Moving Business Intelligence to Cloud Environments

Adrián Juan-Verdejo[1, 2], Bholanathsingh Surajbali[1], Henning Baars[2], Hans-Georg Kemper[2]
[1]CAS Software A.G, Karlsruhe, Germany
[2]Chair of Information Systems I, University of Stuttgart, Stuttgart, Germany
adrian.juan@cas.de, b.surajbali@cas.de, baars@wi.uni-stuttgart.de, kemper@wi.uni-stuttgart.de

***Abstract*—Business Intelligence systems use information technology to supply integrated management support with data coming from several sources of structured and unstructured data. The integrated infrastructures of Business Intelligence (BI) are often too complex and hence costly and inflexible. A solution for these issues is to leverage cloud computing services to enhance legacy BI systems and applications with cost-efficient increased scalability and flexibility. However, the migration of BI systems to cloud environments is usually hindered by strict requirements regarding privacy, security, or availability and a multitude of interdependences with other systems. In this paper, we describe the challenges in the adoption of BI within cloud environments and propose a cloud migration framework to assist decision makers in taking into account the consequences of the migration of BI systems to cloud environments as well as the impact of privacy, security, cost, and performance in so doing.**

I. Introduction

In a moment of economic downturn, organisations are continuously looking for options to increase their competitiveness while reducing their incurred costs [1]. Cloud computing is an emerging cost-efficient computing paradigm offering many value added services for organisations including cost reduction, increased business agility, increased levels of collaboration, scalable resources utilisation, and outsourcing opportunities [1]. . Cloud computing potential economic and technical benefits attract organisation's interest in migrating Business Intelligence (BI) systems [2]. BI refers to IT-based management support [2]. Business Intelligence comprises a set of theories, methodologies, architectures, and technologies to transform raw unstructured data into meaningful and useful information for business purposes. BI profit from a competitive advantage originated from the elastic utilisation of the additional computing, storage, and networking resources that cloud computing offers on a flexible pay-as-you-go manner. BI is built around the concept of integration on the technical, conceptual, and organizational level and represents the potential of BI in cloud environments. Due to the integration characteristic of BI, the needs and characteristics of each BI component, and the interdependencies between those components; the migration of BI to cloud environments presents a lot of challenges at the technical, conceptual and organisational level [3].

Challenges in migrating BI systems to cloud environments include data security and ownership, trust concerns towards cloud providers, the selection of suitable cloud environments, and performance erosion. Current research works in this context focus either on the technical, social, economic, business, sensitivity-related or organizational concerns that affect applications migration [4] [5] [6] [7] [8] [9]. The issue is that they separate aspects of the migration decision that are connected and depend on each other [10]. Additionally, by not taking deeply into account the target system for migration these works cannot include particular characteristics related to the migration of BI systems [11]. What parts of a BI system migrate to cloud environments and how to do it depends on the selected cloud service, the organisation's interest and focus in moving their BI system to it, and the specific BI system's architecture and properties [10]. The cloud service selection is often not considered at all or considered independently from the other interconnected concerns.

We aim to provide a cloud migration framework to help organisations move their BI systems to selected cloud environments. We incorporate, in addition to cross-cutting concerns in the migration to cloud environments, the specific concerns related to the BI migration scenario. Our approach maximises the benefits that attracted organisations to migrate their BI systems. We build our approach on top of our previous work [10] [12] and includes end-to-end security mechanisms to help organisations tackle privacy and security-related concerns related to the migration of BI systems to cloud environments [13] as well as ensuring data synchronisation during the migration process using a synchronisation module [13]. We aim for a secured holistic selection approach that puts together the cloud service selection, how to re-engineer a system to cloud-enable it partially or totally, the multi-dimensional consequences of the migration, and the security and sensitivity-related concerns.

We explain in Section II the main requirements and motivation for building our migration framework by using a generalised use case scenario. Then, in Section III we describe our approach to address these requirements. Next, in Section IV we present the implementation aspects of our migration framework and the security and synchronisation modules. Next, in Section V we provide an analysis of our related work and finally, in Section VI, we offer our conclusion and future work.

II. Motivation

Cloud computing is a delivery model with the potential to let Business Intelligence systems benefit from increased scalability and flexibility at reduced costs [1]. Moving current BI systems to cloud environments might ease existing agility pressures [14], be a response to volatile capacity requirements for functionality used in BI solutions [2] [15] [16], for example social media analysis, planning, or budgeting. The migration offers broad network access to data (such as KPIs and KRIs) increasing the levels of collaboration and opens the door to: outsource services to resource-rich elastic cloud providers; and transformational outsourcing [17]. The wide spectrum of BI SaaS services offered by all large BI vendors and market studies [18] [19] indicate that there are indeed high expectations towards bringing BI to cloud environments. To

978-1-4799-3088-3/14/$31.00 ©2014 IEEE

illustrate the migration of applications, we use a generalised BI Web-based BI management model as shown in Figure 1. In general, BI models follow a three-tier architecture consisting of a presentation layer, a logic layer, and a data layer. The data layer stores the structured and unstructured data coming from operational systems; the logic layer performs different analysis on those data; and the access layer let BI users access the high-level data they need.

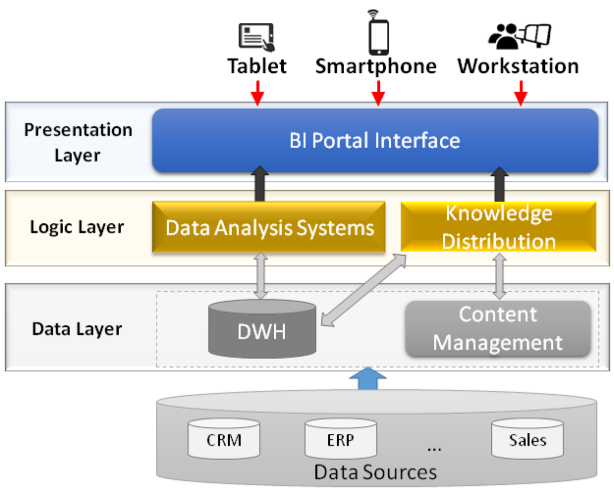

Figure 1: Generalised BI System (non-cloud-based)

When moving such a BI system to cloud environments, the following four factors impact the migration process:

i. Data Security and Trust. The data layer represents the asset of the BI user organisation interested on migrating the BI system to cloud environments. The migration of this layer to cloud environments poses important security concerns for the organisation: i) how trustworthy is the cloud provider to store the data layer; ii) the integrity of the migration process and how secure is storing this layer in cloud environments; iii) how users are going to access their existing data layer. It is therefore crucial to implement mechanisms to secure the migration of a BI system application to cloud environments.

ii. Data Ownership. Another important feature to consider for example: i) who owns the data; ii) what happens in case the provider goes out of business or another party takes over it. On migrating the BI system, the organisation must also consider who manages the data. This is important on the cloud service model the organisation chooses. For instance, in case of opting for a SaaS or PaaS model, it is the software vendor who manages the data layer. In the IaaS model the organisation will be the owner of the rights on the data. Hence, it is important for the organisation to establish the cloud provider model they need and to advocate for transparent contracts that specify the applicable Service Level Agreements (SLAs), legal and regulatory policies.

iii. Performance of migrated BI system. On moving the BI system to the cloud, the size and data sources of the data layer is an important aspect to consider. The data migration requires high bandwidth usage due to the large amount of data moved—which affects the performance of the overall BI solution. Further, distributing some BI solution to interdependent data marts, among different nodes negatively affects the performance of a component placed in a location distant another component it frequently and heavily interacts with. As a result, the performance erodes due to the introduced wide-area communication. Hence, it is important to assess the BI system placement performance to keep interdependent components at the same premises if necessary and ensure data are kept in synchrony during the migration process.

iv. Cloud service offerings and levels of granularity. The cloud deployment model choice affects the decision to migrate to cloud environments: i) private cloud whereby the organisation wants to ensure total data ownership through self data security enforcement; ii) public cloud whereby the organisation trust cloud provider offerings; and iii) a hybrid model whereby the system can use more computational resources on demand while keeping sensitive data in the organisation premises. Furthermore, the cloud service model also influences the migration process:

– *Software as a Service (SaaS).* In case the BI system uses tailored software systems, running SaaS, then the migration process, requires moving only the data-layer only to cloud with suitable legal and SLA agreements between the BI software vendor and the organisation and agreeing on the pay-model. The organisation may also opt to choose a different BI SaaS vendor and agreeing on the best cloud BI model.

– *Platform as a Service (PaaS).* Moving the BI system to a PaaS model influences our migration choice since the organisation needs to have a customised-BI system. The migrated BI can use for example different specialised tools depending on the organisation KPIs. This opens the door to a multi-cloud solution that uses selected PaaS offerings depending on their functionality—BI mashup or best-of-breed scenarios [2].

– *Infrastructure as a Service (IaaS).* In this case the organisation uses cloud provider's software and hardware at the level of virtual machines. Such an option requires extending the SLA by agreeing on the resource utilisation and pay model.

Our cloud migration framework selects a cloud environment depending on these many cloud offerings, their levels of granularity, and properties such as the ability to scale up or the availability of the service. It is worth doing it in order to judge the system's future performance, security provision, and even the applicable legislation after migration. We depict the following three main possible migration strategies based on the above factors:

- **Partial Migration of BI systems**. Whereby the organisation opts for a partial migration of a subsection of the BI systems. For example, from Figure 1 the organisation migrates only the Customer Relationship Management (CRM) BI system, while the sales BI system resides on its own premises.

- **Partial Migration of BI Layers**. The organisation chooses moving only part of the BI layers to the cloud. For instance, for security reasons, the organisation can decide to keep the data layer on its premises while using BI tools in cloud environments to extract information from those data. At the same time, the organisation needs to makes sure the system's performance is not affected by such a model.

- **Migration of all BI layers/System**. Moving the whole BI layers/system to cloud environments affects the data ownership, security, trust, and performance of the resulting BI system.

III. APPROACH

We incorporate in our approach the factors affecting the cloud migration decision so that we accommodate organisations requirements and take into account the different deployment models to alternative cloud service models. We base our explanation on specific examples showing possible outcomes of applying our framework to migrate a specific BI system—such as the example system shown in Figure 2.

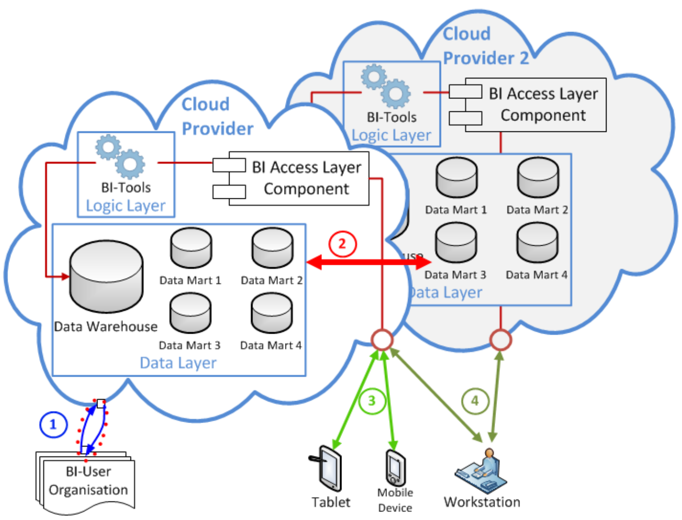

Figure 2: BI system in a cloud provider

The BI-user organisation at the bottom left side of the picture represents the organisation's premises where the BI system was running before the cloud migration. In this deployment the BI-user organisation pushes and pulls data to and from the cloud environment—see rounded circle (1) in Figure 2. Push and pull communications are secured end-to-end by encrypting the dataflow with the Transport Layer Security/Secure Sockets Layer cryptographic protocols, TLS/SSL. Once the BI-User organisation transfers its data to the cloud premises, the BI tools running in cloud environments analyse and transform those data which ultimately are used to generate data analysis and reports. Their meaningful information is stored in the Data Warehouse and can be accessed by a myriad of different devices such as the workstation, tablet, or mobile phone shown at the bottom right part of Figure 2. These devices use the BI Access Layer Component on the cloud provider's side as marked with rounded circle (3) in Figure 2. If the organisation does not entirely trust its sensitive data to a cloud provider, our approach takes a partial migration strategy. Our approach moves some components and data to the cloud providers while others stay locally. Sensitive data stays locally and our approach pushes—see rounded circle (1) in Figure 2—the anonymised data needed to use BI tools on them. The organisation moves their BI tools to IaaS or PaaS platforms to leverage the additional scalable resources or to a SaaS offering to use available BI tools.

Our approach considers the potential deployment of data and computation across different cloud provider's infrastructures—namely cloud provider and cloud provider 2—to leverage the different attributes of the available cloud service offerings, and enforce portability and availability. The decision of where and how to deploy the BI system is assisted by taking into account the requirements defined by the BI users, the characteristic of the BI system to be migrated, and the cloud service offering attributes. Again, we use end-to-end SSL/TLS encryption to secure the communication between cloud premises over the Internet as shown by the rounded circle (2) in Figure 2. In order to select an appropriate migration strategy, we consider the interactions of the non cloud-enabled BI system with other neighbouring components within the organisation's premises. These interdependencies have to be kept after our framework migrates the BI system to cloud environments. This research challenge is related to the integration aspect of BI systems. As an example, if we want to migrate an existing BI system that heavily interacts with a Customer Relationship Management system, CRM in Figure 1; our approach re-engineers the BI system taking into account: i) what CRM components the BI system communicates with; ii) how often does this communication take place; and iii) how much data is interchanged. For instance, one potential outcome in using our approach run the BI system and some CRM components within the same premises to avoid increased latencies which could harm the system's performance beyond acceptance. In the case of moving to a non-trusted cloud provider, the connection marked with a rounded circle (2) in Figure 2 would only synchronise migrated data if relevant.

Rounded circle (3) in Figure 2 shows the broad network access of heterogeneous mobile devices to the BI-cloud system. Our approach transparently postpones mobile data uploading tasks when they are interrupted due to mobile devices disconnections from the Internet. Mobile devices will transfer the data once they re-establish the connection or the user connects to a trusted reliable network.

Our approach transparently supplies users with up-to-date data regardless of the number of cloud environments our framework deploys the BI system to, as marked with rounded circle (4) in Figure 2. For that, we address data synchronisation and space efficiency with a Globally Unique Identifier (GUID)—as shown in Section IV.C—to enforce consistency among data transferred from source to target data storage and harmonise data over time, see rounded circle (2) in Figure 2. We use metadata to help with the discovery and delivery of information and metadata coordination to enable correct data sharing across cloud environments. By deploying a copy of the system to several cloud computing environments with harmonised data between them, we enhance resilience of the overall system and avoid vendor lock-in. We provide isolation so that failures do not spread to healthy components and we can manage the BI system from a safe computing environment outside if we observe a failure. In case of failure, our BI system tolerates it as our framework ensures availability by letting the overall system transparently use the BI system running in another cloud provider. Likewise, if a particular cloud provider went out of business or failed to comply with the Service Level

Agreement, we could connect to the synchronised BI system deployed to other cloud providers.

IV. Implementation Aspects

With the aim of showing how our approach tackles, in practice, the problems with migrating BI systems to cloud environments; we explain the details of our overall cloud migration framework including the security and synchronisation modules. Figure 3 shows a general overview of the cloud migration framework.

A. Cloud Migration Framework

Our cloud migration framework implements a migration process based on the requirements of the organisation whose BI system will be moved to cloud premises, the characteristics of the existing BI system, and the features and characteristics of potential cloud service offerings.

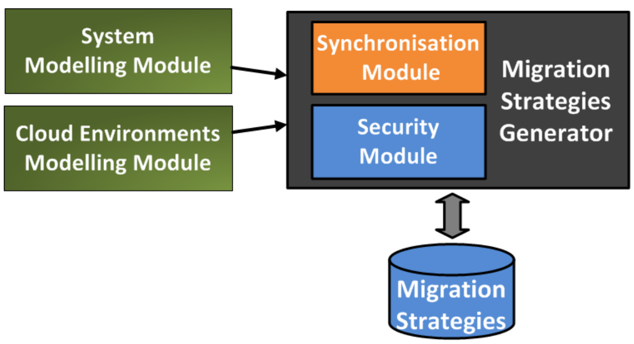

Figure 1: Cloud Migration Framework

In a typical BI system as described in Figure 3, several interactions happen between the local premises and cloud environments. The system deployed in the cloud environment pulls data from the organisation's premises and the latter pushes data back to the virtualised environment. These interactions are affected by several factors. Within the context of BI, the data size of the information to be moved to cloud environments entails implications in terms of the incurred costs due to wide area communications and the overall system's performance. For instance, in the case of performance or the provided QoS, the latter could be lowered during the migration process. Data loss during data transfer might happen so our cloud migration framework backs up data and recover from disaster in order to be protected against this eventuality. Moreover, our framework ensures data integrity after migration by re-computing a checksum to compare it with the stored one. Our framework adapts the migrated BI system to protect the BI data—which is usually very sensitive—from the cloud provider to enforce trust. In turn, this encourages organisations to let their BI systems run in a cloud provider outside their premises. We perform data compartmentalisation to keep the cloud provider oblivious to the data they store so that cloud providers are not able to access and understand the data stored at their premises. Additionally, we support privacy by granting access to these data to users with a user role related to them and the necessary level of authorisation.

We built the migration framework on top of an already presented decision support system based on AHP [10] [12]. We extended our previous work to incorporate several end-to-end security mechanisms to help organisations tackle privacy and security-related concerns related to the migration of BI systems to cloud environments [13]. In Section 4.B, we explain how the security mechanisms have been implemented to provide secured data access, manipulation, and storage. Although we leverage existing security mechanisms to ensure the trustworthiness of our approach, our focus lies on planning this migration.

We implemented a prototype of the cloud migration framework based on Eclipse RCP with EMF-based editors to model the system—in this case a BI system— and the potential cloud environments for selection with the System and Cloud Environments Modelling Module in Figure 3. We can also see in this figure that our cloud migration implementation contains four main components: the two already mentioned to model the system and cloud environments, the migration strategies generator to decide how to migrate the BI system to the suitable specified cloud environments, and the migration strategies repository at the bottom.

We modelled the BI system architecture and properties with the System Modelling Module; likewise, with the Cloud Environments Module we modelled the exemplary cloud environments—that is the Google App Engine and Force.com—properties, and how to adapt systems to them; the Migration Strategy Generator generated and rated migration strategies based on the information gathered by the previous components [12]; finally, the Migration Strategies repository stored these migration options. The Migration Strategies Generator includes a Security and Synchronisation Modules shown in Sections IV.B and IV.C.

B. Security Module

We ensure end-to-end encryption to avoid the data to be compromised at the moment of migration. As some data cannot leave the BI-user organisation's premises, due to law or policies on sensitivity, but could be needed by the BI tools running within the cloud environment. We substitute sensitive data elements with a generated token that represents the sensitive or secret data. This approach for security provision is called tokenisation [20] and comes into play when, as an example, a user accesses client data with a tablet as rounded circle (4) in Figure 2. We do tokenisation to replace the original sensitive data, say the Social Security Number, which never leaves the premises with randomly generated values. We keep the original format of the data and preserve the functionality running on the cloud premises. We translate from token to real data at the cloud provider side. It is compatible with our approach to encryption so that we can guarantee data residency for some scenarios whereas we encrypt data for others.

Growing privacy and sensitivity concerns hinder both data sharing and integration and therefore cannot be taken into account independently [13]. We annotate data with privacy-related metadata to specify the applicable privacy policies. Metadata move along with the data they refer to and can change when they do. Sensitive data is not migrated to non-trusted cloud providers but stay locally within the organisation's premises. Data access depends on users' roles and level of authorisation managed by our discretionary access control for data access, manipulation, and storage [13].

C. *Synchronisation Module*

As for the data synchronisation policies we use the synchronisation framework shown in Figure 4 that we have developed from [13]. It tracks the state of records and their relations and it works highly efficiently as it only transfers data that has really changed. At the beginning of a synchronisation session the framework obtains the state from each of the two synchronised systems and compares them with the known state of the last session.

The ConnectionBridge module controls the communication between the sync framework and the target BI cloud based system to be synchronised. To ensure an independent, reusable implementation the bridge encapsulates the used technology of communication between the system and the synchronisation framework. The bridge has no domain model-based dependencies and therefore the same implementation can be used for different systems which support the implemented technology. The differences in the domain model structure of various systems are resolved using the mapping and link definitions. The ConnectionBridge interface defines a small set of methods whose implementation is needed to fulfil the requirements of the synchronisation process. To support new systems, this interface needs to be implemented but the synchronisation process itself does not need to be changed. This keeps the cost of supporting multiple external systems low. The Sync Framework itself manages the workflow of the entire synchronisation session and manages the communication to the ConnectionBridges. It contains the logic of the synchronisation, which includes the ability to determine the states of the records to synchronise, the creation of the operations based on the record pair state and the strategy. We enforce in a transparent manner the delivery of current data and the availability of these data.

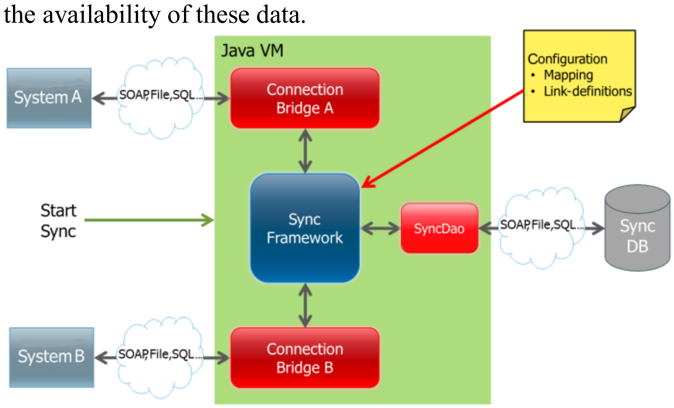

Figure 4: Synchronisation module

V. RELATED WORK

We present approaches for migrating systems and applications to cloud environments with special focus on the reliable migration of data to cloud environments, security mechanisms in the context of cloud computing, and cloud service selection. We analyse those research works and compare them with our approach.

Our approach considers the partial migration of application layers and architectural components to cloud environments and the security-enhanced migration and cloud-enabled BI system. Migrating applications to cloud environments is a multidimensional challenge because how we adapt an application to cloud environments affects migrated systems in different manner and degrees of importance [21]. The division and re-scattering of the target application's components is driven by many technical factors with various business, organisational, economic, security, and privacy implications [12]. The research works explained in our related work focus on a specific implication stemming from the migration transformation and do not consider related consequences. DRACO [22] presents an adaptable, fault tolerant and secure cloud platform for PaaS which helps in the development of complex algorithms for cloud environments. Opposed to our work they do not consider other implications of the cloud migration. Our research work—as others [23]—emphasises the need of a holistic approach to the migration to cloud environments. We differ from [23] as we include more criteria for migration including inherently subjective parameters. We include approaches to minimise the impact of the vendor lock-in issues [24] [25] and Model-based migration [26]; but extend them with our security and synchronisation framework as well as the consideration of how to trade off some aspects of the migration. We take into account the impact of the migration from an economic [6] and performance-related [7] [8] point of view but additionally to these works we show how these implications affect each other when migrating BI to cloud environments. As others [4] [5] [9], we build a decision support system but differ from them in the fact that we consider a broader frame of applications, consider multiple interdependent criteria and parameters, select a suitable cloud environment, and enhance the system's security and synchronisation.

In an effort to provide a secured infrastructure for migration, Hu and his colleagues [27] address privacy of data migration to cloud environments. However, they only address security using encryption of data within the cloud premises, not during the migration process as we do. In [28], the authors offer Virtual Private Networks, VPNs as a mechanism to migrate applications to hybrid clouds while letting enterprises control their data. We take a similar approach but also provide security mechanisms to secure the system on the cloud premises. Some of the already mentioned migration decision support frameworks implement security mechanisms to some extent although security does not represent their main focus [6] [29]. In our framework, we extend their work by including the end-to-end security mechanisms and the security mechanisms for data obliviousness and management on the provider side as explained in Sections IV.A and IV.B.

Several research works confront the migration decisions with the cloud service selection [25] [30] [31] by focusing on a different migration dimension for instance on cost or elasticity. Their research works match up with ours as we state the need of a strong decision support to assist the cloud service selection as offerings grow in number and quality. However they do not explain how the cloud service selection affects the migrated system in a multidimensional fashion that also includes the specific needs of the organisation migrating the system and the system itself as we do.

VI. Conclusion

Although an increasing number of companies are currently adopting cloud computing as the computation model to run their BI systems due to the benefits offered. There are still some concerns related to the migration to cloud infrastructures that have to be addressed as seen in Section II. With this in mind we present a cloud migration framework that leverages state-of-the-art security mechanisms and partial migration in order to protect the extra sensitive BI data. Our framework assists the migration of BI systems to cloud environments based on the user's requirements, how the re-engineered version of the BI system match them, and the characteristics of the different cloud providers. We provide a versatile framework we can apply to different application domains. Within this paper we focus on the BI application domain.

As future work we are interested in progressing in migration interoperability, and want our framework to work more efficiently with several cloud providers, private and hybrid cloud. Additionally we plan on extending our framework in supporting migration of VMs' to environments designed to cope with latency while supporting computing-intensive tasks—such as migrating to cloudlets [34]. Currently, we have extensively tested our framework and our security mechanisms within the private cloud environment but we plan to test and experiment our approach more intensively within the migration to public and hybrid cloud environments.

Acknowledgment

This research work has been supported by RELATE Initial Training Network Marie Curie Action, ITN, within the 7th FP7, funded by the European Commission.

References

[1] Armbrust, M., et al., *A view of cloud computing.* Communications of the ACM, 2010. 53(4): p. 50-58.

[2] Baars, H. and H.G. Kemper. *Business Intelligence in the Cloud?* in *14th Pacific Asia Conference on Information Systems (PACIS)*. 2010. Taiwan.

[3] Popovič, A., P. Coelho, and J. Jaklič, *The impact of business intelligence system maturity on information quality.* Information research, 2009. 14(4).

[4] Menzel, M. and R. Ranjan, *CloudGenius: decision support for web server cloud migration*, in *Proceedings of the 21st international conference on World Wide Web*2012, ACM: Lyon, France. p. 979-988.

[5] Menzel, M., et al., *(MC2) 2: A Generic Decision-Making Framework and its Application to Cloud Computing.* Software: Practice and Experience, 2011.

[6] Hajjat, M., et al. *Cloudward bound: planning for beneficial migration of enterprise applications to the cloud*. 2010. ACM.

[7] Seung, Y., et al. *CloudFlex: Seamless scaling of enterprise applications into the cloud*. 2011. IEEE.

[8] Calheiros, R.N., et al., *CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms.* Software: Practice and Experience, 2011. 41(1): p. 23-50.

[9] Ward, C., et al. *Workload migration into clouds challenges, experiences, opportunities*. in *3rd IEEE Conference on Cloud Computing*. 2010.

[10] Juan-Verdejo, A. and H. Baars. *Decision support for partially moving applications to the cloud: the example of business intelligence*. in *Proceedings of the 2013 Int. workshop on Hot topics in cloud services*. 2013. ACM.

[11] Frolick, M.N. and T.R. Ariyachandra, *Business performance management: One truth.* Information Systems Management, 2006.

[12] Khajeh-Hosseini, A., D. Greenwood, and I. Sommerville. *Cloud migration: A case study of migrating an enterprise it system to iaas*. in *Cloud Computing, 2010 IEEE 3rd International Conference on*. 2010. IEEE.

[13] Glonet, *GloNet Platform Design.* Online: https://sites.google.com/site/glonetproject/8-download/GloNet-D3.1.ppdf, Jun 2012.

[14] Zimmer, M., H. Baars, and H. Kemper. *The Impact of Agility Requirements on Business Intelligence Architectures*. in *System Science (HICSS), 2012 45th Hawaii International Conference on*. 2012. IEEE.

[15] Baars, H. and H.G. Kemper, *Ubiquitous Computing–an Application Domain for Business Intelligence in the Cloud?* 2011.

[16] Thomson, W.J.J. and J.S. van der Walt, *Business intelligence in the cloud* South African Journal of Information Management, 2010. 12(1).

[17] Linder, J.C., *Transformational outsourcing.* MIT Sloan Management Review, 2004. 45(2): p. 52-58.

[18] Qie, L. and H. Baars, *Die Cloud als neuer Ansatz zur Erhöhung der BI-Agilität?* BI Spektrum, 2012. 7(2): p. 26-29.

[19] Gartner. *Nearly One Third of Organizations Use or Plan to Use Cloud Offerings to Augment Business Intelligence Capabilities*. 2012. Gartner.

[20] Clifton, C., et al. *Privacy-preserving data integration and sharing*. in *Proceedings of the 9th ACM SIGMOD workshop on Research issues in data mining and knowledge discovery*. 2004. ACM.

[21] Andrikopoulos, V.B., Tobias; Leymann, Frank; Strauch, Steve, *How to adapt applications for the Cloud environment.* Computing, Springer, 2012. 1.

[22] Celesti, A., et al. *Draco paas: a distributed resilient adaptable cloud oriented platform*. in *IEEE Parallel and Distributed Processing Symposium, 2013*. 2013. IEEE.

[23] Leymann, F., et al., *Moving applications to the cloud: an approach based on application model enrichment.* International Journal of Cooperative Information Systems, 2011. 20(03): p. 307-356.

[24] Binz, T., F. Leymann, and D. Schumm. *CMotion: A Framework for Migration of Applications into and between Clouds*. 2011. IEEE.

[25] Pawluk, P., et al. *Introducing STRATOS: A cloud broker service*. in *IEEE 5th International Conference on Cloud Computing (CLOUD)*. 2012. IEEE.

[26] Frey, S. and W. Hasselbring. *Model-based migration of legacy software systems to scalable and resource-efficient cloud-based applications: The cloudmig approach*. 2010.

[27] Hu, J. and A. Klein. *A benchmark of transparent data encryption for migration of web applications in the cloud*. in *8th IEEE Int. Conference on Dependable, Autonomic and Secure Computing. DASC'09*. 2009.

[28] Annapureddy, K. *Security Challenges in Hybrid Cloud Infrastructures*. in *Securing Services on the Internet*. 2010.

[29] Menzel, M. and R. Ranjan. *CloudGenius: Automated Decision Support for Migrating Multi-Component Enterprise Applications to Clouds*. in *International World Wide Web Conference Committee (IW3C2)*. 2011.

[30] Hao, W., I.-L. Yen, and B. Thuraisingham. *Dynamic service and data migration in the clouds*. in *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International*. 2009. IEEE.

[31] Garg, S.K., S. Versteeg, and R. Buyya. *Smicloud: A framework for comparing and ranking cloud services*. in *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on*. 2011. IEEE.