Chapter 1

Taxonomy of Cloud Lock-in Challenges

Justice Opara-Martins

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.74459

Abstract

This chapter reviews key concepts and terminologies needed for understanding the complexity of the vendor lock-in problem being investigated in this book. Firstly, we present aspects of cloud computing that contribute to vendor lock-in and briefly introduce existing results from cloud-related areas of computer science that contributes to understanding and tackling vendor lock-in. Secondly, we explore the literature on proprietary lock-in risks in cloud computing environments to identify its causes (i.e., restrictions), consequences, mitigations strategies, and related challenges faced by enterprise consumers migrating to cloud-based services. Then, we propose taxonomy of cloud lock-in perspectives based on reports of real experiences on migration to understand the overall cloud SaaS migration challenges. Finally, we narrow down to our perspective on cloud lock-in to three main perspectives which takes the use of sound techniques from IS research discipline and cloud-related literature into consideration, to improve the portability, security and interoperability of cloud (and on-premise) applications in hybrid environments. Collectively, the discussions presented herein, accordingly enables both academia and IT practitioners in the cloud computing community to get an overarching view of the process of combating application and data lock-in challenges, and security risks in the cloud.

Keywords: cloud computing, taxonomy, vendor lock-in, SaaS migration, ICT services

1. Introduction

Cloud computing has been revolutionizing the IT industry by adding flexibility to the way Information and Communication Technology (ICT) services is consumed, enabling organizations to pay only for the resources and services they use [1]. In an effort to reduce IT capital and operational expenditures (OpEx), organizations of all sizes are using clouds to provide the resources required to run their applications. Clouds vary significantly in their specific technologies and implementation, but often provide infrastructure, platform, and software resources

as services [2, 3]. Vendor lock-in problem is a highly referenced topic followed by security in the technical and business IT world [4–8]. Research shows that several companies are already migrating to cloud-based services, but challenges of vendor lock-in is prohibiting a widespread adoption rate across enterprises of different sizes and industry sectors [9–11]. Simply put, businesses are wary of being tied to particular cloud computing vendors due to lack of competing, compatible product [12]. Due to the ever growing interest in cloud computing services, there is an explicit and constant effort to evaluate the current trends in vendor lock-in and security for such technology. Progress of current research effort in demystifying the complexity of vendor lock-in problem in cloud computing technology is contingent on having a rigorous organization of its knowledge domain and a comprehensive understanding of all the relevant elements and components of this technology and their relationship. Currently, there is a lack of sufficient standardization of cloud computing services [4–6, 13], and each cloud service vendor uses different technologies, SLAs, protocols, APIs, security protocols, and formats. This further makes interoperability, portability, and security as elusive tasks to accomplish when working with multiple (hybrid cloud) services. Moreover, with the amount of cloud computing services and vendors increasing quickly, the need for a detailed taxonomy framework rises [14]. Such taxonomy should provide a common terminology and baseline information for easy communication and understandability of vendor lock-in risks when comparing the offers to find the right cloud service/vendor of choice. Therefore, the vast amount of cloud computing services and the lack of universal definitions and standards agreement to avoid lock-in lead to the question whether cloud computing services and related challenges can be classified in a taxonomy based on their characteristics to easily compare them. While the work in [15] proposes taxonomy for a quick classification of cloud services making it easier to compare them, however, it does not specifically addresses the challenges of vendor lock-in affecting widespread cloud adoption and migration.

To this end, the main goal of this chapter is to identify, classify, and organize the main risks of vendor lock-in associated to cloud computing migration, helping in the task of underlying the challenges that remain unanswered from the enterprise perspective. This taxonomy demonstrates a dissection of vendor lock-in problem into three main perspectives, and illustrates their classification and associated elements. It makes it very easy to comprehend the cloud computing vendor lock-in field as a whole, correlate, classify, and compare the various existing industry solution proposals, mitigation strategies, and best practices. In turn, this will provide a solid foundation for future research analysis, and a review to assist academia, and a scientific research community to expedite its contributions and insights regarding lock-in avoidance for enterprise cloud migration use cases. Over the years, taxonomy techniques have been used to create models that allow for the classification of concepts within a domain. In this chapter, we apply taxonomy techniques in the cloud computing domain to discuss the many aspects involved with cloud computing lock-in that are important from an enterprise perspective. Aiming at a better understanding of the categories of applications, data, and security controls that could trigger a lock-in situation during cloud migration, this chapter contributes by proposing a detailed taxonomy based on characteristics that are fundamental for enterprise production applications typically associated with the cloud and big data paradigm.

The remainder of this chapter is organized as follows. Section 2 discusses and reviews related work that is relevant to our work. Section 3 presents the current service models of cloud computing and their specific lock-in challenges. Section 4 briefly highlights an ontology of cloud lock-in perspectives which gives a better understanding and definitions of categories that is to be used in the design of our work. Section 5 presents the classification of perspectives used in our proposed taxonomy of cloud lock-in challenges. Section 6 concludes this chapter and recommends future research directions.

2. Related work

Several taxonomies for cloud computing can be found in [16, 17], but most are created from the perspective of vendors that are part of the market landscape and not from the perspective of enterprise IT, the consumers of cloud services, and software. Providing taxonomic information is essential not only for cloud service providers, but also for enterprise firms, and compliance authorities to detect, manage, and control invasive proprietary components. Taxonomy identifies and enumerates the components of cloud computing that are providing basic knowledge underpinning management and implementation of the cloud computing. There is, however, no standard taxonomy, as everyone tries to define cloud computing and its services in their own way. The taxonomy described by the Cloud Computing Use Case Discussion Group [18] is categorized into three views: service developer, service provider, and service consumers. This taxonomy does not cover the potential challenges of vendor lock-in and related security risks. Crandell [19] defines a taxonomy based on cloud service offerings divided into three layers, namely application services (e.g., Salesforce CRM and other SaaS vendors), platform services (e.g., GAE, Moso, and Heroku), and infrastructure services (e.g., Amazon Web Services, Flexiscale). This taxonomy is valuable for any company with an application that runs in a data center or with a hosted provider that does not want to reinvent the wheel or pay a premium. Laird's [20] cloud vendor taxonomy gives the classifications and vendors with their related group. This taxonomy divides the cloud vendors into infrastructure (i.e., public cloud and private cloud), platform (e.g., business user platforms and DevOps platform), services (billing, security, fabric management, and system integrators), and applications. This taxonomy gives a visual map of the SaaS, PaaS, and cloud computing industries. At the end of the spectrum, Forrester's cloud taxonomy [21] is categorizing cloud services by IT infrastructure vs. business value and by the level of privacy offered. This taxonomy focuses on the dimensions of privacy and business value. It does not address vendor lock-in issues but instead focuses on the modes of cloud computing (public scale-out clouds, public server cloud, virtual private scale-out clouds, virtual private server clouds, private clouds, virtual private SaaS, public SaaS, PaaS, on-premises, ASP concepts, etc.) To provide an even clearer and more explicit perspective on the complexity of cloud computing vendor lock problem, we propose taxonomy of cloud lock-in challenges building on several incremental enhancements of existing taxonomies. In this chapter, we will adjust, refine, and extend those taxonomies, making them even more suitable and flexible for understanding the complexity of cloud vendor lock-in problem.

Few studies recently, articles, have attempted to establish a similar structure for cloud computing and its components [22–25]. Although they attain some valuable understanding of several cloud services and components, they tend to be more general classifications without specifics about vendor lock-in. They neither went to the level of detail in the analysis as we did (in Section 4 and 5), nor they included all the cloud layer attributes we captured in our taxonomy. Their main objective is to classify the commercial cloud offerings in order to analyze the cloud computing market opportunities. As such, they do not address the specific lock-in potentials or limitations of the several cloud layers, nor the research opportunities associated with each cloud layer. We believe our proposed cloud ontology is more comprehensive, and encompass more detailed analysis of the cloud computing knowledge domain.

Providing lock-in taxonomy of unified and holistic SaaS architecture has not been addressed yet in a way comparable to the approach proposed in this chapter. Pursuing this further, SaaS architectures have been compared and analyzed in several studies [26–28]. Mahjoub et al. [29] conducted a survey on current cloud providers and technologies in order to help users choosing the better cloud offer that compiles with their needs or building their own cloud infrastructure with the most suitable open source technologies. The characteristics, architectures, and applications of several popular cloud computing platforms are analyzed and discussed in the paper by Peng et al. [30]. Wind [31] derived criteria from the literature analysis and compares existing open-source Cloud Computing management platforms. Important high-level criteria are taken into account (i.e., security, interoperability, user interface, etc.). Notwithstanding, cloud computing taxonomies have already been defined in several works [32–38]. The National Institute of Standards and Technology (NIST) [34], Rimal et al. [37], and Intel [38] presented a general cloud computing taxonomy. In contrast to our taxonomy, they did not address vital SaaS capabilities, such as data lock-in, contract lock-in, and application lock-in. Furthermore, Forrester [39] introduced a market-oriented taxonomy of cloud computing and did not incorporate technical capabilities of SaaS platforms and applications as discussed in our work. OpenCrowd [37] presented a general cloud computing taxonomy. The taxonomy only addresses IaaS layer and identifies four components: storage, compute, services management, and cloud broker. In contrast, our taxonomy addresses 11 components (relevant to IaaS, PaaS, SaaS, XaaS) and categorizes them into ordered layers.

3. Service models and vendor lock-in risks

Currently, there is little on offer in the way of tools, procedures or standard data formats or service(s) interfaces that could guarantee data and service portability in the cloud computing environment. This makes it extremely difficult for a customer to switch cloud providers, or to move data and services from an in-house IT environment to the cloud. In effect, this potential dependency for service provision on a single cloud provider, may lead to organizational risks should the cloud provider, for instance, go out-of-business or bankrupt. Organizations considering adopting cloud computing models are concerned about the potential for lock in and the operational challenges that a storage migration (as an example) would require. Thus, it becomes important to understand that the extent and nature of lock-in varies per cloud type:

- SaaS lock-in: SaaS providers typically develop a custom application tailored to the needs of their target market. The consumer data of a SaaS product is typically stored in a custom database schema designed by the SaaS provider. However, if the provider does not offer readymade data export functionality, the customer will need to develop a program to extract their data and write it to a file ready for import to another provider. Where the customer has developed programs to interact with the provider's API directly (e.g., for integration with other applications), these will also need to be re-written to consider the new provider's API. SaaS suffers from data lock-in, contract lock-in, and application lock-in risks.

- PaaS lock-in: occurs at both the API layer and at the component level. At the API layer, PaaS lock-in occurs as different providers offer different APIs. PaaS lock-in happens at the component (i.e., runtime) layer as standard runtime environments are often heavily customized to operate safely in a specific cloud environment. PaaS suffers from framework lock-in and data lock-in (as in SaaS), but in this case, the onus is completely on the customer to create compatible export routines and more importantly for the customers' developers to understand and consider these differences that are pointed out.

- IaaS lock-in: varies depending on the specific infrastructure services consumed. Virtual machines (VMs) that can be moved to the cloud from (heterogeneous) data centers, and between vendors' IaaS clouds, are an asset for organizations. However, doing so requires cloud IaaS providers to support a standardized VM file format. Currently, there is a little in offer in terms of standardized file format for virtual machine images and VM management. While virtualization can remove concerns about physical hardware, distinct differences exist between common hypervisors such as ZEN, VMware, and others. For example, data lock-in is the obvious concern with IaaS storage services. IaaS storage provider offerings vary from simplistic key-/value-based data stores to policy enhanced file-based stores. Moreover, feature sets can vary significantly, hence so do storage semantics. However, application level dependence on specific policy features (e.g., access controls) may limit customer's choice of IaaS provider.

However, since the focus of this chapter is on mitigating potential risks of vendor lock-in at SaaS layer of the cloud computing stack, therefore, the following sub-section(s) presented below: (1) narrows the discussion parameters for SaaS application migration scenarios, and (2) serves the purpose of highlighting some but certainly not all the cases where interoperability, portability, and security are important issues when migrating in the cloud computing environment.

3.1. SaaS lock-in challenges

Despite the numerous advantages of cloud computing to organizations, many challenges such as data lock-in, application lock-in, and contract lock-in remain inadequately addressed. In this section, we aim to address these issues of concern as it pertains to SaaS usage and their implications to enterprise cloud adopters. We tackle the vendor lock-in challenges that act as barriers to either adopting cloud-based SaaS services in enterprises, or migrating/switching between SaaS vendors. Thus, our line of reasoning here provides a concise yet relevant

discussion and in-depth analysis of these issues with some fundamental guidelines that should be observed by organizations, entering a cloud computing service SaaS contract. While it is important to understand that the extent and the nature of vendor lock-in vary as per the cloud type, be aware, however, that our focus within this chapter is aimed at SaaS lock-in, specifically. Both PaaS lock-in and IaaS lock-in is outside the scope of this thesis.

As cloud computing adoption rate soars across enterprises (small or large), the risks of vendor lock-in is prevalent. Limited studies exist, except for [40–44], to analyze and highlight the complexity of vendor lock-in problem in the cloud environment. Therefore, when selecting SaaS offerings from cloud vendors, organizations need to consider and balance service criticality against the significance of avoiding potential risks of vendor lock-in. Though it is claimed that vendor lock-in is not exclusively a computing problem, since it also occurs in the classic IT setting—in this case, the customer has more control over the data and services. However, Conway and Curry in [45, 46] argues that due to the immaturity of current cloud computing environment, data, applications, and services are primarily vulnerable to the risk of lock-in. In general, with cloud computing architectures, the risk of vendor lock-in rises with the number of hardware and software components the vendor provides. Thus, the highest lock-in risks occur with SaaS services because the vendor controls all key components of the customer's information system. SaaS lock-in affects both data and applications. Besides, cloud SaaS offerings are often based on proprietary non-standard data formats and application logic, which can make migrating data and services to another cloud SaaS vendor difficult. This potential dependency for service provision on a cloud SaaS vendor may lead to specific data and application lock-in challenges as described below.

- Data lock-in challenge: in using cloud SaaS offerings, enterprise data are typically stored in a custom database schema designed by the SaaS vendor. SaaS cloud vendors generally do not provide conceptual or logical data models for their service. Most SaaS vendors offer API calls to read and export data records. However, if the provider does not offer readymade data "export" functionality, the enterprise will need to develop a program to extract their data and write it to a file ready for import to another vendor. It should be noted that database schemas, data formats, and application programming interfaces (APIs) are valuable in providing the function of interoperability of communication and processing within the SaaS cloud [41, 44]. However, the closed proprietarily coding of these key components across SaaS vendor offerings results in the need for resource (i.e., human effort, time, and cost) to be focused into developing a solution to break free from having the enterprise data locked into SaaS offerings (e.g., data models, platforms, and programming languages). While custom code may be needed for data transformation, it is also wise to check that standard data formats used by the enterprise can be supported by other cloud SaaS vendors or there is a transformation mechanism available. This further drives the requirement for consumers using the SaaS services to understand the business and associated data that needs to be managed to support the business process being automated or replaced, before making important migration decisions.
- Application lock-in challenge: replacing an on-premise ICT system with its cloud SaaS counterpart benefits from the advantages of converting capital expenditure to operational

cost [47, 48]. However, cloud SaaS applications are developed to run on a particular operating system. SaaS vendors typically develop these custom applications tailored to the needs of their target market. Porting them to operate on another cloud SaaS provider's environment is a significant effort, because the application processing logic is supplied by the vendor and data may be proprietary [43]. Likewise, a company can spend a considerable amount of time and effort moving its SaaS applications (and data stored in one system) to a cloud SaaS environment due to application lock-in risks. For instance, enterprise SaaS customers with a large user-base can incur very high switching costs when migrating to another SaaS vendor as the end-user experience is impacted (e.g., re-training staffs). However, it may be easy in the case of SaaS to terminate a service from one cloud vendor and start service with another. If the terminated vendor is contractually required to provide data, migrating may be of questionable use without significant cooperation and resources provided by the vendor. For example, if the data is maintained in a proprietary database architecture (e.g., NoSQL data models), a conversion effort will be required, and, unless the appropriate cooperation is obtained, the project may prove costlier and take longer than forecast. Furthermore, where the customer has developed programs to interact with the vendor's API directly (e.g., for integration with other applications), this will also need to be re-written to consider the new vendor's APIs. Accordingly, as pointed out by Polikaitis [49], standardizing on cloud SaaS environment is a serious decision with long-term financial implications for an enterprise.

The vendor lock-in challenges discussed in this section are high-category risks that organizations must tackle when considering cloud SaaS solutions. They present two potential drawbacks for cloud service consumers; first, the provider has the customer organization at a disadvantage, as it can push disagreeable terms on the customer because it has no viable exit strategy. Secondly, if the provider goes out business in the worst case, the customer may have trouble sourcing an alternative. This can take considerable time, cost, and effort to find a SaaS replacement and move the entire organization's data. However, regarding these challenges, an exit strategy will either mitigate or exacerbate the impact of such risks. There is a need for these organizations to understand what the exit strategy looks like, even if it is unlikely that they will exit a service soon—besides, no company would want to buy into a service where they feel they had no alternative provider [49]. An exit strategy in this context refers to a way of moving to another SaaS vendor if the enterprise wishes to do so. Hence, a missing exit strategy is said to exacerbate data and application lock-in risks in SaaS offerings.

3.2. SaaS lock-in dimensions and approaches for adoption

In any relationship between a cloud SaaS service vendor and cloud SaaS consumer, vulnerabilities exist that can result in vendor lock-in situations [50]. For example, a lack of standard technologies and unification of interfaces within the cloud stack creates barriers for migration. In today's cloud computing marketplace, data, applications, and services are vulnerable to the risk of lock-in. It is the cloud service customer's data that is the primary asset at risk from lock-in situations here. Hence, if a cloud SaaS customer's data cannot be migrated, accessed, or retrieved due to related challenges with portability and interoperability issues at the individual levels of

the cloud computing stack, business continuity is at risk. These issues, consequently, translate into two core dimensions of SaaS lock-in as precisely described below.

- Horizontal lock-in: cloud service consumers face horizontal lock-in situations when vendors restrict them to freely replace a SaaS solution with a similar or competitive product offering. This situation can arise when a customer wishes to move to another SaaS solution but is hindered by obstacles or migration limitations put in place by their vendor. This consequently affects data portability, re-creation of cloud-based services to on-premise (i.e., roll-back), integration and interoperability, etc. Some of the likelihood of issues with SaaS cloud vendors or technology products which give rise to horizontal lock-in situations are: discontinuing software products without clear roadmaps for replacement, developing economically unsupportable solutions, releasing products without appropriate quality checks, vendor application highly customized to suit enterprise, etc.
- Vertical lock-in: in this situation, cloud SaaS customers are restricted to the use of specific software and hardware within the overall cloud service stack because of a chosen SaaS solution. This implies also that the use of an operating system, database hardware vendor, and even any required implementation (or integration) partner during migration may be dictated by vendor. At the SaaS layer, vertical lock-in can be difficult to avoid since the choice and location of hardware at the cloud provider's data center is out of the cloud service customer's control. Thus, the idea will be to ensure whether the data centers are locked or not into a particular operating system environment through their choice of virtualization. Common issues and challenges fraught with vertical SaaS lock-in includes but not limited to enterprise infrastructure built around vendor proprietary standards, SaaS applications built using vendor proprietary APIs, data in SaaS cloud products resides in proprietary database with no ability to export, and the vendor owns data rights necessary to operate SaaS solution, etc.

Therefore, while the business value of cloud computing is compelling, it is clear from raised above that many organizations still face the challenge of lock-in when adopting cloud SaaS service capabilities. With regards to cloud adoption approaches in enterprises, for simplicity, in this section, we categorize cloud computing SaaS services into two broad titles, namely: (1) horizontal SaaS offerings and (2) vertical (or sector-specific) SaaS offerings. Horizontal SaaS offerings are typically applicable to organizations across a range of business sectors, i.e., they are not specific to a business but can be found in almost any kind of organization. Some common horizontal SaaS applications are in the areas of email, customer relationship management (CRM), productivity, collaboration, analytics, etc. With the proven success and maturing of horizontal SaaS offerings, sector-specific SaaS offerings are emerging to include application in the areas of logistics and supply chain management (SCM), for example. Vertical SaaS offerings refer to specialized applications that will be used to support a focused business function or core processes that are found within that industry, e.g., patient record management for hospitals, hotel management software, etc.

Being that cloud SaaS solutions are strategically engineered to have control points, it makes difficult for customers to migrate away from their technology to competing solutions [51]. Thus, it is important that customers review the SaaS lock-in discussed above, to determine

cloud vendors and technologies that have the highest replacement or switching costs, and are most likely to create operational, financial, or legal issues. Organizations should also analyze SaaS offerings (i.e., vertical or horizontal) in terms of Total Cost of Ownership (TCO)/Return of Investment (ROI) against associated risks such as vendor lock-in, interoperability, portability, and security, including defining a clear strategy for both private and public implementations before adopting specific SaaS offerings.

4. Ontology of cloud lock-in perspectives

To identify open challenges and facilitate future advancements, it is essential to synthesize and classify the research on cloud computing vendor lock-in conducted to date. In this section, we discuss causes and problems of vendor lock-in, and present a taxonomy of cloud lock-in challenges covering the hardware, operating system, virtualization, and data center levels. A model encompassing the various elements (or triggers) of vendor lock-in risks in cloud computing is presented. The analysis of this multi-dimensional model shows that each element can create different effects of lock-in on specific business processes operating in a cloud environment. With the intent to create a cloud lock-in model, both for studying proprietary lock-in challenges in the context of service migration and for supporting decision-making for enterprise cloud adoption. Authors' aim in this section is to consider the various risks and challenges of vendor lock-in presented in **Figure 1**, and organize them in hierarchical categories of perspectives, thus creating a cloud computing vendor lock-in taxonomy. But before doing so, it is important to make clear that for any given information processing system (whether in cloud or non-cloud environments), there are a few user categories—or more accurately, several "*roles*"—that have an interest in the system. Each role is interested in the same system, but their relative views of the system are different, they see different issues, they have different requirements, and they use different vocabularies (or languages) when describing the system. In this direction, rather than attempting to deal with the full complexity of cloud lock-in problem, author mainly attempts to recognize these different interests by defining different

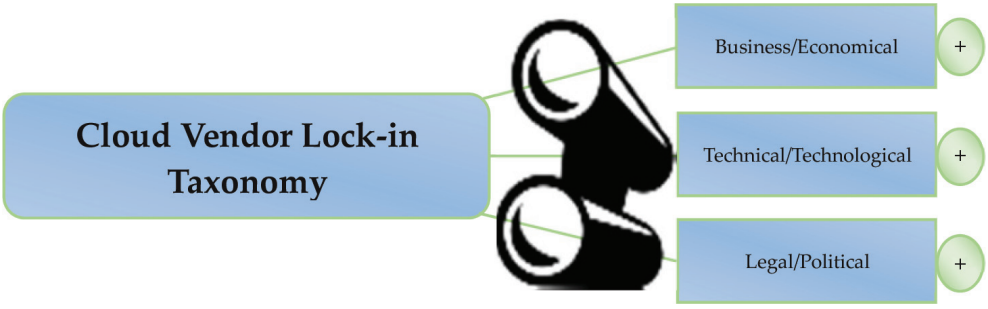

Figure 1. Perspectives for categorizing vendor lock-in risks in cloud computing. Top level overview of the viewpoints of cloud lock-in taxonomy, highlighting the three main perspectives to view the broad problem of vendor lock-in—related to business, technical and legal categories.

viewpoints of the lock-in problem in question. Each of these perspectives or viewpoints is chosen to reflect one set of inter-related consumer cloud lock-in concerns.

Across the three inter-related perspectives of vendor lock-in, organizations can use the proposed taxonomy to review their existing processes for cloud adoption and migration, data governance, and purchase policies to see if these support a strategy to achieve a high-level of flexibility and control to reduce the chance of being unavoidably locked into a single cloud provider offering. The aim of this taxonomy is to give both cloud service consumers (i.e., enterprises, end-users, developers, etc.) and cloud service providers guidance in the provision and selection of cloud services, indicating how to mitigate the risk of being tied to a cloud service provider—due to the difficulty and costs of switching to use equivalent cloud service from other providers. The taxonomy of cloud vendor lock-in perspectives partitions the challenges to be addressed into three viewpoints: business, technical, and legal. Each of the viewpoints can be used as problem analysis technique as well as solution space of the relevant issues of the lock-in problem domain. The main structure of the taxonomy along with its top levels of classification is depicted in **Figure 1**. The illustration is not meant to be exhaustive but to give a precise yet accurate view of the broad problem of cloud lock-in from different perspectives.

The three main perspectives of cloud vendor lock-in problem(s) are: business (or economics) perspective, technical (or technological) perspective, and legal (or political) perspective. Together they provide a complete picture of cloud computing vendor lock-in challenge. The concerns addressed in each of the perspectives are precisely presented. For instance, the business dimension is subdivided into standards, interoperability, portability, and security. The technical perspective includes constraints related to integration, compatibility, and APIs that are implementation-specific requirements or restrictions which may hinder interconnectability and/or trigger lock-in situation in the cloud. The complete organization of this scenario is presented in Section 5.3. While the first two categories correspond to enterprise architecture requirements (for enabling interoperability and portability) of products and IT services based on standard interfaces to interact seamlessly without the need for a large amount of integration efforts, the legal or political perspective is split into four sub-categories (i.e., SLA compliance, contract termination, cloud migration strategies, and metadata and data ownership) per the service life cycle and measures in which various aspects of cloud services offered and managed for a cloud service consumer can result in a lock-in situation. It is also noted that the lock-in risks in this dimension or perspective cover the complete information lifecycle (i.e., generation, use, transfer, transformation, storage, archiving, and destruction) inside the cloud providers' perimeter and in its immediate boundaries (or interfaces) to the consumers. The expansion of this categorization is depicted in **Figure 4**.

5. Taxonomy of vendor lock-in risks in cloud computing

A clear perspective of the main risk factors that contribute to a lock-in situation in the cloud environment and how such risk(s) should be organized to ease decision-making is the main step for having a comprehensive analysis of the status of cloud computing vendor lock-in

challenges. To organize the complex and broad data related to cloud lock-in problems and to facilitate further studies in this area, based on our previous work [44], the main problems (i.e., risks or challenges) of cloud lock-in are identified and grouped into a model composing of 11 categories namely: standards, portability, interoperability, security, integration, compatibility, APIs, data, contracts, SLA compliance, and cloud migration (in/out) strategies. These elements are placed in a hierarchical order of significance to the broad lock-in problem, in general. Moreover, the elements are significant considerations to the use of cloud services, and are also indicators to how component may trigger and/or intensify the risk of lock-in involved. The hierarchical categorization approach employed in this work assists in demonstrating how each element of vendor lock-in relates to several other components in the architecture of cloud computing. At a high level, the model establishes a common language (i.e., ontology) for easy understanding and communication of the capabilities and requirements which should be standardized in a cloud environment to facilitate open collaboration and interoperability amongst cloud providers, thereby avoiding the risk of a single provider lock-in. At a low level, the model is further composed into taxonomy to support consumers cloud service selection and adoption strategy in terms of validating cloud provider's solutions to achieve architectural integrity of business solutions of an enterprise's cloud ecosystem.

5.1. Classification methodology

Prior to presenting the proposed taxonomy, it is worthy to mention that the identification of elements and components of the categorization used is based on the critical review of key literatures in [40–45], the preceding section and subsequent sections. This critical review followed the systematic approach proposed by [52]. Some of these studies include standards and proposal documents from academia and industry as well as independent quantitative and qualitative studies conducted by author. The systematic review also covered general computing, IT and information systems (IS) journals, conference proceedings, books, industrial white papers, and technical reports. The fundamental purpose was to identify broadly any possible factors and issues that might lead to or intensify potential risks of vendor lock-in. Through this extensive and critical literature review, author established and proposed a set of potential cloud lock-in risk factors using taxonomy. The taxonomy is explained using case-examples from existing services of major cloud providers with an emphasis on the distinction made between services in software application programs (SaaS), platform (PaaS), and infrastructure (IaaS), which are commonly used within traditional enterprise computing or as the fundamental basis for cloud service classification. Based on the review of existing literature studies and the results extrapolated from our systematic study, the following constraints and challenges have been identified with switching between cloud SaaS vendors: switching cost, data portability, API propagation and integration issues, interoperability and standards, security risks, contract and SLA management, and legal challenges (data location constraints, data ownership rights, cloud in/exit issues, legal jurisdiction and compliance, etc.). They have been further grouped into three main challenge (i.e., technical, business environment, and legal) areas of SaaS migration, and briefly analyzed below. The first four are technical constraints to the growth (i.e., in terms of migration to, and adoption) of cloud computing SaaS services; the next four are internal business environment obstacles to switching between cloud vendors

once the SaaS solution has been and/or replaced; and the last four challenges are policy and legal issues intrinsic to cloud SaaS migration process. These challenges represent shared concerns that need to be addressed prior to SaaS adoption, or switching between cloud SaaS services and vendors.

As an example, integration and data portability, for instance, are two core lock-in risk factors mentioned and discussed in several of the referenced studies. This is because as new cloud SaaS services are deployed within an existing enterprise environment, the need to integrate them with various on-premise systems and other cloud services becomes important. Thus, the integration task and the need to ensure data portability have increased the complexity of decision-making in respect of enterprise cloud SaaS migration [41, 42, 53–55]. Therefore, as organizations struggle with the complexities of integrating cloud services with other critical systems residing on-premise, the ability to share data (i.e., portability) across these hybrid environments remains critical, and continues as more enterprise workloads and projects are committed to cloud computing SaaS services. As would be seen in the subsequent section, different elements of lock-in encountered in each category is described below to aid readers' understandability of the overall complexity of cloud lock-in situation in more details. Each of these elements in the categorization (or classification) model below, results in subdivisions highlighting the main risk factors of vendor lock-in that have been identified.

5.2. The business perspective

It focuses on the needs of the consumers of a cloud product or service offering. It describes the business challenges of vendor lock-in in terms of answering what is required of a cloud provider to meet customers' expectations to avoid over dependency on a product and the vendor. From a business perspective, avoiding vendor lock-in is requested by reasons varying from optimal service selection regarding utilization, costs or profits, to technology (hardware or software) changes. The adoption of cloud computing is still hindered by the lack of proper technology (or technology maturity), knowledge (of use), transparency, and trust issues. One of the problems spanning across these reasons is the low level of portability and interoperability of cloud applications and data storage services. The vendor lock-in challenge with respect to both low-level resource management and application level services is related also to the lack of world-wide adoption of standards or interfaces to leverage the dynamic landscape of cloud related offers. Portability and interoperability standards provide customers the ability to switch cloud providers without a lock-in to a provider. Moreover, data and applications in the cloud reside on systems' consumers who do not own and likely have only limited control over—which can result in loss of data and application security issues. Lack of interoperable and portable standards for different security policy or control, key management or data protection between providers may open undiscovered security gaps when moving to a new provider or platform. Hence, it becomes important to consider several items, for portable and interoperable security standards, to protect sensitive data being moved to or in the cloud. In this direction, author acknowledges that not all information used within a cloud system may qualify as confidential or fall under regulations requiring protection. Therefore, the security categories proposed in this case are based on information security lifecycle for protecting data

in terms of confidentiality, availability, and integrity (which can be applied not only to cloud environments, but also to any solution which requires basic interoperable and portable security integration). The complete organization is depicted in **Figure 2**.

5.3. The technical perspective

The technical dimension is subdivided into integration, compatibility, and APIs. In this case, the classification proposed are based on technical constraints placed on consumer's ability to achieve seamless integration and compatibility with user, administrative, and programming interfaces for using and controlling a cloud service. Since the interfaces and APIs of cloud services are not standardized, different providers use different APIs for what are otherwise comparable cloud services. These APIs expose the semantics (i.e., description of cloud services by its provider) and technologies (i.e., middleware and applications used to support a cloud service) used by a provider by providing the service management functionality. This implicit lack of standards (as pointed earlier) adoption by cloud providers is in fact a breeding ground for various types of heterogeneity (e.g., hardware and platform), because each cloud provider uses different technologies, protocols, and formats. This heterogeneity is a crucial problem as it gives rise to vendor lock-in situations in cloud computing. Thus, the need for a well-defined standard interface plays an important role toward achieving compatibility and manageability inside and between clouds. Then, cloud service consumers can take advantage of seamlessly integrating different provider offerings, combining benefits of each cloud to build solutions

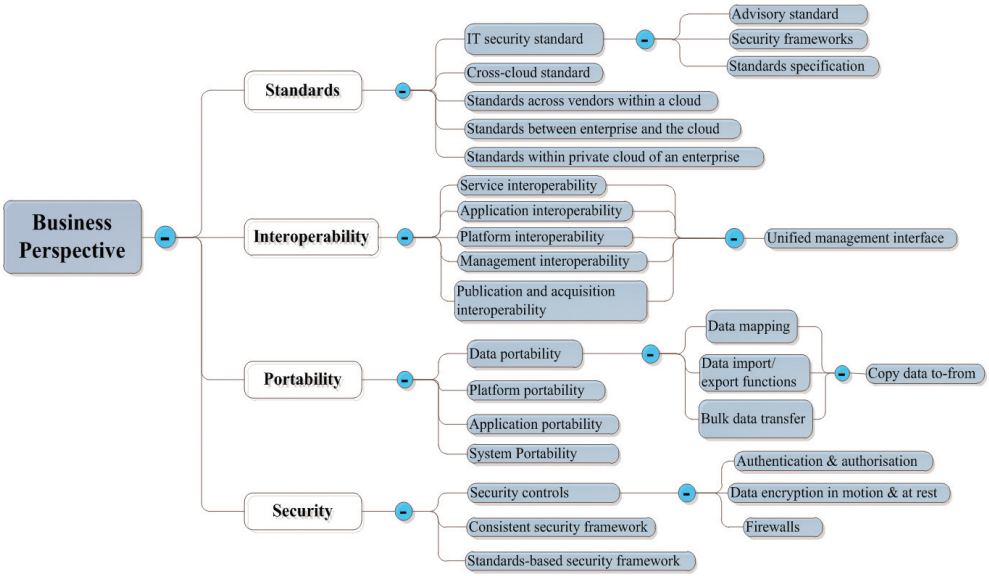

Figure 2. Vendor lock-in taxonomy-business perspective. NB: components from the business perspective of vendor lock-in are subdivided into four categories (i.e., standards, interoperability, portability and security). These elements are significant considerations to the use of cloud services, and are also indicators to how each component may trigger and/or intensify the risk of lock-in involved.

that are coherent to their respective business goals. The complete categorization of technical perspective of lock-in is presented in **Figure 3**.

5.4. The legal perspective

The need to avoid the risk(s) of cloud vendor lock-in from a legal perspective is to limit possible constraints on data, application, and services per the locations or national laws, as well as grant customers the free will to avoid dependence on only one external provider. The categorization in this dimension includes aspects related to contract and license issues, exit process or termination of use of a cloud service, judicial requirements and law (such as multiple data locations and privilege management). The legal perspective is split into four sub-categories (i.e., SLA compliance; contract termination and exit process; cloud migration strategies; and metadata and data ownership) per the service life cycle and measures in which various aspects of cloud services offered and managed for a cloud service consumer can result in a lock-in situation. It is also noted that the lock-in risks in this scenario cover the complete information lifecycle (i.e., generation, use, transfer, transformation, storage, archiving, and destruction) inside the cloud providers'

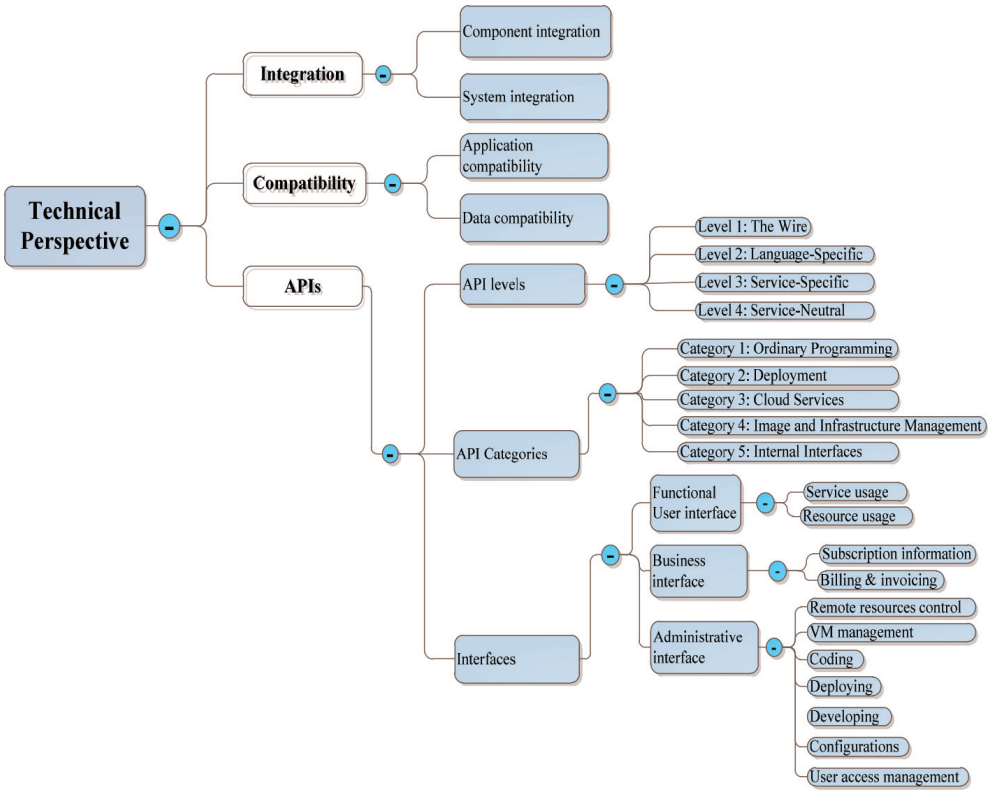

Figure 3. Vendor lock-in taxonomy—technical perspective.

perimeter and in its immediate boundaries (or interfaces) to the consumers. Audit and monitoring are also important aspects worth considering in the legal dimension, due to the requirements that a cloud provider should ensure to fulfill service agreements. For instance, the exit process or termination of the use of a cloud by a customer requires careful planning from an information security perspective. From a data security and storage perspective, it is important that once the customer has completed the termination process, none of the customer's data should remain with the provider. Thus, the exit process must allow customer to retrieve their data in a suitably secure form, backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must be retained until the exit process is complete. Meanwhile, customers are advised to negotiate directly with their cloud service provider to ensure appropriate exit process provisions and assurances that are included and adequately documented in their cloud SLA and contracts. The expansion of this categorization is depicted in **Figure 4**.

5.5. Our contribution

In this section, we examined current proprietary lock-in risk factors in cloud computing services and proposed a model for classifying these to aid better enterprise cloud procurement

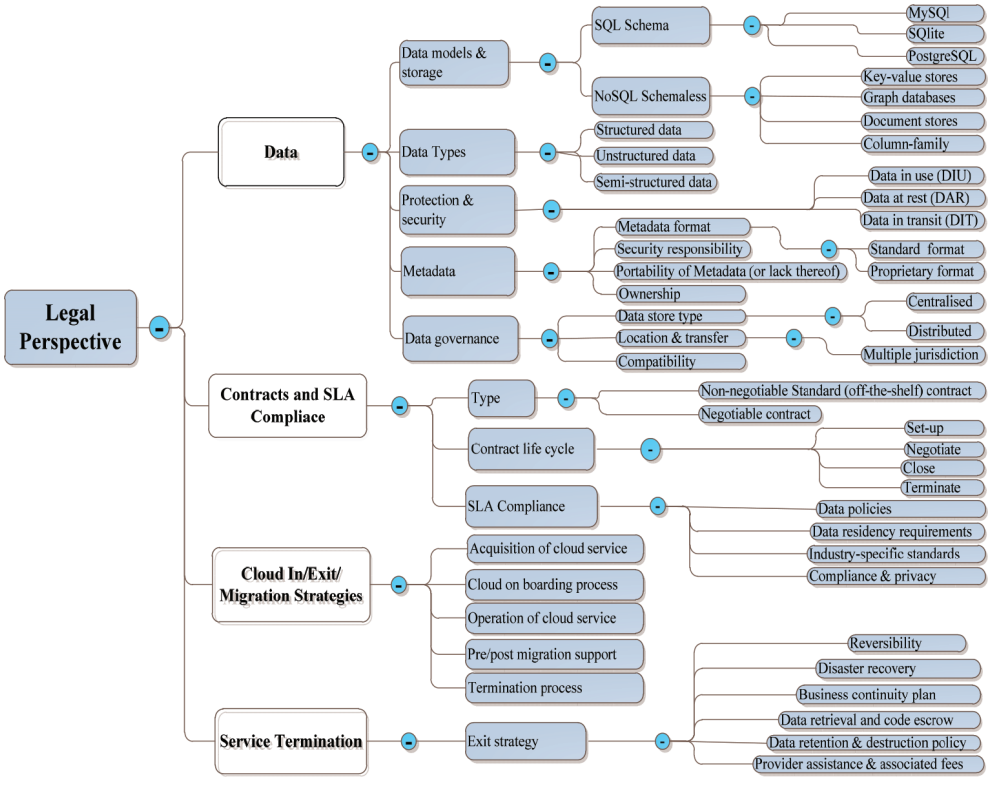

Figure 4. Vendor lock-in taxonomy—legal perspective.

and migration decision process. Aiming to organize this information into a useful tool for comparing, relating, and classifying already identified lock-in challenges and risks as well as future ones, we present a taxonomy proposal for cloud computing vendor lock-in. We focus on issues that are specific to cloud computing, without losing sight of important issues that also exist in other distributed IT systems. Here proposed taxonomy is capable of classifying both current and future cloud computing services for potential risks of single provider lock-in. The simple layered-tree structure used in the taxonomy development allows quick and easy analysis, by giving the user a set of core elements at each level. This clear structure makes analyzing and understanding the complexity of vendor lock-in challenges in cloud computing services more efficient than using table-based comparisons. While, table-based comparisons of cloud computing services exist [59], however, they are mainly for commercial use and the degree of detail varies greatly. Further, the taxonomy not only helps to categorize a cloud lock-in risk scenario, but it also helps potential customers and developers to point out what characteristics the service they seek or wish to develop should have (to avoid lock-in).

In summary, the contribution of this chapter is twofold. First, we identified the main risk factors of vendor lock-in that must be considered when transforming IT services to cloud-based solutions, or migrating to a cloud computing environment. These lock-in challenges were derived based on an extensive literature review and previous works on enterprise migration to public/private and/or hybrid cloud environment. We believe that the identified lock-in challenges are pertinent issues that require urgent solutions in the cloud environment, in order to pave the way for providing more standard and secured cloud services. Second, in order to classify and categorize the core elements of cloud computing lock-in, using a systematic classification scheme, taxonomy of cloud lock-in challenges is proposed. Moreover, this taxonomy extends our previous works presented in, respectively, providing an enhanced review of the cloud computing lock-in challenges previously presented, as well as a deeper analysis of the related work by discussing the main SaaS lock-in risk dimensions. Furthermore, we discuss the PaaS and IaaS lock-in aspects related to cloud computing, a fundamental yet still underserved field of research.

6. Conclusion

This chapter provides a comprehensive analysis of cloud computing vendor lock-in problem, and proposed taxonomy of cloud lock-in perspectives. The three main perspectives of cloud vendor lock-in problem(s) are: business (or economics) perspective, technical (or technological) perspective, and legal (or political) perspective. Together they provide a complete picture of cloud computing vendor lock-in challenge. The concerns addressed in each of the perspective have been precisely and concisely discussed in this chapter. The hierarchical categorization approach used in taxonomy assists in demonstrating how each element of the vendor lock-in problem relates to several other components in the architecture of a cloud computing system. At a high level, the model establishes a common language (i.e., ontology) for easy understanding and communication of the capabilities and requirements which should be standardized in a cloud environment to facilitate open collaboration and interoperability amongst cloud providers—thereby avoiding the risk of a single provider lock-in for cloud consumers. At a low

level, the model is further composed into taxonomy to support consumers cloud service selection and adoption strategy in terms of validating cloud provider's solutions to achieve architectural integrity of business solutions of an enterprises' cloud ecosystem. In contrast to existing works in the field, our study extends the current scope of cloud computing migration beyond one specific challenge area, instead it addresses the complex vendor lock-in problem from three main perspectives or categories—thereby contributing substantially to the growing body of knowledge on cloud computing.

In our future work, we present a high-level (combined) view of the proposed taxonomy. It will show the transformation between the different vendor lock-in perspectives. This high-level taxonomy of vendor lock-in risks identifies the key cloud computing interoperability, portability, API interface categories, as well as other relevant and intricate components of cloud systems that should be portable and interoperable. For example, standardization of the interfaces between these components is the first step to achieving interoperability and portability—as it prevents being locked into any cloud or provider. In the expanded taxonomy diagram, a layer represents a set of functional and non-functional requirements that provide similar capabilities or serve a similar purpose to support a vendor neutral (and technology-independent) sourcing strategy for cloud applications and services. We also survey various key works in the area and map them to our taxonomy to guide future design and development efforts.

Author details

Justice Opara-Martins

Address all correspondence to: joparamartins@bournemouth.ac.uk

Computing and Informatics Research Centre, Bournemouth University, Bournemouth, United Kingdom

References

[1] Sun X, Gao B, Zhang Y, An W, Cao H, Guo C, Sun W. Towards delivering analytical solutions in cloud: Business models and technical challenges. In: Proceedings of the IEEE 8th International Conference on e-Business Engineering (ICEBE 2011). Washington, USA: IEEE Computer Society; 2011. pp. 347-351

[2] Assunção MD, Calheiros RN, Bianchi S, Netto MA, Buyya R. Big data computing and clouds: Trends and future directions. Journal of Parallel and Distributed Computing. 2015;**79**:3-15

[3] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computing Systems. 2009;**25**(6):599-616

[4] Opara-Martins J, Sahandi R, Tian F. Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. Journal of Cloud Computing. 2016;**5**(1):4

[5] Di Martino B, Cretella G, Esposito A, Sperandeo RG. Semantic representation of cloud services: A case study for Microsoft windows azure, In: Intelligent Networking and Collaborative Systems (INCoS), 2014 International Conference on. 2014. pp. 647-652. DOI: 10.1109/INCoS.2014.76

[6] Satzger B, Hummer W, Inzinger W. Winds of change: From vendor lock-in to the meta cloud. IEEE Internet Computing. 2013;**1**:69-73

[7] Binz T, Breiter G, Leyman F, Spatzier T. Portable cloud services using tosca. IEEE Internet Computing. 2012;**3**:80-85

[8] Petcu D, Macariu G, Panic S, Craciun C. Portable cloud applicationsfrom theory to practice. Future Generation Computer Systems. 2013;**29**(6):1417-1430. DOI: 10.1016/j.future.2012.01.009

[9] Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. Above the Clouds: A Berkeley View of Cloud Computing, Technical Report UCB/EECS-2009-28. Electrical Engineering and Computer Sciences: University of California at Berkeley, Berkeley, USA; February 2009

[10] Katz DS, Jha S, Parashar M, Rana O, Weissman JB. Survey and Analysis of Production Distributed Computing Infrastructures. CoRR abs/1208.2649

[11] Toosi AN, Calheiros RN, Buyya R. Interconnected cloud computing environments: Challenges, taxonomy, and survey. ACM Computing Surveys (CSUR). 2014;**47**(1):7

[12] Hilley D. Cloud Computing: A Taxonomy of Platform and Infrastructure-Level Offerings. Georgia Institute of Technology; 2009

[13] Di Martino B, Cretella G, Esposito A. Classification and positioning of cloud definitions and use case scenarios for portability and interoperability. In: Future Internet of Things and Cloud (FiCloud), 3rd International Conference on. 2015. pp. 538-544. DOI: 10.1109/FiCloud.2015.119

[14] Abadi DJ. Data management in the cloud: Limitations and opportunities. IEEE data Engineering Bulletin. 2009;**32**(1):3-12

[15] Höfer CN, Karagiannis G. Cloud computing services: Taxonomy and comparison. Journal of Internet Services and Applications. 2011;**2**(2):81-94

[16] Rimal BP, Choi E, Lumb I. A taxonomy, survey, and issues of cloud computing ecosystems. In: Cloud Computing. London: Springer; 2010. pp. 21-46

[17] Clemons EK, Chen Y. Making the decision to contract for cloud services: Managing the risk of an extreme form of IT outsourcing. In System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE; 2011. pp. 1-10

[18] Cloud Computing Use Case Discussion Group. Cloud computing use case. White Paper version 1.0.5. 2009

[19] Crandell M. Defogging cloud computing: A taxonomy. 2008. Available from http://gigaom.com/2008/06/16/defogging-cloud-computing-a-taxonomy/

[20] Laird P. Different strokes for different folks: A taxonomy of cloud offerings. Enterprise cloud submit, INTEROP. 2009

[21] Ried S. Yet another cloud—How many clouds do we need? Retrieved from Forrester Research. 2009. http://www.forrester.com/

[22] Wang L, Ranjan R, Chen J, Benatallah B, editors. Cloud Computing: Methodology, Systems, and Applications. CRC Press; 2017

[23] Zafar F, Khan A, Malik SUR, Ahmed M, Anjum A, Khan MI, Javed N, Alam M, Jamil F. A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. Computers & Security. 2017;**65**:29-49

[24] Wan Z, Wang P. A survey and taxonomy of cloud migration. In: Service Sciences (ICSS), 2014 International Conference on. IEEE; 2014, May. pp. 175-180

[25] Islam T, Manivannan D, Zeadally S. A classification and characterization of security threats in cloud computing. International Journal of Next-Generation Computing. 2016;**7**(1)

[26] Di Martino B., Cretella G, Esposito A. Towards a unified owl ontology of cloud vendors' appliances and services at paas and saas level. In: Complex, Intelligent and Software Intensive Systems (CISIS), 2014 Eighth International Conference on. IEEE; 2014, July. pp. 570-575

[27] Fatema K, Emeakaroha VC, Healy PD, Morrison JP, Lynn T. A survey of cloud monitoring tools: Taxonomy, capabilities and objectives. Journal of Parallel and Distributed Computing. 2014;**74**(10):2918-2933

[28] Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem. 2016. arXiv preprint arXiv:1609.01107

[29] Mahjoub M, Mdhaffar A, Halima RB, Jmaiel M. A comparative study of the current cloud computing technologies and offers. In: Proceedings of the 2011 First International Symposium on Network Cloud Computing and Applications. IEEE Computer Society; 2011. pp. 131-134

[30] Peng J, Zhang X, Lei Z, Zhang B, Zhang W, Li Q. Comparison of several cloud computing platforms. In: Proceedings of the 2009 Second International Symposium on Information Science and Engineering. IEEE Computer Society; 2009. pp. 23-27

[31] Wind S. Open source cloud computing management platforms: Introduction, comparison, and recommendations for implementation. In: 2011 IEEE Conference on Open Systems, ICOS. 2011. pp. 175-179

[32] Cordeiro T, Damalio D, Pereira N, Endo P, Palhares A, Goncalves G, Sadok D, Kelner J, Melander B, Souza V, Mangs JE. Open source cloud computing platforms. In: 2010 9th International Conference on Grid and Cooperative Computing, GCC. 2010. pp. 366-371

[33] de Oliveira D, Baiao FA, Mattoso M. Towards a taxonomy for cloud computing from an e-science perspective. In: Cloud Computing. London: Springer; 2010. pp. 47-62

[34] Liu F, Tong J, Mao J, Bohn R, Messina J, Badger L, et al. NIST cloud computing reference architecture. September 2011. http://www.nist.gov/manuscriptpublication-search.cfm?pub_id=909505

[35] Rimal BP, Eunmi C, Lumb I. A taxonomy and survey of cloud computing systems. In: Fifth International Joint Conference on INC, IMS and IDC, 2009, NCM'09. 2009. pp. 44-51

[36] Beloglazov A, Buyya R, Lee Y, Zomaya A. A Taxonomy and Survey of Energy Efficient Data Centers and Cloud Computing Systems. 2010

[37] OpenCrowd—Cloud computing vendors taxonomy. September 2012. http://cloudtaxonomy.opencrowd.com/

[38] Intel Corporation. Cloud computing taxonomy and ecosystem analysis. September 2012. http://www.intel.com/content/dam/doc/case-study/intel-it-cloudcomputing-taxonomy-ecosystem-analysis-study.pdf

[39] Forrester. The evolution of cloud computing markets. September 2012. www.forrester.com/go?docid=57232

[40] Opara-Martins J, Sahandi R, Tian F. Critical review of vendor lock-in and its impact on adoption of cloud computing. In: Information Society (i-Society), 2014 International Conference on; November. IEEE; 2014. pp. 92-97

[41] Opara-Martins J, Sahandi R, Tian F. Implications of integration and interoperability for enterprise cloud-based applications. In: International Conference on Cloud Computing. Springer International Publishing; 2015. pp. 213-223

[42] Opara-Martins J, Sahandi R, Tian F. A business analysis of cloud computing: Data security and contract lock-in issues. In: P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on; November. IEEE; 2015. pp. 665-670

[43] Opara-Martins J, Sahandi R, Tian F. Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. Journal of Cloud Computing. 2016; **5**(1):1-18

[44] Opara-Martins J, Sahandi R, Tian F. A holistic decision framework to avoid vendor lock-in for cloud SaaS migration. Computer and Information Science. 2017;**10**(3):29

[45] Conway G, Curry E. Managing cloud computing—A life cycle approach. In: CLOSER. 2012. pp. 198-207

[46] Conway G, Curry E. The IVI cloud computing life cycle. Cloud Computing and Services Science. 2013:183-199

[47] Sahandi R, Alkhalil A, Opara-Martins J. SMEs' perception of cloud computing: Potential and security. In: Working Conference on Virtual Enterprises; October. Springer Berlin Heidelberg; 2012. pp. 186-195

[48] Sahandi R, Alkhalil A, Opara-Martins J. Cloud computing from SME's perspective: A survey-based investigation. Journal of Information Technology Management. 2013;**24**(1):1-12

[49] Polikaitis A. Vendor and Sourcing Management: Maintaining Control of Vendor Relationships by Avoiding Vendor Lock-in. IDC Opinion Report. 2015. http://core0.staticworld.net/assets/2016/04/19/idc-vsm-avoiding-vendor-lock-in.pdf [Accessed 12 November 2016]

[50] Burns M. Cloud-based ERP: The risk of vendor lock-in. In: Emerging Issues and Technologies for ERP Systems, Class of Enterprise Systems Integration, 2011-12. UK: School of Computing and Mathematics, University of Derby; 2012. pp. 77-80

[51] Sakr S, Liu A, Batista D, Alomari M. A survey of large scale data management approaches in cloud environments. IEEE Communications Surveys Tutorials. 2011;**13**(3):311-336

[52] Peng HT, Hsu WW, Chen CH, Lai F, Ho JM. September. FinancialCloud: Open cloud framework of derivative pricing. In: Social Computing (SocialCom), 2013 International Conference on. IEEE; 2013. pp. 782-789

[53] Dillion T, Wu C, Chang E. Cloud computing: Issues and challenges, Advanced Information Networking and Application (AINA). In: 24th IEEE International Conference; 2010. 2010. pp. 752-757

[54] Garg SK, Versteeg S, Buyya R. A framework for ranking of cloud computing services. Future Generation Computer Systems. 2013;**29**(4):1012-1023

[55] Cusumano M. Cloud computing and SaaS as new computing platforms. Communications of the ACM. 2010;**53**:27-29

[56] Ardagna D, Di Nitto E, Casale G, Petcu D, Mohagheghi P, Mosser S, Matthews P, Gericke A, Ballagny C, D'Andria F, Nechifor CS. Modaclouds: A model-driven approach for the design and execution of applications on multiple clouds. In: Proceedings of the 4th International Workshop on Modelling in Software Engineering. IEEE Press; 2012. pp. 50-56