is 1 if asset k is in the list of assets [1] for risk scenario i. Please note again that there are 53 vulnerabilities and 23 assets listed in [1]. The other two parameters ε_k and γ_k in Equation 3 and 4 are derived from the answers to the questionnaires for CSP and CSC (i.e., CAIQ and A4Cloud Questionnaire). The vulnerability related parameter ε_k is elaborated later in subsection III.A. The asset related parameter γ_k is given value 0 if the CSC's answer to the question that "Does the service that you seek will involve any asset of yours that fall in the same category as asset k?" is "No", and value 1 otherwise.

We would like to highlight that CARAM is independent from the number of incident scenarios and probability, impact, vulnerability and assets assigned to the incident scenarios. Moreover, it is possible to assign weight values for each of assets and vulnerabilities if some of them are assumed as of higher importance comparing to the others.

$$\vartheta_i = \frac{\sum_{k=1}^{53} v_{ki} \times \varepsilon_k}{\sum_{k=1}^{53} v_{ki}} \qquad (3)$$

$$\alpha_i = \frac{\sum_{k=1}^{23} a_{ki} \times \gamma_k}{\sum_{k=1}^{23} a_{ki}} \qquad (4)$$

A. The Vulnerability Parameter for a CSP

We use CSP's responses to CAIQ from [7] to assign a value to the vulnerability related parameter ε_k. CAIQ aims at collecting data directly from CSP on how much they comply with the regulations/standards and how secure is their infrastructure. It consists of questions grouped into the control areas shown in Table 1, asking about the state of implementation. The CSPs are expected to answer these questions as "Yes", if the control is implemented and as "No" otherwise. However, most of the CSPs that have answered the questionnaire in STAR used free text explanations rather than simple "Yes" or "No", which is more informative but unsuitable for automated analysis. CARAM provides the following mechanism to map the answers given to the questions in CAIQ to one of the categories in Table 2. Please note that the category "Yes" in Table 2 means the control is implemented, which is positive. The answer "Yes" to CAIQ questions do not always imply a more secure system (i.e., the control is implemented). For example, the "Yes" answer to CAIQ Question RS06-01 "Are any of your datacenters located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?" implies a negative outcome, which means the control is not implemented. Therefore, CARAM maps the answer "Yes" to this question as "No: the control is not implemented".

TABLE 1 THE CONTROL GROUPS IN CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE

1. Compliance	6. Legal
2. Data Governance	7. Operations Management
3. Facility Security	8. Risk Management
4. Human Resources Security	9. Release Management
5. Information Security	10. Resiliency
	11. Security Architecture

TABLE 2 THE CATEGORIZATION OF THE ANSWERS GIVEN TO THE QUESTIONS IN CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE

Yes: the control is implemented
Yes, conditionally: the control can be implemented under some conditions

No: the control is not implemented Not available: the answer is not given Not applicable: the control is not applicable to the provided service

Given that there are about 100 of CSPs in the mentioned registry providing answer to about 200 questions each, the automation of this categorization could save significant time. For the automatic classification of the free text answers to CAIQ questions we use supervised machine learning algorithms provided by the WEKA tool [8]. For that we have provided a training set representing a random sampling of around 300 classified answers out of overall circa 9000 answers and used it to classify the other remaining answers. The 10-folds cross-validation provided an accuracy of around 84% of correctly classified instances, which we consider enough for our purpose.

After classification of the answers to one of the categories in Table 2, the implementation value q_m is assigned for each of the controls. If the answer to a question is "Yes", that trivially means the control implied in question m is available (i.e., $q_m=0$) and hence the related vulnerabilities are mitigated. For "Not applicable" $q_m=0$: these controls do not impact the risk value. The "No" and "Not available" classes imply that the control will not be available, and therefore $q_m=1$. If the class is "Yes Conditionally", the CSC needs to clarify with the CSP if the control can be implemented. If yes, $q_m=0$. Otherwise, $q_m=1$.

When q_m is known for a CSP and a CSC, Equation 5 gives the vulnerability related parameter ε_k for the CSP and the CSC. Please note that this value is for a specific CSP and CSC pair.

$$\varepsilon_k = \frac{\sum_{m=1}^{n} r_{m,k} \times q_m}{\sum_{m=1}^{n} r_{m,k} \times b_m} \qquad (5)$$

In Equation 5, n is the number of questions in CAIQ. $r_{m,k}$ is the mapping of the CAIQ questions to vulnerabilities: it is 1 if the question m is related to vulnerability k, and 0 otherwise (we do not provide it here for space constraints).

Finally, $b_m=0$ if the answer to the question m is "Not Applicable" and 1 otherwise. This allows discarding the unrelated questions avoiding wrongly penalizing the CSPs.

In Equation 5 ε_k receives a minimum value 0 if all the controls related to the vulnerability k are implemented and hence the vulnerability does not impact negatively the risk values. The more controls related to the vulnerability k are not implemented, the higher ε_k is. Its maximum value is 1, which means the CSP has no measures against the vulnerability k.

B. *Relative Risk Assesment Based CSP Selection with Posterior Articulation of CSC Preferences*

ENISA Risk Assessment Model is based on 35 incident scenarios. This is too many in numbers for selecting a CSP that fits best to a CSC's requirements. Therefore, we first reduce the number of criteria from these 35 incident scenarios to three categories of cloud risks: security, privacy and service [2]. For that, we compute the probability that a privacy (β_r), a security (β_s) and a service (β_e) incident can occur and the impact of a privacy (δ_r), a security (δ_s) and a service (δ_e) incident by applying Equations 6 to 11. In Equations 6 and 9, r_i is 1 if ENISA incident scenario i is related to privacy, and 0 otherwise (we do not provide this mapping here for space constraints). ω_{ri} and α_{ri} are real numbers between 0 and 1. They are the weight factors for probability and impact respectively. The significance of every scenario may not be the same when calculating an aggregated value for privacy, security and service incidents. Moreover, the scenarios may need to be treated differently for each CSC especially when calculating the aggregated impact values. The weight factors are for making these adjustments. If the significance of each scenario is the same, then the weight factors can be assigned 1. Similar to r_i, s_i and e_i are the mapping values for security and service risks respectively. ω_{si} and α_{si} are the weight factors for security scenarios, and ω_{ei} and α_{ei} are the weight factors for service scenarios.

$$\beta_r = \frac{\sum_{i=1}^{35} \beta_i \times r_i \times \omega_{ri}}{\sum_{i=1}^{35} r_i \times \omega_{ri}} \qquad (6)$$

$$\beta_s = \frac{\sum_{i=1}^{35} \beta_i \times s_i \times \omega_{si}}{\sum_{i=1}^{35} s_i \times \omega_{si}} \qquad (7)$$

$$\beta_e = \frac{\sum_{i=1}^{35} \beta_i \times e_i \times \omega_{ei}}{\sum_{i=1}^{35} e_i \times \omega_{ei}} \qquad (8)$$

$$\delta_r = \frac{\sum_{i=1}^{35} \delta_i \times r_i \times \alpha_{ri}}{\sum_{i=1}^{35} r_i \times \alpha_{ri}} \qquad (9)$$

$$\delta_s = \frac{\sum_{i=1}^{35} \delta_i \times s_i \times \alpha_{si}}{\sum_{i=1}^{35} s_i \times \alpha_{si}} \qquad (10)$$

$$\delta_e = \frac{\sum_{i=1}^{35} \delta_i \times e_i \times \alpha_{ei}}{\sum_{i=1}^{35} e_i \times \alpha_{ei}} \qquad (11)$$

When probability (i.e., β) and impact (i.e., δ) values are calculated, they are mapped to the qualitative scale as follows:

[0, 1] → Very low
(1, 2] → Low
(2, 3] → Medium
(3, 4] → High
(4, 5] → Very high

Finally, by using the same approach as shown in Figure 1, the risk values for privacy R_r, security R_s and service R_e are obtained in a qualitative scale: Very Low < Low < Medium < High < Very High for each CSP-CSC pair.

At this stage, the CSC (the customer that needs relative risk assessment) provides CARAM with the maximum acceptable levels of risks for privacy R_{rmax}, security R_{smax} and service R_{emax}. The CSC may also provide a set $U=\{p_1, ..., p_n\}$ of CSPs that should be excluded from the assessment due to reasons like business relations, politics, past experience, etc. When

this information is available, CARAM creates a set F of feasible CSPs out of the set S of all the CSPs available for assessment (i.e., CSPs that have a completed CAIQ in STAR) such that:

$$F \subset S$$

$$p_i \in F \text{ iff } (p_i \notin U) \wedge (R_{rmax} > R_{ri}) \wedge (R_{smax} > R_{si}) \wedge (R_{emax} > R_{ei})$$

where R_{ri}, R_{si} and R_{ei} are the privacy, security and service risks for the CSP p_i.

F can be an empty set, a set with only one element or multiple elements. If F is an empty set, there is no feasible solution for the CSC. If F has only one element, that is the only feasible solution for the CSC under the given constraints. In both of these cases, CARAM informs the CSC directly with the result. If F has multiple elements, all CSPs in F but the non-dominated ones are removed from F. In the resulting non-dominated set F' there cannot be any CSP which has all R_{ri}, R_{si} and R_{ei} values smaller than any other CSP in F'. If the resulting F' includes only one CSP, CARAM informs the CSC about the solution that fits best to it. If there are multiple CSPs in F', the CSC is given the complete F' for the posterior articulation of the preferences.

IV. LIMITATIONS

The accuracy of the risk assessment results using this method depends on the accuracy of the input data and the appropriateness of the proposed formulas. We believe that major sources of systematic errors are: 1) incorrect classification of the CAIQ answers; 2) vague CAIQ answers; 3) ineffective implementation of controls. The first and, to an extent, second errors may be estimated by the classification algorithm itself and appropriate statistical formulas for calculating the absolute error of a function of random variables (we do not provide them here for space constraints). Addressing the last one would require additional methods for evaluating control effectiveness, e.g. penetration testing or analysis of previous incidents (see [2], [20] for example approaches).

V. CONCLUSION

CARAM is a qualitative and relative risk assessment model for assisting CSCs to select a CSP that fits their risk profile best. It is based on the existing frameworks such as ENISA, CAIQ, CNIL developed in Europe for the last decade and complements them to provide the CSC with a practical tool. It is a risk assessment approach such that evaluation is carried out for a specific CSC, which means assessment for each CSP-CSC pair is for that pair and not generic.

We have implemented a Proof-of-Concept prototype as part of the Data Protection Impact Assessment tool developed in A4Cloud[1] project. The tool asks a (potential) CSC to select a CSP from a given list of around 50 providers, which answered to the CAIQ and evaluates a risk landscape of 35 risks from Table 3 grouped into 3 categories: service, security and privacy. Also the tool allows the CSCs to compare the risk profiles of any two providers, thus helping to select the most suitable CSP from the security point. We used the prototype to do a risk assessment of a fictitious cloud adoption scenario. Further, we plan to run user trials within A4Cloud to collect feedback on the usefulness of the approach, and work on proposing a more systematic evaluation.

[1] a4cloud.eu

ACKNOWLEDGMENT

This work is conducted as part of the EU-funded FP7 project titled as "Accountability for Cloud and Other Future Internet Services" (A4Cloud) which introduces an accountability-based approach for risk and trust management in cloud ecosystems.

VI. APPENDIX

TABLE 3 ENISA'S LIST OF RISK SCENARIOS AND THEIR CATEGORIES

Risk Category	Risk name
Policy & Organizational	P1. Lock-in P2. Loss of governance P3. Compliance challenges P4. Loss of business reputation due to co-tenant activities P5. Cloud service termination or failure P6. Cloud provider acquisition P7. Supply chain failure
Technical	T1. Resource exhaustion (under or over provisioning) T2. Isolation failure T3. Cloud provider malicious insider - abuse of high privilege roles T4. Management interface compromise (manipulation, availability of infrastructure) T5. Intercepting data in transit T6. Data leakage on up/download, intra-cloud T7. Insecure or ineffective deletion of data T8. Distributed denial of service (DDoS) T9. Economic denial of service (EDOS) T10. Loss of encryption keys T11. Undertaking malicious probes or scans T12. Compromise service engine T13. Conflicts between customer hardening procedures and cloud environment
Legal	L1. Subpoena and e-discovery L2. Risk from changes of jurisdiction L3. Data protection risks L4. Licensing risks
Not Specific to the Cloud	N1. Network breaks N2. Network management (ie, network congestion / mis-connection / non-optimal use) N3. Modifying network traffic N4. Privilege escalation N5. Social engineering attacks (ie, impersonation) N6. Loss or compromise of operational logs N7. Loss or compromise of security logs (manipulation of forensic investigation) N8. Backups lost, stolen N9. Unauthorized access to premises (including physical access to machines and other facilities)

	N10. Theft of computer equipment N11. Natural disasters

REFERENCES

[1] ENISA, "Cloud Computing; Benefits, Risks and Recommendations for Information Security," 2009 Edition, http://www.enisa.europe.eu, June 2014.

[2] Cayirci, E. and A.S. Oliveira, "Modelling Risk and Trust for Cloud Service Mashups," IEEE Transactions on Computers (submitted).

[3] Cayirci, E. 2013a. "A Joint Trust and Risk Model for MSaaS Mashups," In *Proceedings of the 2013 Winter Simulation Conference*, edited by R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc. pp 1347-1358, December 2013.

[4] Kaplan, S., and B.J. Garrick. 1981. "On The Quantitative Definition of Risk," *Risk Analysis* 1(1): 11-27.

[5] Ezell, B.C., S.P.Bennet, D. Von Winterfeldt, J.Sokolowski, and A.J.Collins. 2010. "Probabilistic Risk Analysis and Terrorism Risk," *Risk Analysis* 30(4): 575-589.

[6] CSA, "Consensus Assessment Initiative Questionnaire (CAIQ)," https://cloudsecurityalliance.org/research/cai/, June 2014.

[7] CSAN, "Security, Trust & Assurance Registry (STAR)," https://cloudsecurityalliance.org/star/#_registry, June 2014.

[8] WEKA: Data Mining Software in Java, http://www.cs.waikato.ac.nz/ml/weka/, June 2014.

[9] CSA, "The Notorious Nine Cloud Computing Top Threats in 2013," https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf, June 2014.

[10] EU, "Opinion 05/2012 on Cloud Computing (2012)," http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[11] CNIL, "Methodology for Privacy Risk Management: How to Implement the Data Protection Act," 2012 Edition, http://www.cnil.fr/english/publications/guidelines/, June 2014.

[12] Jansen, W. and T. Grance, "Guidlines on Security and Privacy in Public Cloud Computing," NIST Special Publication 800-144, December 2011.

[13] Gadia S., "Cloud Computing Risk Assesment: A Case Study," ISACA Journal, Vol. 4, pp 1-6, 2011.

[14] ISACA, "COBIT 5: A Business Framework for the Governence and Management of Enterprise IT," http://www.isaca.org/cobit/pages/default.aspx, June 2014.

[15] ISO 31000, "Risk Management (2009 Edition)," http://www.iso.org/iso/home/standards/iso31000.htm, June 2014.

[16] ISO/IEC 31010, "Risk Management-Risk Assesment Techniques (2009 Edition)," https://www.iso.org/obp/ui/#iso:std:iso-iec:31010:ed-1:v1:en, June 2014

[17] Luna, J. L., Langenberg, R., & Suri, N. (2012). Benchmarking cloud security level agreements using quantitative policy trees. *Cloud Computing Security Workshop*, 103. doi:10.1145/2381913.2381932

[18] CSA, "Cloud Control Matrix (CCM)," https://cloudsecurityalliance.org/research/ccm/ , June 2014.

[19] Luna J., et.al. (2011). Quantitative Assessment of Cloud Security Level Agreements: A Case Study. In Proc. of Security and Cryptography, (In Press).

[20] Habib, S. (2013). A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces. *... , Security and Privacy in ...*, 459–468. doi:10.1109/TrustCom.2013.58

[21] Habib, S. M., Ries, S., & Muhlhauser, M. (2011). Towards a Trust Management System for Cloud Computing. *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, 933–939. doi:10.1109/TrustCom.2011.129