A Holistic Model for Making Cloud Migration Decision

-A Consideration of Security, Architecture and Business Economics

Bjorn Johnson
Colorado Technical University
Colorado Springs, CO 80907, USA
johnsonb2@asme.org

Yanzhen Qu
Colorado Technical University
Colorado Springs, CO 80907, USA
yqu@coloradotech.edu

***Abstract*—The emergence of cloud computing services has created an additional dimension in the decision for creating a new business plan which requires computing resources. Although quite a few of the recent published analytical models have provided some very good ground work for assessing the cost difference between in-house systems and leasing cloud services for the same set of computing requirements, there is a need for research towards providing a company with risk analysis tools that will allow business managers to assess the viability of migrating business applications to the cloud with broader considerations. This article consolidates several genres of analysis on cloud computing risk. We derive an new analytical model that takes into account business economics, and other business requirements such as various considerations on security and availability. This model applies these considerations to the already well researched buy-or-lease models currently used by business management professionals which allows for an easy transition to this more thorough model. We made a comparison research through evaluating the service requirement situation from published research against two service providers. The results of this research demonstrates the veracity of our model. The rationale for this research is to provide a more complete and robust model that encompasses the entire spectrum of considerations yet holds a high degree of precision.**

Keywords*- *cloud computing, security, business modeling, logistic regression, risk analysis

I. Introduction

The emergence of cloud computing services has created a new paradigm in business software development and business application implementations. It is clear that there are tangible benefits of cloud computing, for instance fast access to additional computational power and Information Technology (IT) skills [1]. Also the ability to address volatile demand patterns with additional resources through cloud computing has reduced the risk of over/under provisioning on company's IT or Enterprise Information System (EIS) infrastructure [2]. There is, however, the emergence of a more convoluted set of variables that need to be taken into consideration when deciding on a business plan that incorporates software applications, files storage, computational needs, or platform services. In example, loss of governance and control over resources could lead to ambiguity in the roles and responsibilities of personnel [3]. Cloud computing (as well as grid and cluster computing) continues to aim at allowing access to large amounts of computational power and virtual computing space [4] thus attracting more potential utilization from corporations looking for IT options. The decision business managers now have to determine is whether the risk of migration to cloud services is scalable, secure and generates the required Return-On-Investment (ROI).

Coincidental to the emergence of cloud computing, there has been the emergence of research on the viability of cloud services. However due to the infancy of cloud computing, there is a limited amount of data available for research. The current research also segregates variables in the decision model such as business motivation or security and does not focus on a holistic view of the situation [5–10]. For example, most of the existing research work has only focused on comparing the cost between hosting a set of computing resource in-house verse leasing the same set of computing resource from cloud service providers. Although this type of research has grasped certain essential aspects of cloud computing, due to oversimplified assumptions the research work has made, the conclusions based on this type of research sometimes can be either impractical or sometimes incorrect. Also most of the existing research are convoluted and directed to IT professionals or economics mathematicians[11–14], and not to the business managers who need to make the decisions based on broad scope of, sometimes conflicting, business requirements.

In this research we have created a model which takes into account a much broader scope of business considerations including business economics, security, availability as well as other quality of service attributes, that can be used to inform decision makers on whether to migrate services to the cloud. We then place the model against a use case for a medium sized company that has been reported in another published research work [14]. We demonstrated that in some cases, we may conclude quite differently after considering much broader business requirements than what the author of [14] has concluded after considering much broader business requirements.

This paper is structured as follows. Section II presents an extensive literature review on the past attempts to create decision support models and their contributions. Section III is the problem statement and the hypothesis. Section IV presents our model with definitions and descriptive reasoning for their use. Section V provides the application of the model against a typical business consideration for migrating storage requirements to the cloud, and also describes the results of the computations and analysis application. Finally, Section VI concluding remarks develops the final recommendations.

II. Related Work

Researchers in this field are comprised mainly of two sets which has inherently left the research bifurcated. There are IT researchers that have conducted analysis on the security, architecture, availability and quality of cloud computing. There are also business economics researchers that have tried to assess business risk on a buy-or-lease type paradigm.

A. Business Considerations

As with any process that inherently contributes to the bottom line of corporations, thorough business practices need to be taken into consideration. In his look into the economics of cloud computing, Walker [13] emphasized the fact that business organizations have been conducting research on buy-or-lease economics for over 40 years. Further work to model the buy-or-lease decision for data storage led Walker et al [14] to use basic buy and lease present value estimates to derive a function that evaluates the efficacy of leased storage compared to adding infrastructure. They provided a hypothetical use case for a medium and large business model and showed that their derivation provided a sound estimate for decision making. Their derivation only takes into account business motivational factors dealing with data storage and is self-admittedly an initial catalyst to stimulate discussion, debate and future work in the benefits of leasing versus buying storage. Our model looks at a more holistic view of cloud computing services and there corresponding risk factors.

Klems et al [15] provided a conceptual framework for comparing the viability of cloud computing over the costs of IT infrastructure. They ran their model against two use cases; first was the New York Times Time Machine which required large access to data with varying periods of demand volume. The second was Major League Baseball Website hosting which fell into the realm of peak seasonal demand. Due to the early nature of their research no results were posted for comparison. Conversely, we subsidize the sparse data with an example to provide tangible results for analysis and future research.

Research into managerial considerations has been conducted to evaluate the risk of managing a system deployed on several clouds. The possible need for extra management personnel to liaison with various cloud providers could be considered a hidden cost of cloud computing [11]. As a result researchers have determined that this extra managerial requirement is a critical information point that needs to be provided to the business decision makers [1], [16], [17]. Our model incorporates this hidden cost by utilizing the *leased asset's net present value* (LNPV) for business cost considerations which factors in additional managerial personnel into the equation.

B. Security Considerations

Though there are many technologically based benefits for migrating to the cloud, such as universal access [18], [19], simplified disaster provisioning [20], [21] and reduced run response time [2], [20], [22], [23], the primary hindrance to migration to the cloud is most recognized as an inability to determine the security of service providers and the lack of security protocols. In their technical paper for Gartner, Inc., Heiser and Nicolett presented a process for assessing the security risks of cloud computing [24]. They provided a definition for several evaluation criteria which includes privileged user access, compliance, data location, data segregation, availability, recovery, investigative support, viability, and support in reducing risk. They offered guidelines for how a company should proceed on an evaluation and provide recommendation to either hire internal personnel to conduct the evaluation or contract out to an agency that can conduct such assessments. Though very clear in the definition of each subject area and its propensity to help or hinder an assessment they did not describe methods or derive models in which to conduct the evaluation. There identification of security subject areas is profound and well stated and provides a basis for the security considerations in this research.

The types of attacks possible in cloud providers is quite similar to those faced by every business. There is an escalating factor since multiple organizations can be adversely affected by these attacks. Researchers have recommended network monitoring tools placed outside of the cloud provider to detect or intercept attacks such as denial of service [5–7], [25]. Another concern is interception of data management messages that could lead to third party manipulation of data. The use of secure communications protocols and multiple authentication has been recommended to mitigate this risk [5]. Vulnerabilities, particularly those concerning browsers can be overcome with the use of security updates via the software provider [7], [26]. It is clear through the list of possible security risks to cloud computer providers and their clients that a model must incorporate mitigation of these risks.

Though most research regarding security is interested in the provider's security model or methods and practices, there is another needed consideration; how critical is the information to the company? Highly critical information or data is that data that would cause the company great harm should it be lost or disclosed to outside agencies (competitors, foreign nations, etc...). Ranking data sensitivity will provide a value for the security computation. Misra and Monda [12] presented this type of data sensitivity classification which has been further defined in this research, to include incident values. The highest level of criticality is federal government and intelligence agency data; data concerning national security and national defense or military information. This is incrementally reduced down to a 'not sensitive' category which is categorized as free software, blogs, and any authorized downloaded material such as pictures, or music. Misra and Monda provided a numeric value to each category through a score card[12]. This method is not adopted though since at its maximum value the total security impact to their fitness computation is less than ten percent of all considerations. For this reason a we will use a logistic regression to provide a more vociferous factor in the calculation.

Finally, Khajeh-Hosseini et al. [11] provided a rigorous survey of benefits and risks in cloud computing based on organizational, legal, security, technical, and financial considerations with currently researched mitigations for each risk. Our research furthers this work by distilling these risks into calculable criteria and combining them with a Likert scale [27] to evaluate the efficacy of a provider's security and availability offerings for incorporation into the model.

C. Availability Considerations

Our final consideration deals with availability of the computing resources from cloud providers. Like security, availability is twofold. Of less concern due to modern high performance computing standards is the availability due to system architecture. Successful providers will have the adequate back-up hardware and systems to ensure above 99% availability. This should be confirmed based on the fact that commercial enterprises often outsource more than they can handle. It should be assessed whether the provider’s hardware is adequate to source the current work load and the future work load goals. Over selling of computational time can lead to availability problems. Also, recent outages from Google, Salesforce and Amazon has demonstrated a failure to deliver services due to architectural or system hardware limitation [28].

The primary concern is the interoperability of systems and the cost inherent in getting all software systems to communicate. It has been suggested that cloud middle-ware is a viable solution for this problem [5] but it adds additional cost to the lease consideration and must be a point of information given to business economists calculating the buy-or-lease formula. The inability to compute on all of the cloud provider's resources will adversely affect your availability.

Amburst et al. [29] discussed several availability short comings that affect clients. Financial viability of the provider and the provider's efficacy in the market was of primary concern. The practice of poor business planning on behalf of the provider could result in financial ruin, bankruptcy and going out of business. This could leave a company that is well invested in the services of the provider without the means to conduct business. The researchers mitigate this problem with a well balanced utilization of several cloud providers typical to having a well dispersed stock portfolio. This method, though, multiplies work needed to assess the risk of multiple companies thus increasing the initial cost.

The last consideration should be to your service contract and your priority among the other customers the provider is servicing. You may have a priority level that causes you to be without services while other, higher priority customers are serviced. The service level agreement should be given close scrutiny on what level of priority of service you will be given.

III. Problem Statement and Hypothesis

A. Problem Statement

Current analytical models for determining the viability of migrating business applications to the cloud rarely consider both business economics as well as other business requirements such as security and architectural risk factors. This causes a less informative model for decision makers to use in business strategy planning which can lead to improper determination of a service provider's fitness causing increased, yet hidden, risk.

B. Hypothesis

An analytical model encompassing both business economics offset by security and architectural risk analysis factors will provide a more in depth statistical description of cloud migration benefits and risks to business applications.

IV. Methodology

These same considerations evaluated in the literature are used to derive the model and computational methods for the model and application.

A. Business Economics Considerations

The first business consideration is business economics. At the basic level this is accomplished through a *purchased asset's net present value* (PNPV) [30]. Calculating this value for a set of variables will provide the net profit expected by purchasing the computing asset and resources needed to provide the computational service. Conversely, the *leased asset's net present value* (LNPV) will provide the expected profit from leasing the same computing asset and resources [31]. The PNPV is expressed as a sum over the life of the purchased computing asset:

$$PNVP = \sum_{t=0}^{n} \frac{R_t^P - C_t^P - E_t^P}{(1+I)^t} + \frac{S}{(1+I)^n} \quad (1)$$

Where R_t^P is the annual revenue resulting from the purchased computing asset and resources in year *t*. C_t^P is the expected annual operating cost of computing assets and resources in year t. I is the interest rate due on the debt procured to finance the purchase of computing asset and resources[32]. The variable n is the expected life of the computing asset and resources in years, S is the asset's estimated salvage value and E_t^P is the amortized capital cost of the purchased computing asset and resources in year *t*.

Thusly, the LNPV is the sum of the revenue minus the lease cost per year of operation and can be expressed as:

$$LNPV = \sum_{t=0}^{n} \frac{R_t^L - C_t^L - F_t^L}{(1+I)^t} \quad (2)$$

Where R_t^L and C_t^L are the expected profit and company's cost for the leased computing asset and resources. Cost in this case is a function of administering the lease and uploading files, data or applications as needed. It does not imply any cost held by the cloud service provider. *t* is the current year, F_t^L is the annual leasing fee in year *t* and I is the interest rate for any subsequent financing for the cloud service lease[33].

It then follows that we can derive △NPV from the difference of the PNPV and the LPNV [14]. This formula becomes the basis for our model since it now takes into account the basic business economics between purchasing or leasing. The criteria for making a decision should be to buy if

$\triangle$NPV > 0 and to lease should $\triangle$NPV ≤ 0. This differs from Walker et al since they include zero in the buy criteria (no explanation given). We include zero in the lease criteria for the consideration that all other factors being equal (PNPV = LNPV) it is physically less work to lease the service then it is to install, use and then salvage the hardware. For instance, leasing does not require the hiring of installation personnel or additional administrators nor the need for post operational salvage activities and thus is deemed the simpler solution. The base equation for further derivation is:

$$\triangle NPV = PNPV - LNPV = NPV' \tag{3}$$

If we assume $R_t^P = R_t^L$:

$$NPV' = \sum_{t=0}^{n} \frac{(F_t^L + C_t^L) - (C_t^P + E_t^P)}{(1+I)^t} + \frac{S}{(1+I)^n} \tag{4}$$

B. Other Business Requirements Considerations

With a well defined and mature derivation of the business economics for buy-or-lease analysis, a close look at other stimuli needs to be taken in order to evaluate any factors that will have an effect on the behavior of the base equation. These factors are identified, derived and applied to the base model starting with concerns about security in the cloud.

We have identified several aspects that are important in modeling security risks in a cloud environment.

1) Compliance: Considerations to be taken into account for compliance are twofold. First there is the cloud service provider's compliance with standard Internet and IT security. Do they have trained security professional on staff and do they comply with regulatory measures for Internet security? This can be a difficult assessment since there is no clearly defined regulation yet for cloud computing but it is quite easy to apply standard corporate practice evaluations on the cloud service provider. For instance do they have a sufficient firewall to prevent intrusion? What is their protection against Mal-ware? These questions can be based against any standard regulatory governances that control business. Second is the providers compliance with inspection [24]. Is the cloud service provider amicable to inspection by prospective customers or third parties hired to assess security in a company? This could be a telling factor on whether the provider is truly secure and willing to demonstrate their measures or whether they are professing abilities or securities they do not actually employ.

2) Data Location: Data location can be the basis for a large amount of concern. Considering possible sensitive national security data, it is clear that an organization will not want a cloud service provider to use computational assets in a country not allied with the customer. Therefore there is a need to look at the different geographical areas the provider has assets. Also, you will need to assess the cloud service provider's ability to control the segregation of your data to ensure that it can be controlled.

3) Recovery: Recovery deals with the provider's ability to recover data and minimize the down time that may occur due to a disaster that affects their assets. The main factor to consider is whether or not they have a disaster recovery plan. You should be able to review the recovery plan to verify whether they are *compliant* with industry standards and the needs of your business operation requirements.

4) Data Sensitivity: The last factor in the security aspect of a decision model is the sensitivity of your data. This assessment should be easily evaluated through your own business security practices.

Another final architectural related business consideration is the availability of the cloud services and the cloud services provider. Availability is the long-term viability of the cloud service provider. Are they financially secure and do they have plans and processes to ensure survivability of the organization at least through the duration of your required computational needs? You must also consider what happens should the provider falter. How are assets, that might hold your data, going to be liquidated? Again a *compliant* cloud service provider should be able to answer these questions.

C. Model Other Business Requirements

We use a logistic regression model to capture all the considerations mentioned previously as the probability of the need to lease more computing asset and resources. For example, to address availability consideration, we may need to lease more virtual machines for backup and restore functions. Also, to address security consideration, we may need to lease more storage space and more network bandwidth to store and transfer data in encrypted format. To this end, the predictor variables of the regression were generalized to allow for the widest application across the *aaS architecture. The regression is defined in equation (5). Equation (6) shows the derivation for the predictor variable and the coefficients. The coefficients were resolved by the analysis of randomly generated data sets for the values in Table (1).

$$\delta(z) = \frac{e^z}{1+e^z} = \frac{1}{1+e^{-z}} \tag{5}$$

$$z = b_0 + b_1(X_2) + b_2(X_2) + \ldots + b_n(X_n) \tag{6}$$

Where the probability that an observation is a member of a given class is given by $\delta(z)$, X_n is the observation and z the summation of the intercept b_0 and the coefficient b_n times the variable X_n for each of the trait variables described above.

To use this model, we first need to define the set of predictor variables. Based on the discussions above, we have chosen our predictor variables as follows:

- Architecture (A) – those factors dealing with the hardware and software of the cloud service provider, e.g. Communication protocols, encryption and virus protection.
- Compliance (C) – those factors that deal with the cloud service providers compliance with government and community regulation

- Personnel and Facilities (P) – those factors that deal with the training and vetting of personnel and the cloud service provider's facilities
- Transparency (T) – those factors that deal with the cloud service providers propensity to be forthcoming with certain aspects of security, performance and financial stability
- Data Sensitivity (D) – those factors that deal with the level of sensitivity of the data that will be migrated
- Availability (AV) – those factors that deal with the availability of and assurance of availability of the cloud service provider

The combination of these predictor variables in Equation (6) and randomly generated data was then processed using R statistical library functions to generate the regression intercept and predictor variables' coefficients. To accurately determine the coefficients a total of 1000 cases was used. The results of which are presented in Table 1.

Table 1: Regression predictor variable coefficients. P value resolving to zero shows a high statistical significance.

Coefficients	Estimate	Std. Error	t Value	Pr(>|t|)
(Intercept)	-2.48053	0.10935	-22.684	<2e-16
Architecture	0.18672	0.01742	10.716	<2e-16
Availability	0.21706	0.02006	10.821	<2e-16
Compliance	0.1934	0.01761	10.984	<2e-16
Data Sensitivity	0.23293	0.00673	34.613	<2e-16
Personnel/Facilities	0.18815	0.02023	9.301	<2e-16
Transparency	0.18019	0.01849	9.747	<2e-16

As is shown in Table 1 the P value is essentially zero for all coefficients thus showing that their contribution is statistically significant. We can then use these values to calculate the logistic regression as follows:

$$\begin{aligned} z &= b_{+0} + b_1(A) + b_2(C) + b_3(P) \\ &+ b_4(T) + b_5(D) + b_6(AV) \\ &\Rightarrow -2.48053 + 0.18672(A) + 0.19340(C) \\ &+ 0.18815(P) + 0.18019(T) + 0.23293(D) \\ &+ 0.21706(AV) \end{aligned} \tag{6}$$

D. A Unified Model

Because we have transformed all other business considerations into a probability of the need to lease more computing asset and resources from the cloud providers, it is very natural to consider δ(z) as a “cost adjustment factor” for both F_t^L and C_t^L . Therefore we can combine Equation (4) and Equation (5) into one equation. The resulting model from the inclusion of both business economics and other business requirements such as security and availability towards the lease cost is then:

$$NPV' = \sum_{t=0}^{n} \frac{(1+\delta(z))(F_t^L + C_t^L) - (C_t^P + E_t^P)}{(1+I)^t} + \frac{S}{(1+I)^n} \tag{7}$$

Where is δ(z) defined by Equation (5). The remaining variables are the same as defined in the previous equations. Comparing Equation (4) and Equation (7), we can clearly see that δ(z) will play a role in deciding the final outcome of NPV'. Therefore it does prove our claim in both our problem statement and our hypothesis statement.

V. Application of the Model

In order to demonstrate the value of our model, we have applied it to a published use case from the literature. Using tenants of Walker, Brisken and Romney's [14] medium sized company, our example is that of a company looking to migrate storage requirements to the cloud. Walker, Brisken and Romney determined that this would be a prime example of cloud resources outperforming infrastructure in cost. They, however, did not consider security or availability in their model. We show, via our holistic model, that this inclusion adds another level of depth to the evaluation and an apparently sound determination to migrate to the cloud can be reversed due to poor service provider fitness.

A. The Service Providers

For the example we developed two service providers, Provider A and Provider B, and evaluated them against the criteria built into our model. Both providers are considered to be within 3 percent of cost of each other which concludes to a positive outcome from the standard buy-or-lease evaluation for each service provider.

As shown in Table 2, the service providers' scores, which are the data values for the set of six predictor variables such as A, C, P, T, D and AV, were made to differ drastically giving one service provider who scored high and one service provider who scored low.

Table 2: Two providers' values for predictor variables

Predictor Variables	A	B
ARCH	1	5
COMP	2	3
PER/FAC	1	4
TRANS	0	4
DAT/SEN	0	0

B. The Client

As mentioned above the client is a medium sized company of tens to hundreds of servers which represents 50% of companies in the United States in 2007. For this example we will consider the company requires an additional 10 Tb of storage with a 1 Tb increase over the next 10 years. The first option would be to purchase the drives and install and operate them on the premises. To do this it is estimated that an annual salary of 35,000 will be required which we adjust for cost of living by 3% each year. We estimate a $350.00 cost for the drives and a $2000.00 cost for the RAID controller which can each handle 5 drives. Typical energy consumption for the equipment is placed against an average electrical cost for the United States in 2011. An annually depreciated salvage cost is estimated to finish the requirements for the purchasing options.

For the lease option, it is assessed that company employment requirements will be but a fraction of the full time operator required to manage hardware infrastructure. Also, the lease cost is estimated, for the volume required, from Ubuntu One advertised per month storage pricing neglecting any possible large volume discounts offered by the provider.

The numbers were calculated and then put into the model twice, once with provider A and once with provider B. The variable values and the outcome are shown in Table 3. It should be noted that with a well evaluated provider the outcome of the model is similar to that of Walker, Brisken and Romney but the depth of confidence is greater since the additional considerations where taken into account. Also for the less suited provider the decision to migrate to the cloud is less advantageous in lieu of adding infrastructure

Table 3: Evaluation of service provider fitness using our holistic model. Results show that for the same service requirement, recommendations differ now that security and availability are considered.

Year	Required Tb	Drives Purchase	Drive cost	Salary Purchase	Utilities Purchase	RAID Controller Purchase	Salvage (S)	Capital Cost (E^P)	Operating Cost Purchase (C^P)	Operating Cost Lease (C^L)	Lease Cost (F^L)	ΔNPV Service Provider A	ΔNPV Service Provider B
1	10	10	$3,500.00	$35,000.00	$280.51	$4,000.00	$875.00	$7,500.00	$35,280.51	$8,750.00	$15,000.00	-$12,752.78	$2,190.07
2	11	1	$350.00	$36,050.00	$248.95	$2,000.00	$306.25	$2,350.00	$36,298.95	$9,012.50	$16,500.00	-$7,017.02	$8,720.00
3	12	1	$350.00	$37,131.50	$248.95	$0.00	$164.06	$350.00	$37,380.45	$9,282.88	$18,000.00	-$4,118.05	$12,381.02
4	13	1	$350.00	$38,245.45	$248.95	$0.00	$128.52	$350.00	$38,494.40	$9,561.36	$19,500.00	-$3,100.09	$14,129.91
5	14	1	$350.00	$39,392.81	$248.95	$0.00	$119.63	$350.00	$39,641.76	$9,848.20	$21,000.00	-$2,117.38	$15,813.39
6	15	1	$350.00	$40,574.59	$248.95	$2,000.00	$117.41	$2,350.00	$40,823.55	$10,143.65	$22,500.00	-$2,963.30	$15,639.03
7	16	1	$350.00	$41,791.83	$248.95	$0.00	$116.85	$350.00	$42,040.78	$10,447.96	$24,000.00	-$313.03	$18,932.60
8	17	1	$350.00	$43,045.59	$248.95	$0.00	$116.71	$350.00	$43,294.54	$10,761.40	$25,500.00	$506.14	$20,367.69
9	18	1	$350.00	$44,336.95	$248.95	$0.00	$116.68	$350.00	$44,585.91	$11,084.24	$27,000.00	$1,271.50	$21,722.45
10	19	1	$350.00	$45,667.06	$248.95	$0.00	$116.67	$350.00	$45,916.02	$11,416.77	$28,500.00	$1,984.55	$22,999.27
											Total ΔNPV	-$28,619.45	$152,895.43

C. Results

It was shown that security and availability play a pertinent role in the business evaluation for cloud migration. It is clear from the application example that the two service providers do not evaluate equally and a company considering use of either should choose to lease from service provider B. Also, it is clear that if only service provider A was available the company should invest in internal infrastructure to solve their storage requirement as the risk of using service provider A is much too great. Conversely, if service provider B was the only option besides infrastructure improvements it is clear that leasing from service provider B is a viable, low risk option and should be seriously considered.

VI. Conclusion

In this paper we have demonstrated a holistic model that takes into consideration broader business and IT motivations and concerns. Specifically, it was proven that there needs to be consideration for both security and availability in the decision support models for cloud migration. These then can be added to the business economics formula in order to consolidate the evaluation and assessment. To this end, the contribution of this work is twofold:

- We have presented a unified model for assessing a cloud service provider through several facets to include business economics, and other business considerations such as security and availability.
- We have also provided standard criteria for assessing the security and availability of cloud providers and allow for a calculable value from this assessment.

Our example showed the difference between taking these factors into consideration and not considering them. This resulted in the risk for identical service requirements being evaluated differently between two service providers, an outcome that would not have been discovered with a standard buy-or-lease analysis.

Reference

[1] J. Dibbern, T. Goles, R. Hirschheim, and B. Jayatilaka, “Information systems outsourcing: a survey and analysis of the literature,” *ACM SIGMIS Database*, vol. 35, no. 4, 2004, pp. 6–102.

[2] M. Armbrust et al., “Above the clouds: A berkeley view of cloud computing,” Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

[3] A. Khajeh-Hosseini, I. Sommerville, and I. Sriram, “Research challenges for enterprise cloud computing,” *Arxiv preprint arXiv:1001.3257*, 2010.

[4] R. Buyya, J. Broberg, and A. G. sci nski, *Cloud computing*. Wiley Online Library, 2011.

[5] D. Catteddu, “Cloud Computing: benefits, risks and recommendations for information security,” *Web Application Security*, 2010, pp. 17–17.

[6] R. Clarke, “Computing clouds on the horizon? Benefits and risks from the user’s perspective,” *23rd Bled eConference*, 2010.

[7] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On technical security issues in cloud computing,” in *Cloud Computing, 2009. CLOUD’09. IEEE International Conference on*, 2009, pp. 109–116.

[8] A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, “Cloud migration: A case study of migrating an enterprise it system to iaas,” in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 2010, pp. 450–457.

[9] P. C. Palvia, “A dialectic view of information systems outsourcing: pros and cons,” *Information & Management*, vol. 29, no. 5, pp. 265–275, 1995.

[10] L. Mastroeni and M. Naldi, “Long-range Evaluation of Risk in the Migration to Cloud Storage,” in *Commerce and Enterprise Computing (CEC), 2011 IEEE 13th Conference on*, 2011, pp. 260–266.

[11] A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, and P. Teregowda, “Decision Support Tools for Cloud Migration in the Enterprise,” in

Cloud Computing (CLOUD), 2011 IEEE International Conference on, 2011, pp. 541–548.
[12] S. C. Misra and A. Mondal, “Identification of a company’s suitability for the adoption of cloud computing and modelling its corresponding Return on Investment,” *Mathematical and Computer Modelling*, vol. 53, no. 3, pp. 504–521, 2011.
[13] E. Walker, “The real cost of a CPU hour,” *Computer*, vol. 42, no. 4, pp. 35–41, 2009.
[14] E. Walker, W. Brisken, and J. Romney, “To lease or not to lease from storage clouds,” *Computer*, vol. 43, no. 4, pp. 44–50, 2010.
[15] M. Klems, J. Nimis, and S. Tai, “Do clouds compute? a framework for estimating the value of cloud computing,” *Designing E-Business Systems. Markets, Services, and Networks*, pp. 110–123, 2009.
[16] B. A. Aubert, M. Patry, and S. Rivard, “A framework for information technology outsourcing risk management,” *ACM SIGMIS Database*, vol. 36, no. 4, pp. 9–28, 2005.
[17] M. J. Earl, “The risks of outsourcing IT,” *Sloan management review*, vol. 37, pp. 26–32, 1996.
[18] J. F. Rayport and A. Heyward, “Envisioning the cloud: The next computing paradigm,” *Whitepaper. Marketspace*, 2009.
[19] D. Chappell, “Windows Azure and ISVs,” Technical report, Microsoft. http://www. microsoft. com/windowsazure/whitepapers, 2009.
[20] J. Varia, “Architecting for the cloud: Best practices,” *Amazon Web Services, Jan*, 2010.
[21] T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, J. Van Der Merwe, and A. Venkataramani, “Disaster recovery as a cloud service: Economic benefits & deployment challenges,” in *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*, 2010, pp. 8–8.
[22] J. Carolan et al., “Introduction to Cloud Computing architecture-White Paper,” 2009.
[23] K. Jeffery and B. Neidecker-Lutz, “The Future of Cloud Computing Opportunities for European Cloud Computing Beyond 2010,” *European Commission Information Society and Media*, 2010.
[24] J. Heiser and M. Nicolett, “Assessing the security risks of cloud computing,” *Gartner Report*, 2008.
[25] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,” in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 199–212.
[26] S. Mansfield-Devine, “Danger in the clouds,” *Network Security*, vol. 2008, no. 12, pp. 9–11, 2008.
[27] R. Likert, “A technique for the measurement of attitudes.,” *Archives of psychology*, 1932.
[28] W. Michalk, B. Blau, J. Stosser, and C. Weinhardt, “Risk-Based Decision Support in Service Value Networks,” 1999, pp. 1–9.
[29] M. Armbrust et al., “A view of cloud computing,” *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[30] P. F. Anderson and J. D. Martin, “Lease vs. Purchase Decisions: A Survey of Current Practice,” *Financial Management*, pp. 41–47, 1977.
[31] R. W. Johnson and W. G. Lewellen, “Analysis of the lease-or-buy decision,” *The Journal of Finance*, vol. 27, no. 4, pp. 815–823, 1972.
[32] W. G. Lewellen, *The cost of capital*. Wadsworth Pub. Co., 1969.
[33] G. B. Harwood and R. H. Hermanson, “Lease-or-Buy Decisions,” *J. Accountancy*, vol. 142, no. 3, pp. 83–87, 1976.
[34] J. A. Sokolowski and C. M. Banks, Modeling and simulation fundamentals: theoretical underpinnings and practical domains. Wiley, 2010.