CSCCRA: A novel quantitative risk assessment model for cloud service providers

Author

Akinrolabu, O, New, S, Martin, A

Published

2019

Conference Title

Information Systems

Version

Accepted Manuscript (AM)

DOI

10.1007/978-3-030-11395-7_16

CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers

Olusola Akinrolabu[1] and Steve New[2] Andrew Martin[1]

[1] Department of Computer Science, University of Oxford, OX1 3PR, UK,
olusola.akinrolabu@cs.ox.ac.uk andrew.martin@cs.ox.ac.uk
[2] Said Business School, University of Oxford, OX1 1HP, UK,
steve.new@sbs.ox.ac.uk

Abstract. Assessing and managing cloud risks can be a challenge, even for the cloud service providers (CSPs), due to the increased numbers of parties, devices and applications involved in cloud service delivery. The limited visibility of security controls down the supply chain, further exacerbates this risk assessment challenge. As such, we propose the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, a quantitative risk assessment model which is supported by cloud supplier security assessment (CSSA) and cloud supply chain mapping (CSCM). Using the CSCCRA model, we assess the risk of a Customer Relationship Management (CRM) application, mapping its supply chain to identify weak links, evaluating its security risks and presenting the risk value in dollar terms, with this, promoting cost-effective risk mitigation and optimal risk prioritisation.

Keywords: Cloud Computing, Quantitative Risk Assessment, Supply Chain, Transparency, Security Rating Service

1 Introduction

The use of cloud resources has changed the way data is stored, shared, and accessed. The use of public cloud typically means that organisation's data and applications are managed outside their *trust boundary* and often require a complex and dynamic supply chain which lacks clearly defined boundaries. This new approach to IT service delivery introduces a new set of risks. While we argue that cloud is often more secure, compared to many enterprise networks, the extent of this security is hard to verify, seeing that CSPs who should be more aware of cloud risks, find it difficult to audit or assess risks due to limited visibility of security controls and lack of supplier transparency down the supply chain [14].

The multi-tenancy characteristics of the cloud, coupled with its dynamic supply chain have been identified as two areas of challenge to cloud risk assessment. This challenge is further exacerbated by the predominant use of qualitative or weak quantitative, traditional IT risk assessment methods in assessing cloud risks [2]. Studies into the supply chain of cloud services have shown that at least 80% of a typical software-as-a-service (SaaS) application is made up of assembled parts, with each component representing a different level of risk [17]. As

such, IT risk assessment methods, e.g. ISO 27005, which were developed in the days of end-to-end service delivery, are now unable to cope with the inherent risks within the dynamic cloud supply chain[16].

This study presents CSCCRA, a quantitative risk assessment model which adopts the systems thinking approach to solving complex system problems [8]. The CSCCRA model is built out to empower CSPs to make reliable inferences about the risk of their cloud service after careful analysis of its interconnected supply chain and an assessment of the security posture of component suppliers. It builds on existing risk assessment standards and guidance documents such as ISO/IEC 27005:2011, ISO/IEC 31010:2009, NIST 800-30v1, and the Factor Analysis of Information Risks (FAIR) methodology. Using the CSCCRA model, we conceptualise and analyse the security risk of a CRM cloud application.

The structure of the paper is as follows - we present the literature on cloud risk assessment and supply chain risks in section 2. Then we articulate the CSCCRA model in section 3. The CSCCRA is used to assess the risk of a CRM application in section 4, followed by conclusions and future work in section 5.

2 Literature review

This section focuses on a review of existing risk assessment models, the cloud supply chain, and identifies a gap in cloud risk assessment.

2.1 Cloud Risk Assessment

Cloud risk assessment is defined as a step by step, repeatable process used to produce an understanding of cloud risks associated with relinquishing control of data or management of services to an external service provider [11]. Currently, and despite the very many discourses about cloud computing risks, there is no structured framework for identifying, assessing and managing cloud risks [10]. The lack of a systematic approach and expert subjectivity synonymous with risk assessments, particularly qualitative, has led to inconsistencies in cloud risk assessment.

Seeing that cloud deployments are rapidly evolving due to new service provider offerings and changing compliance and regulatory landscape, risk assessment solutions would seem not to be keeping pace with cloud growth. In Table 1, we present a cross-section of proposed cloud risk assessment methods which like CSCCRA, are quantitative and can be used by CSPs to assess the risk of cloud service provision.

2.2 Cloud Supply Chain Risks

The supply chain of a cloud service can be defined as a complex system of two or more parties that work together to provide, develop, host, manage, monitor or use cloud services [1]. We define cloud supply chain risk as the probability of an internal or external event targeted at a cloud service or its extended network

Table 1. Existing Cloud Risk Assessment Models

Author/ Year	Cloud Risk Assessment Description	Method	Implem-entation	Risk value	Use of Experts	Supply chain
(Djemame et al., 2011) [5]	Risk assessment framework with methodologies for the identification, evaluation,mitigation & monitoring of cloud risks during the various stages of cloud provision.	Semi-quanti-tative	No	Risk Score	No	Yes
(Fito et al., 2010)[6]	A cloud risk assessment model for analysing the data security risks of confidential data. It prioritises cloud risks according to their impact on Business Level Objectives(BLO).	Semi-quanti-tative	Yes	Risk Score	No	No
(Saripalli & Walters, 2010) [15]	A quantitative risk and impact assessment of cloud risk events based on six key security objectives.	Semi-quanti-tative	No	Risk Score	Yes	No
(Sendi & Cheriet, 2014)[16]	The model uses fuzzy multi-criteria decision-making technique to assess cloud risks.	Quanti-tative	Yes	Risk Score	No	No
(Sivasubram-anian et al., 2017)[18]	The model measures cloud risks in terms of impact, occurrence and disclosure, to arrive at a Risk Priority Number (RPN).	Semi-quanti-tative	No	Risk Score	No	No

of suppliers, causing a disruption or failure to cloud operation and leading to reductions in service levels and security posture, with a possible increased cost of remediation. The cloud supply chain employs "aggressive sourcing" based on free-market principles rather than collaboration, which increases cloud risks. Furthermore, the risks associated with the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of cloud services increases with the on-demand, automated, and multi-tenanted cloud, down the supply chain [3].

2.3 Research Gap and Proposal

As shown in Table 1, only one of the risk assessment models used by CSPs considered the inherent risks in the supply chain. With the cloud supply chain made up of small and medium businesses (SMBs), whose vulnerability to cyber attacks magnifies into the supply chains, there is a need to assess cloud risks from a supply chain perspective, identifying the sub-providers involved in service delivery and evaluating their security controls.

As such, we propose the CSCCRA model, which we argue, addresses the problem of supply chain risks in the cloud. Currently, no in-depth study has been conducted to address this problem, and since information security is all about decision-making, we believe that our quantitative and iterative approach to cloud risk assessment, will provide organisations with an objective result, that

is consistent, easy to understand, and encourages continuous mitigation of cloud risks.

3 The CSCCRA Model

The CSCCRA model (see Fig. 1) considers the dynamism of the cloud supply chain and looks to address the gap on cloud supply chain transparency, and how the lack of visibility of supplier's security controls have contributed to the inadequate level of cloud risk assessment. Given the scarcity of initiatives for the practical implementation of a quantitative cloud risk assessment, the development of the CSCCRA model aims to contribute towards improving the state-of-the-art in cloud risk assessment. It hopes to achieve this by showing how a holistic quantitative risk assessment and decision analysis model provides a unique capability for capturing the dynamic behaviour of risks within a cloud supply chain and measuring the overall risk behaviour. While numerous scholars have openly questioned the subjectivity of expert's estimate in quantitative analysis, our implementation of CSCCRA aims to prove that despite the lack of historical data, cloud risk assessments can achieve increased objectivity through the use of controlled experimentation, clearly defined model, peer reviews, and calibration of the expert judges [7].

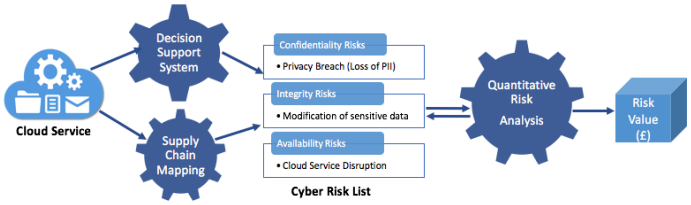

Fig. 1. Overview of CSCCRA model

The three components of the CSCCRA model are as follows [1]:

1. **Quantitative Risk Assessment**: The CSCCRA model goes beyond the IT industry norm to apply a quantitative assessment method to cloud risks. It expresses risk as the combination of the probability of an event and its consequences as per ISO Guide 73:2009, and follows a rigorous process in the identification and evaluation of security risk factors. With uncertainty being the primary factor in risk analysis, the CSCCRA model makes use of a probabilistic estimate of risk factors, e.g. threat frequency, vulnerability and loss magnitude, representing the forecast as a distribution (e.g. PERT, Poisson).
2. **Cloud Supplier Security Assessment**: The CSSA is a decision support system and a novel addition to cloud risk assessment. It functions as a Security Rating Service (SRS) for the suppliers involved in the delivery of the

cloud service [12]. The CSCCRA model requires cloud providers to be aware of their supply chain and have sufficient information about the processes and capabilities of their vendors. Being a Multi-criteria security assessment tool, the CSSA follows a formal and rigorous process which involves decomposing the cloud service into its component objects and using an improper linear model to rate suppliers based on identified security criteria, resulting in the identification of suppliers with poor security postures.

3. **Cloud Supply Chain Mapping**: Providing end-to-end supply chain visualisation while assessing cloud risk makes it amenable to analyse and explore areas of weakness, strengths and the potential risks to a cloud service while also supporting collaboration and decision-making within the chain [19]. The benefit of a graphical representation of the inherent risk in the supply chain helps to counter any documented biases in risk estimation and decision-making and is thought to have an impact in reducing the cognitive load involved in the estimation of risk factors [9].

4 Scenario of a SaaS Provider using CSCCRA model

In this section, we describe the steps involved in the risk assessment of a CRM SaaS application using the CSCCRA model (see Fig. 2). The CRM application is built using the services of Platform-as-a-Service (PaaS-A) provider, whose function is hosted on Infrastructure-as-a-Service-A (IaaS-A) and uses a Structured Query Language (SQL) database hosted by IaaS-B. Furthermore, the CRM application makes use of four API providers for services such as customer billing, custom 'social search', monitoring, and identity & access management (IAM). To further complicate the relationship, the IAM and monitoring API providers built their applications using the same platform provider, PaaS-B, who also runs on the IaaS-A infrastructure.

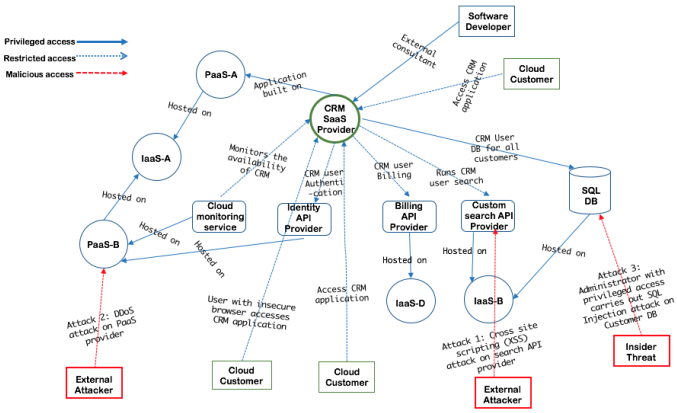

Fig. 2. The Supply Chain Map of the CRM Cloud Service

4.1 Cloud Supplier Security Assessment

The CSCCRA model is designed in such a way that both CSSA and CSCM processes take place before cloud risk identification, to enable the CSP to acquire a sound knowledge of the underlying factors contributing to their security risks (see Fig. 1). Using the details contained in the supply chain map, stakeholders within the CSP rate the suppliers on security capabilities, process, reliability and compliance factors. According to Robyn Dawes, human judges are good at picking out the right predictor variables (risk factors) and coding them, but poor at integrating information from diverse and incomparable sources [4].

As part of overcoming the human subjectivity challenge, the CSSA tool is implemented based on an improper linear model, known as Dawes model, which employs the z-score method of unit-weighted regression. Fig. 3 shows the rating of the Five Tier-1 suppliers based on six predictive attributes: estimated outage, supplier criticality, past Service Level Agreement (SLA), security practice, security certification, and process maturity.

CSP's list of suppliers	Estimated outage duration (hrs)	Criticality of the supplier (1 for critical, 0 for commodity)	Past SLA performance (0 for didn't meet SLA, 1 for achieved SLA)	General security practice (controls and processes) (1-10 with 1 being very poor, 5-moderate, 10-	Industry security certification and standard compliance (0 for non certified, 1 for industry certified)	Process Maturity (1-5, with 1 being Initial, 2-Repeatable, 3-Defined, 4-Measured, 5-Optimised)	Weighted z-scores ======>>>	z-score Estimated outage	z-score Criticality of the supplier	z-score Past SLA performance	z-score General security practice	z-score Industry certification	z-score Maturity	Total Weighted z-scores. In this case, a negative z-score means the risk is lower than average. A positive z-score means it is higher
PaaS-A Hosting	3	1	1	9	1	4		-1.33	0.45	-0.45	-1.23	-0.45	-0.73	-0.62
Identity CSP	5	1	1	8	1	4		-0.59	0.45	-0.45	-0.35	-0.45	-0.73	-0.35
Billing CSP	8	0	1	8	1	4		0.52	-1.79	-0.45	-0.35	-0.45	-0.73	-0.54
Custom API CSP	10	1	0	7	0	3		1.26	0.45	1.79	0.53	1.79	1.10	1.15
Database CSP	7	1	1	6	1	3		0.15	0.45	-0.45	1.40	-0.45	1.10	0.37

Fig. 3. Security Assessment of the CRM Suppliers

4.2 Risk Identification and Analysis

From the vantage point of the just concluded supplier assessment, the CSP stakeholders can visualise their areas of weakness. With the Search API vendor being a critical supplier, who has missed SLA in the last year and has the highest estimated outage, the focal CSP will be paying close attention to this supplier when drawing up their comprehensive list of security risks. A potential risk identified by the CSP is the compromise of confidential customer data due to a Cross-Site Scripting (XSS) attack on the custom search vendor.

For this scenario, the stakeholders assess the confidentiality risk using the available information about the custom search supplier, its criticality, security assessment rating etc. This information assists them in making estimates on the impact, probability, and frequency of the risk. These estimates are presented as a probability distribution, including lower bound, most likely, and upper bound values, made to a 90% confidence interval. The risk factor estimates are then used as input into the Monte Carlo simulation tool, see Table 2. The use of Monte Carlo helps to build models of possible risk results, reducing the impact of inherent uncertainty involved in the risk estimation. It calculates the risk result

over a specific number of iterations, each time using a different set of random values from the probability functions and at the end producing a distribution of possible risk values for a risk item [13].

Table 2. Risk calculation of custom search API attack using @RISK software for Monte Carlo Simulation (10,000 iterations & 5 simulations)

	Parameter of Distribution			
Uncertain Inputs	**Distribution**	**Lower Bound**	**Most Likely**	**Upper Bound**
Probability of risk (without controls) (PWC)	PERT	5%	7%	10%
Control Efficiency (CE)	PERT	2%	3%	4%
Impact cost (IC)	PERT	£5,000	£14,500	£70,000
Frequency of occurrence per year (Fr)	Poisson	1		
Estimated Risk Value (ERV)	Without Controls	With Controls		
5% Percentile	£0	£0		
Mean	£3,177.30	£1,828.40		
95% Percentile	£9,105.86	£5,452.16		

5 Conclusion and Future Work

This study set out to identify the supply chain gap in cloud risk assessment and propose the CSCCRA model as a way of bridging this gap. Using the proposed model, we showed how the decomposition of risk items into its various risk factors, allows decision makers to investigate cloud risks, avoiding extreme subjectivity in their evaluation. Although targeted at CSPs, a distinctive contribution of this study is that it caters for the complexities involved in cloud delivery and adapts to the dynamic nature of the cloud, enabling CSPs to conduct risk assessments at a higher frequency, in response to a change in the supply chain. The CSCCRA is a rigorous and dynamic risk assessment model, which combines aspects of various disciplines and can be applied to the risk assessment of many composite services.

Future work will see us integrate the security factors achieved during our recently completed Delphi study into the CSSA tool, and develop the CSCCRA model into a web application. A current limitation of this study is its lack of practical application, which we plan to address by conducting case studies of three SaaS provider organisations who will use the model to carry out a comprehensive real-world assessment of their cloud service.

Collectively, we anticipate that the implementation of the CSCCRA model will reveal that this inclusive, structured and systematic approach to cloud risk assessment, can deliver objective risk results, saving the CSP time and effort as they mature into the use of the model.

References

1. Akinrolabu, O., New, S., Martin, A.: Cyber supply chain risks in cloud computing - bridging the risk assessment gap. Open Journal of Cloud Computing (OJCC) **5**(1) (2018) 1–19
2. Badger, L., Patt-corner, R., Voas, J.: Cloud Computing Synopsis and Recommendations Recommendations of the National Institute of Standards and Technology. Nist Spec. Publ. **800**(146) (2012) 81
3. Boyens, J., Paulsen, C., Moorthy, R., Bartol, N.: Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Spec. Publ. (2015)
4. Dawes, R.M.: The robust beauty of improper linear models in decision making. Am. Psychol. **34**(7) (1979) 571–582
5. Djemame, K., Armstrong, D.J., Kiran, M.: A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. Computing (c) (2011) 119–126
6. Fito, J., Macias, M., Guitart, J.: Toward business-driven risk management for Cloud computing. Netw. Serv. Manag. (CNSM), 2010 Int. Conf. (2010) 238–241
7. Freund, J., Jones, J.: Measuring and Managing Information Risk. (2015)
8. Ghadge, A., Dani, S., Chester, M., Kalawsky, R.: A systems approach for modelling supply chain risks. Supply Chain Manag. an Int. J. **18**(5) (2013) 523–538
9. Gresh, D., Deleris, L.A., Gasparini, L., Evans, D.: Visualizing risk. In: Proceedings of IEEE Information Visualization Conference. (2011)
10. Islam, S., Fenz, S., Weippl, E., Mouratidis, H.: A Risk Management Framework for Cloud Migration Decision Support. Journal of Risk and Financial Management **10**(2) (2017) 10
11. Kaliski-Jr, B.S., Pauley, W.: Toward Risk Assessment as a Service in Cloud Environments. Proc. 2nd USENIX Conf. Hot Top. cloud Comput. (2010) 1–7
12. Olcott, J.: Input to the Commission on Enhancing National Cybersecurity: The Impact of Security Ratings on National Cybersecurity (2016)
13. Palisade: Monte Carlo Simulation: What Is It and How Does It Work? - Palisade (2017)
14. Pearson, S.: Data Protection in the Cloud. Cloud Security Alliance Online (2016) 10–13
15. Saripalli, P., Walters, B.: QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. 2010 IEEE 3rd Int. Conf. Cloud Comput. (2010) 280–288
16. Sendi, A.S., Cheriet, M.: Cloud Computing: A Risk Assessment Model. 2014 IEEE Int. Conf. Cloud Eng. (2014) 147–152
17. Sherman, M.: Risks in the Software Supply Chain. Softw. Solut. Symp. (2017) 1–36
18. Sivasubramanian, Y., Ahmed, S.Z., Mishra, V.P.: Risk Assessment for Cloud Computing. International Research Journal of Electronics and Computer Engineering (ISSN Online: 2412-4370); Vol 3 No 2 (2017) (2017)
19. Sourcemap: Sub-Supplier Mapping : Tracing Products to the Source with a Supply Chain Social Network. (2011) 5