A Decision Framework Model for Migration into Cloud: Business, Application, Security and Privacy Perspectives

Shareeful Islam
School of Architecture, Computing and Engineering
University of East London
United Kingdom
shareeful@uel.ac.uk

Edgar R. Weippl
SBA Research
Favoritenstraße 16
1040 Vienna, Austria
EWeippl@sba-research.org

Katharina Krombholz
SBA Research
Favoritenstraße 16
1040 Vienna, Austria
KKrombholz@sba-research.org

ABSTRACT

Cloud computing offers a different, affordable approach for supporting the IT needs of organisations. However, despite the unprecedented benefits cloud migration may bring, there are numerous difficulties involved in moving business critical applications, legacy systems or corporate data into the cloud.It is necessary to consider a broad view over all business areas, and taking into account the technical and business minutiae of a full scale cloud migration, as well as the wider concerns of security, privacy and other business and technical risks. A detailed understanding of all these areas is required in order to make the correct decisions concerning cloud migration. This paper aims to take a broad view of the issues relating to migration. We propose a process model to identify risks and requirements, as well as to provide control assurance during the migration decision. We also define an outline migration strategy by focusing on the context of the organisation.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*; D.2.9 [**Software Engineering**]: Management—*software process model*

General Terms

Theory Cloud computing, Requirements, Process Model

Keywords

cloud migration, risk management, security, privacy

1. INTRODUCTION

IT infrastructure is shifting from locally managed software enabled platforms and physical hardware to outsourced virtual infrastructure managed by *Cloud Service Providers (CSP)*. Benefits such as cost reduction, reduced maintenance overheads and flexibility in computation provide a powerful motivation for an organisation to migrate into cloud. Organisations are now quickly becoming reluctant to purchase more in-house hardware and software, even for business-critical functions. Both small and large organisations are seriously considering adopting cloud computing as a strategic decision, with new technology and business collaboration ([6, 3]). However the benefits and advantages of Cloud Computing must be balanced against the risks. In particular, risks concerning security, privacy, financial aspects and the wider organisation are vital, and require serious consideration before a cloud migration. CSP may not provide adequate technical measures to manage and protect user's data comparing to the traditional outsourcing. A recent cloud migration research review by [4] emphasises the necessity of a comprehensive migration framework to support an organisation through the migration decision.

In order to efficiently come to the correct decision about cloud migration with respect to business needs, an organisation should be able to objectively consider the aggregated risks of cloud adoption as determined by [7]. Appropriate justification is necessary to align the cloud strategy with existing business models, potentially also revising the current business model, taking into account the new dimension of collaboration, new dependencies and requirements, and dealing with customer needs in a cloud environment. The process of a cloud migration is therefore a complex undertaking, depending on many factors that contribute both for and against a decision to migrate. This work looks to move in this direction; in particular we develop a decision framework model that takes into account a much broader range of decision components, including business needs, security, and privacy, and identifies a number of important attributes from each of them. The proposed process within the framework considers an organisation's potential needs in the cloud, and analyses risks, requirements and assurances in support of those needs. This work looks to help provide a simpler, informed decision making process that is applicable to any size of organisation, and both those for whom the cloud may or may not be the best decision.

2. RELATED WORK

There are works that focus on the issues relating to cloud migration. Johnson and Qu (2012) develop an analytical holistic model based on business economics for analysing cloud migration risks [5]. Klems et al. [8] proposes a concep-

iiWAS2014, 4-6 December, 2014, Hanoi, Vietnam.

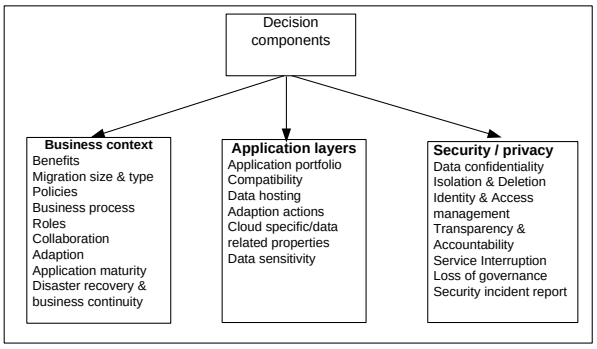

Figure 1: An Overview of Decision Components

tual model for comparing IT infrastructure costs and cloud computing viability, although the results of the use cases do not show the applicability of the model. [7] introduces cost, benefits and risk tools for public IaaS cloud migration decisions. Risks are considered from organisational, legal, security, technical and financial perspectives. however, most of the existing works focus on comparing the cost of hosting models between in-house and outsourced cloud contexts without analysing critical decision components such as business context, security, and privacy. Jamshidi et al. [4] perform a systematic literature review of cloud migration research; the results show that there is a lack of works focusing on a comprehensive decision framework for cloud migration. In particular, a decision framework should support the organisations in undertaking their migration decision by analyzing requirements, feasibility and migration strategies, along with the execution, evaluation and cost cutting concerns of the move. This work contributes towards filling these gaps by proposing a decision framework taking into account an in-depth understanding of the business, security and privacy needs based on the organisational context.

3. DECISION COMPONENTS

The decision framework components aid in the understanding of the existing state of the organisation before any cloud migration. Their primary purpose is to extract key attributes and aid in the collection of data useful for the decision making process. We reviewed the existing literature based on six main keywords (cloud migration, application, security, privacy, business context and risks), along with our three inclusion criteria of decision factors for migration into the cloud, methods and tool support for migration, and risks before and after the migration. Based on our review, we can define three main decision components: *business context*, *application*, and *security and privacy*. Figure 1 shows the decision components with key areas. An overview of individual components is given below. This section provides a brief overview of each component.

Business Context.

Business context considers the issues based on the business and organisational needs; for example, organisation entities, IT usage, costs and benefits of migration, role and size of the migration, future business needs, and the cloud portfolio both before, during and after the migration decision. The current state of the organisational and business entities (goals, infrastructure provisioning, business and IT policies, access capabilities, SLA, upfront costs) are analysed to understand the requirements of the migration. Such analyses support the understanding of how the migration affects the organisation, and whether existing policies, roles and responsibilities and the organisationś business strategy will need to be revised. Business context determines the cloud portfolio, indicating the chosen cloud model and other necessary parameters to support the migration.

Application.

Before migrating an application to the cloud, it is necessary to understand the applicationś characteristics without using any cloud technologies. Various factors must first be analysed, such as application type, in-house deployment and application maturity, a determination of the operation of the application in mixed in-house and cloud environments (Cloud-native or Cloud-enabled), along with looking at data storage, programming models, and quality assurance. Generally, an application is structured upon presentation, business and data layer [2]. This layer based abstraction helps determine which part (or all) of the application could migrate into the cloud. The business layer is responsible for managing business functionalities using business process, services and their supporting infrastructure. A number of issues must be considered before any cloud migration: for instance, identification of business process logic, business service and application components, supporting infrastructure, KPI and their adaptability into the cloud. The Business Layer communicates with the Database Layer located on both non-cloud and cloud data stores. It is clear that any amendment of cloud data stores and services should not affect the business layer. The Data Layer is responsible for data storage for an application through Data Access Layer (DAL) and Database Layer (DBL). Migrating the data layer into the cloud requires the migration of the DBL into cloud and adaption of DAL for managing the access control. Furthermore, it is also necessary to analyse compatibility issues such as database schema semantics and data types of the database so that there are no inconsistencies between the database layer before and after the cloud migration. It is for instance possible that the DBL could contain several instances, and parts of those instances could be migrated into the cloud. In that case, the synchronization of on-premises and off-premises parts can be achieved through the DAL.

Security and Privacy.

Security and privacy issues are among the most important concerns that primarily hinder the migration decision. A recent survey of potential cloud adopters indicates that security is the primary concern hindering its adoption [1]. It is therefore vital to understand security and privacy needs that are new to the cloud compared to traditional computing systems. Attacks against cloud infrastructure, such as resource depletion, unauthorized access, or DoS, are major challenges. The main challenge for an attacker is to find the target location, co-locate with the target on the same physical system and gather information about the target. [9] claims up to 40% success in co-residence with a target VM in an attack launched against Amazon EC2 instances. Attackers can map the cloud infrastructure to determine the location and use heuristics for the co-residency of VMs before exploiting the cross VM-leakage. When a security in-

cident is discovered, users need to know the details of the incident. In particular, providers' support for data layer migration and associated applications is one of the driving factors in the future expansion of cloud computing. Providers should ensure transparency of the data stored within their infrastructure. Furthermore, anonymity and pseudonymity of sensitive data stored in the public cloud must be ensured.

4. DECISION FRAMEWORK MODEL

When users intend to migrate their in house application into the cloud, it is necessary to understand the needs of both the application and user in adapting to the cloud environment, and how cloud provider supports these needs. We propose a systematic process to evaluate the usersńeeds and benefits, provider offers, risks and trade-off among these aspects. The proposed model provides a comprehensive understanding of these issues. Figure 2 shows the two main elements of the framework. The decision component includes attributes that need to be analysed for the migration decision. The process model includes activities and steps within the activity to support overall migration. The activities require active involvement of various roles within the organization context such as senior executives,business managers,IT staffs, auditors (Internal or External), and cloud service provider.

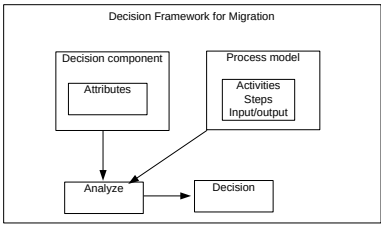

Figure 2: Decision Framework Elements

Migration Process.

A migration process is necessary to support a careful, systematic plan for a cloud migration. It covers tasks to facilitate major decision making, such as a study of migration feasibility, decisions as to which application sub-system is to be migrated, major risks to be controlled, and which cloud provider to choose. The process comprises four activities and each one has specific inputs and results in specific output artifacts. These artifacts should provide accurate information for the migration decision and process, and should be applicable within the existing business context. Figure 3 shows the steps involved within the activities.

Activity 1: Define Migration Portfolio: . This activity deals with the existing organisation context so that the appropriate migration portfolio can be defined and implemented if decision for migration is undertaken.

Step 1.1: Understand Organisational Context: . This step analyses the existing organisational context by identifying organisational entities such as actors, infrastructure, internal and external application, services, and data. Therefore, this step aims to define the extent of organisational entities that could potentially deployed into the cloud if the migration decision is taken.

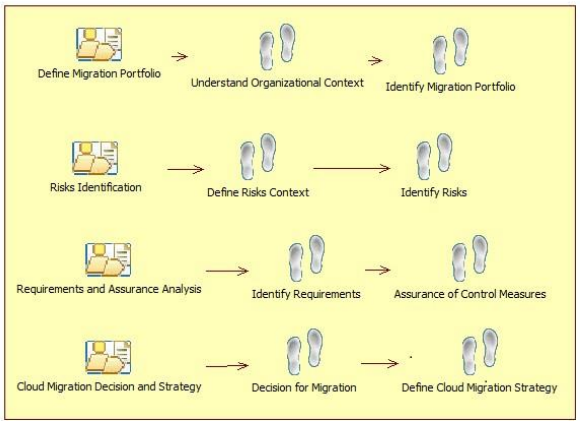

Figure 3: Activities and Steps for the Migration Process

Step 1.2: Identify Migration Portfolio. Migration portfolio rationalizes the migration needs and helps to undertake the critical strategic migration decision. This step needs involvement of key organisational people through brainstorming workshop(s) to identify key migration needs and to understand the whether cloud supports the existing business context. This step identifies several properties for the migration portfolio. They are given below:

- **Migration goals**: These goals are the main rationalization behind the cloud migration. This property emphasizes business value of the migration in terms of primary benefits.
- **Business process:** Business process amendment to adapt to cloud based infrastructure.
- **Policies:** Amendment of existing business and security policies due to new dependencies with the cloud provider.
- **Organisational strength and knowledge gap:** It is necessary to identify the key organisational strengths and knowledge gaps before making the transition to cloud computing. Roles involved in the migration should be clearly identified if the migration plan is executed. Employees should have adequate skills to execute the adoption actions for both applications and data.
- **Application & data profile:** Applications and data must be analysed to determine which of their parts should be migrated. Application criteria such as number of integration points, external systems, HW devices, and application complexity must all be identified and data size is also necessary to determine the migration cost.
- **Migration and operational cost saving:** The migration and operation cost calculates the provider cost model, software and hardware operation cost and compares the cost with the in-house local data center cost and varies with the migration type.

Activity 2: Risks Identification . This activity focuses on understanding the risks associated with the cloud migration so that appropriate control measures can be taken.

Step 2.1 Define Risk Context. This step defines the boundary of the risks management. In particular, the main focus is are the risks relating to business, security and privacy perspectives. The context also determines how risky the cloud migration would be in terms of cost and schedule, CSP support, adaption actions, security, privacy and other related factors. The riskiness can be determined in three different scales: high, medium and low. Generally, if in-house applications need major amendment, employees lack the skills for the migration, security controls and CSP support are poor, PII data is to be migrated, then cloud migration could be a high risk project for the organisation.

Step 2.2 Identify Risks. This step identifies the potential risks both before and after the migration. The risks are caused by both internal and external users. In particular, malicious insiders such as CSP employees, contractors, or any other relevant stakeholder can misuse using the system resource in a way that could violate the confidentiality of user data. In case of the cloud, such a threat could be exploited by a malicious application, system, virtual or hosting administrator. We categorize the risks based on the attributes of the decision components. They are:

- **Cost/ Revenue:** Uncertainty in Cloud utility billing model due to actual resource used by the provider and deployment options, over-provision and under-provision of applications and inaccurate usage estimation
- **Employee skill & roles:** Employees have inadequate experience with cloud technology and unclear roles for the adaption actions and maintenance with migrated entities.
- **CSP Support & Compliance:** Lack of CSP support and non compliance with the relevant regulation and industry specific standards.
- **Application Data Adaption Actions:** Unclear adaption actions such as business logic amendment and incompatible data format for the application and data.
- **Data Confidentiality:** Leakage of user data for any unintended usage.
- **Isolation & Deletion:** Isolation failure allows malicious to obtain control over other tenant storage area and incomplete disposal of data.
- **Identify & Access Management:** Poor identity access management pose for unauthorized access to the legitimate user resources.
- **Services interruption:** Unavailability of cloud services pose interruption of critical business services and slower performance than expected.
- **Transparency & Accountability:** User critical asset is stored in an environment which is out of user control. Inadequate monitoring and auditing of user critical asset pose any potential risk and lack of user trust to the cloud provider.
- **Loss of governance:** Loss of control over collecting, processing, sharing, and storing of data is a key concern for cloud adaption.
- **Disaster recovery & business continuity :** Poor disaster recovery and business continuity plan and mismatch with the user and provider plan.
- **Security incident report:** No knowledge about security incident report

Activity 3: Requirement and Assurance Analysis. This activity assists in identifying the requirements for addressing the risks and collects the evidences relating to control measure to fulfill the requirements.

Step 3.1 Identify Requirements. Requirements are the cloud user desire to support the migration goals and constraints. This step identifies business, application, and security and privacy requirements as criteria for undertaking the migration decision. These requirements aim to support the migration goals. Similar to the risks, these requirements follow the main attributes of the decision components and emphasize to mitigate the risks. Therefore, the requirements are identified by analyzing the risks and by following other sources such as migration portfolio, application context, organisational goals, users needs, and existing security policies. The requirements types follow the risks types such as we need to identify requirements relating to cost/revenue, employee skill, CSP compliance, adaption actions, security and privacy.

Step 3.2 Assurance of Control Measure. This step collects the evidences for the assurance of control measures. Evidence originates from both user and CSP supports assurance for fulfillment of the requirements and mitigation of the risks. The evidences are various types such as documented report, approved policy, security and privacy measure, list of any specific information, and any other relevant entities. Therefore both user and CSP are responsible for implementing their own evidence collection mechanism. It drives the users for making migration decision into cloud. The user should identify and review the evidences based on the key decision components attributes requirements.

Activity 4: Cloud Migration Decision and Strategy. This activity assists making the final decision once information relating to requirements and assurances have been identified, and the migration strategy is in favour of cloud migration.

Step 4.1 Decision for Cloud Migration . The migration decision step performs cloud fit analyses based on the risks, requirements and assessment of assurance for the final migration decision. The decision is based on the level of completeness of the assurance of control measure for fulfilment of the requirements by the CSP and user. bThree levels of granularity are considered for determining the level of completeness,i.e., level 1 none(little to no evidence of assurance of control measure), level 1 partial (limited evidence of for the assurance of control measure), and level 3 full (adequate evidence of the assurance of control measure). Completeness level assists the user gaining confidence for a CSP and undertaking the migration decision. Full completeness specifies

that both user and CSP impose adequate control measure and that the organisation should make the migration decision with the chosen CSP. However, this case is not always possible. In the case of partial completeness, the user should make a decision depending on the fulfilment of the requirements that are critical for the organisational context. Hence fulfilment of critical requirements helps to control the risks.

Step 4.2 Define Cloud Migration Strategy . If the decision is to migrate into the cloud, then it is necessary to develop a migration strategy. The cloud migration strategy depends on several parameters and links with the migration portfolio. The parameters are given below:

- **Migration type:** Type I (replacement), Type II (partial), Type III (whole stack migration), and Type IV (cloudification)
- **Service/deployment model:** Appropriate service and deployment model.
- **Migration assessment index:** prioritized application and data for migration.
- **Data store & hosting type:** centralized/distributes and On-premises/ off-premises and single-tenanted / multi-tenanted hosting.
- **Adaption actions:** application adaption actions such as extract/adapt service, adapt business process, and reconfiguration of application and data adaption actions such as resolve incompatibilities, reconfigure data access layer, transform queries, and coupling data into cloud infrastructure.
- **Migration testing:** Test real resource usage by the chosen application and migrated application and in house existing application functionalities to support the business continuity.
- **Adaption constraints:** key requirements and assurance that need to be monitored.
- **Roles and responsibilities:** Assign roles to the organisation employee and agreed support from the CSP.

5. CONCLUSIONS

The impact of cloud computing on business is huge. Organisations should however not opt for cloud computing without analysing the factors involved in making migration decisions and the potential consequences after the migration. There are indeed considerable concerns regarding business, security, privacy issues that require adequate attention. This work supports an organisation in making an informed migration decision in a systematic way. We consider risks, requirements and audit from the decision components. These allow on one hand an understanding of the potential risks both before and after the migration, and on the other hand allow requirements to be used as guiding constraints to address the risks and audit through evidence to fulfill requirements. The process model supports the identification of the migration portfolio based on the organisation context. The portfolio then analysed through the risks, requirements and audit so that an accurate decision can be taken for the migration, and migration strategy can be defined for a successful migration. Therefore, the proposed approach provides an in-depth analysis of the issues that require adequate attention for the migration into the cloud. The next step of our work is to implement the process into a real business scenario context and to develop tool support for the decision making process. This allows us to understand the applicability of our approach as well as automate the activities to extract the artefacts.

6. ACKNOWLEDGMENTS

This research was funded by the Austrian Science Fund (FWF): P 26289-N23 and COMET K1, FFG - Austrian Research Promotion Agency.

7. REFERENCES

[1] T. B. C. Bruening P. J. Cloud Computing: Privacy, Security Challenges, Bureau of Nat'l Affairs. online, 2009. available at: http://www.hunton.com.

[2] M. Fowler. *Patterns of enterprise application architecture*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[3] S. Islam, H. Mouratidis, and E. Weippl. A goal-driven risk management approach to support security and privacy analysis of cloud-based system. *Security engineering for cloud computing: approaches and tools. IGI Global Publication, Hershey*, 2012.

[4] P. Jamshidi, A. Ahmad, and C. Pahl. Cloud migration research: a systematic review. 2013.

[5] B. Johnson and Y. Qu. A holistic model for making cloud migration decision: A consideration of security, architecture and business economics. In *Parallel and Distributed Processing with Applications (ISPA), 2012 IEEE 10th International Symposium on*, pages 435–441. IEEE, 2012.

[6] C. Kalloniatis, H. Mouratidis, M. Vassilis, S. Islam, S. Gritzalis, and E. Kavakli. Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces*, 36(4):759–775, 2014.

[7] 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*, pages 541–548. IEEE, 2011.

[8] M. Klems, J. Nimis, and S. Tai. Do clouds compute? a framework for estimating the value of cloud computing. In *Designing E-Business Systems. Markets, Services, and Networks*, pages 110–123. Springer, 2009.

[9] 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*, pages 199–212. ACM, 2009.