Opara-Martins *et al. Journal of Cloud Computing: Advances, Systems and Applications* (2016) 5:4
DOI 10.1186/s13677-016-0054-z

Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH **Open Access**

Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective

Justice Opara-Martins*, Reza Sahandi and Feng Tian

Abstract

Vendor lock-in is a major barrier to the adoption of cloud computing, due to the lack of standardization. Current solutions and efforts tackling the vendor lock-in problem are predominantly technology-oriented. Limited studies exist to analyse and highlight the complexity of vendor lock-in problem in the cloud environment. Consequently, most customers are unaware of proprietary standards which inhibit interoperability and portability of applications when taking services from vendors. This paper provides a critical analysis of the vendor lock-in problem, from a business perspective. A survey based on qualitative and quantitative approaches conducted in this study has identified the main risk factors that give rise to lock-in situations. The analysis of our survey of 114 participants shows that, as computing resources migrate from on-premise to the cloud, the vendor lock-in problem is exacerbated. Furthermore, the findings exemplify the importance of interoperability, portability and standards in cloud computing. A number of strategies are proposed on how to avoid and mitigate lock-in risks when migrating to cloud computing. The strategies relate to contracts, selection of vendors that support standardised formats and protocols regarding standard data structures and APIs, developing awareness of commonalities and dependencies among cloud-based solutions. We strongly believe that the implementation of these strategies has a great potential to reduce the risks of vendor lock-in.

Keywords: Cloud computing, Vendor lock-in, Enterprise migration, Cloud adoption, Cloud API's, Interoperability, Portability, Standards, DevOps

Introduction

Cloud computing is to offer an opportunistic business strategy to enterprises (small or large), to remain competitive and meet business needs [1–3]. Whilst this seems like an attractive proposition for both public and private companies, a number of challenges remain inadequately addressed. A recent survey conducted by [4] reported security and vendor lock-in as major barriers to cloud adoption across the United Kingdom (UK) market. The European Network and Information Security Agency (ENISA) and European Commission (EC) have recognized the vendor lock-in problem as a one of the greatest obstacles to enterprise cloud adoption [5].

The reviews of existing literature [6–12] have shown that previous studies have focused more on interoperability and portability issues of cloud computing when lock-in is discussed. Amongst many problems being discussed are: the lack of standard interfaces and open APIs [13], the lack of open standards for VM format [14] and service deployment interfaces [15], as well as lack of open formats for data interchange. These issues result in difficulties in integration between services obtained from different cloud providers as well as between cloud resources and internal legacy systems [16]. Consequently, this renders the interoperability and portability of data and application services difficult. The emergent difficulty is a direct result of the current differences between individual cloud vendors offerings based on non-compatible underlying technologies and proprietary standards. In essence, cloud providers often propose their own solutions and proprietary interfaces for access to resources and services. This heterogeneity of cloud provider solutions (i.e. hardware and software) and

* Correspondence: joparamartins@bournemouth.ac.uk
Faculty of Science and Technology, Bournemouth University, Bournemouth, UK

© 2016 Opara-Martins et al. **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

service interfaces is a crucial problem since most of the current resources bind the customer to stick with one cloud technology due to high cost in porting the applications and data to a different provider's interface. The heterogeneity in cloud computing is simply the existence of differentiated hardware, architectures, infrastructure, and technology used by cloud providers. Many cloud vendors provide services based on custom-built policies, infrastructure, platforms, and APIs that make the overall cloud landscape heterogeneous. Such variations cause interoperability, portability, and integration very challenging.

Following the principle that compatible interfaces are important in a cloud environment, two implementations of the same cloud service may store and process data very differently. This may well also involve storing derived and implementation specific data differently [17]. Without proper definitions for import and export formats, a set of data from one service implementation will probably be meaningless when imported into another cloud service. For example, a cloud service may be accessed and used by a wide variety of clients, including mobile, desktops and even tablet PCs. However, the information created and consumed by those services can still be limited to a single vendor if a proprietary data format is used. Further, this can create a degree of instability and data incompatibility issue as interfaces to the functionality may be proprietary, and thus any solution that is built to leverage the functionality provided cannot be easily migrated to a competitive cloud service offering [15]. So, while customers might be able to access and use the services from a variety of clients, the ability to move seamlessly from one vendor to another may be difficult because of other dependencies such as different data formats. Clearly, this problem has an impact on interoperability and data portability between clouds.

At the core of all these problems, we can identify concerns about consumers' demand to migrate data to and from different clouds (data portability), and interoperability between clouds. Research has already addressed movability and migration on a functional level [18, 19]. However, migration is currently far from being trivial. The two main reasons are the lack of world-wide adopted standards or interfaces to leverage the dynamic landscape of cloud related offers [14], and absence of standards for defining parameters for cloud applications and their management. Without an appropriate standardized format, ensuring interoperability, portability, compliance, trust, and security is difficult [12]. Standards continue to rapidly evolve in step with technology. Hence, standards may be at different stages of maturity and levels of acceptance. But, unless the standards are well-accepted and widely used, such standards remain a questionable solution [20]. In other words a partially adopted standard would represent a poor solution. Essentially, this explicit lack of standards to support portability and interoperability among cloud providers stifles the market competition and locks customers to a single cloud provider [21]. To expatiate further, potential difficulties (by primarily technological means) in achieving interoperability and portability lead to lock-in – resulting in customer dependency on the services of a single cloud computing provider [22]. From a legal stance, the dependency can be aggravated by the abusive conduct of a cloud computing provider within the meaning of Article 102 TFEU (Treaty on the Functioning of the European Union) [18], where other providers are excluded from competing from the customers of the initial cloud provider. In such situations, limitations to interoperability and portability could be seen as an abuse by a dominant provider using this practice as a technical means to stifle (i.e. monopolize) competition. Such practices distort competition and harm consumers by depriving them of better prices, greater choices and innovation. Hence, the competition law has the role of ensuring competition is maintained and enforced in the market by regulating anti-competitive conduct by cloud providers. To this end, it can be concluded that cloud interoperability (and data portability) constraints are potential results of anti-competitive environment created by offering services with proprietary standards.

Vendor lock-in

The vendor lock-in problem in cloud computing is the situation where customers are dependent (i.e. locked-in) on a single cloud provider technology implementation and cannot easily move in the future to a different vendor without substantial costs, legal constraints, or technical incompatibilities [23]. To substantiate further from the lenses of a software developer, the lock-in situation is evident in that applications developed for specific cloud platforms (e.g. Amazon EC2, Microsoft Azure), cannot easily be migrated to other cloud platforms and users become vulnerable to any changes made by their providers [24]. Actually, the lock-in issue arises when a company, for instance, decides to change cloud providers (or perhaps integrate services from different providers), but is unable to move applications or data across different cloud services because the semantics of resources and services of cloud providers do not match with each other. This heterogeneity of cloud semantics [25] and cloud Application Program Interfaces (APIs) creates technical incompatibility which in turn leads to interoperability and portability challenges [26]. This makes interoperation, collaboration, portability and manageability of data and services a very complex and elusive task. For these reasons, it becomes important from the view point of the business to retain the flexibility to change providers according to business concerns or even keep in-house some of the components that are less mission-critical due to security related risks. Interoperability and portability among cloud providers can avoid the problem of vendor lock-in. It is the way toward a more competitive market for cloud providers and customers.

Lock-in affects cloud migration

Interoperability and portability are essential qualities that affect the cloud under different perspectives [7, 13], due to the risk of vendor lock-in. While many studies cite vendor lock-in as a major barrier to cloud computing adoption [3, 27–32], yet due to its complexity, a lack of clarity still pervades. Without a clear insight into how such complex decision is made to avoid lock-in, it is difficult to identify gaps where further research is beneficial for business adopters. Existing solutions and studies addressing the lock-in problem have predominantly been technological oriented, where the focus is on knowledge garnered through logical deduction and technical expertise. Such approach is compromised by ignoring organisations' awareness and perception of the lock-in problem. For example, how is cloud lock-in experienced or understood from the business stance? Limited in-depth studies exist to investigate the complexity of cloud lock-in problem within enterprise organisations. Likewise the customers, who are willing to choose the cloud services without being strictly bond to a specific solution, are mostly neglected. Advances in cloud computing research have in recent years resulted in a growing interest for migration towards the cloud. But due to concerns about the risks of vendor lock-in, as noted by [33], organisations would particularly welcome standards that address application migration (e.g. Open Virtualization Format (OVF)) and data migration (e.g. Amazon S3 API) because such standards mitigate lock-in concerns. Various standardisation solutions from different industry bodies have been developed for increasing interoperability and portability within diverse cloud computing services [32, 34]. However, initiatives by multiple standard bodies, researchers, and consortiums could indirectly lead to the possibility of multiple standards emerging with possible lack of consensus, thereby deteriorating the lock-in problem even further.

In spite of these legitimate concerns and technical complexity, our study aims to answer the following two questions of interest to business adopters: *1)* "How to avoid being locked-in to a single cloud provider? *2*) How easy and secure is it to deploy existing cloud artefacts (e.g. software applications, databases, data, virtual servers etc.) on another service provider's platform without modification to the artefacts – which would reduce the financial benefit of the migration?" The former applies more to companies who have migrated or are looking to adopt more cloud solutions, whereas the latter is closely related to companies considering moving core systems into the cloud environment. Giving answers to these questions is deceptively easy and straightforward, but the reality is different. Presently, for many companies, there is a large amount of sensitive data and IT assets in-house which can deter them to migrate to the cloud due to risks of vendor lock-in, security and privacy issues. For these reasons, it becomes not only critical to consider security and privacy concerns but also related issues such as integration, portability, and interoperability between the software on-premise and in the cloud [35], should be taking into account. Therefore, organisations must be aware of appropriate standards and protocols used by cloud providers to support data/ application movability. Moreover, the ease of moving data across (i.e. portability) cloud providers' platform mandates data to be in a compatible format [34], and includes the need to securely delete the old storage [36]. In other words, the ability to move data/application about is of crucial importance, as much as the effort involved in actually moving – inability to achieve this portends large as a management issue for cloud computing. To further complicate matters, maintaining compliance with governmental regulations and industry requirements adds another layer of considerations to the management of data. Whether or not organisations can easily shift their data/application about seamlessly, still remains one of the biggest issues facing cloud adoption across diverse industries. Based on our findings, we propose strategic solutions that enterprises can follow to avoid entering into vendor lock-in situations.

Methodology

Research design

To explore factors that contribute to a lock-in situation in cloud computing, epistemologically, our study design in this paper consists of two distinct phases, as depicted in Fig. 1.

Phase 1: pilot interview study

In the pilot study, qualitative data were collected through the use of open-ended interviews with IT practitioners to explore the business-related issues of vendor lock-in affecting cloud adoption. Five participants from different industry sectors and organizations were purposely selected for in-depth interviews. They included a security expert, cloud advisor, IT technician, business end user, and an IT manager. The purpose was to explore the cloud lock-in problems, and explore the

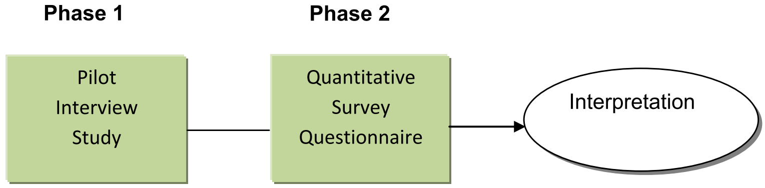


Fig. 1 Two phase exploratory research design

prevalence of its dimensions, by gaining a range of insights from different IT professionals.

Each interview data collected was transcribed verbatim, and the data was analysed using the Nvivo 8 QSR software package for data storage, coding, and theme development [37]. Due to the participatory and time consuming nature of this pilot phase, it was deemed important that each interview be given considerable time for analysis. Seven themes emerged in relation to participants' perception of vendor lock-in problem and how this affects their migration and adoption decisions. The themes were; (1) standards, (2) interoperability in the cloud environment, (3) the need for portability, (4) integration challenges, (5) contract exit strategy, (6) data ownership (7) security and privacy issues. The analysis of the responses across the seven themes showed the participants' priority of the themes. As a result, data portability and interoperability concerns were the most discussed theme in relation to vendor lock-in. However, participants were less interested to divulge about the security and contract exit strategies, including data ownership and privacy risks. Subsequent to the pilot interviews a questionnaire was designed for a survey. The main issues raised at the interviews were incorporated into the questionnaire.

Phase 2: quantitative survey questionnaire

The goal of phase 2 was to identify and evaluate the risks and opportunities of vendor lock-in which affect stakeholders' decision-making about adopting cloud solutions. This phase of the research design is based on an online survey tool [38]. Participants were selected and invited by e-mail to participate in the survey. The aim of the survey was an in-depth study of the effect of vendor lock-in in migration of enterprise IT resources to the cloud (Additional files 1 and 2).

Questionnaire data collection

The target population mainly consists of large corporations and small to medium-sized enterprises (SMEs) located in the United Kingdom (UK). Participants in the survey varied between IT professionals, managers and decision-makers within their respective business enterprise. A total of 200 companies were invited to participate in the survey. Overall, 114 participants responded and completed the online survey, which constituted a satisfactory response rate of 57 %. To supplement for a higher response rate as possible and to avoid skewing the data, a paper-based questionnaire was administered in person to participants at conferences and workshops. 12 completed responses were received, giving a good response rate of 63 %. Prior to presenting the findings of the survey, it should be pointed out that the questionnaire comprised of many questions, however only those which revealed important issues of lock-in are presented and discussed in context. For the purpose of analysis, Table 1 presents a socio-demographic profile of the companies and participants in the survey. As shown in Table 1, the samples were slightly dominated by organisations sized between 251 and 500 employees, and majority came from ICT organisations, followed by education, consumer business, public sector and healthcare.

Organisations in the survey

In Fig. 2, a vast majority of the respondents were IT managers and CIOs. These are the key people responsible for

Table 1 Socio-Demographic profile of participant organisation

Organisation Size	Percentage
1–24	7 %
25–50	12 %
51–250	28 %
251–500	39 %
Over 501 Employees	14 %
Total:	100 %
Industry Sector	Percentage
Construction sector	3.5 %
Consumer Business	10.5 %
Education sector	15.8 %
Financial services	4.4 %
ICT services	17.5 %
Production & Manufacturing	7.0 %
Public sector & Healthcare	11.4 %
Services industry	10.5 %
Other	19.3 %
Total:	100

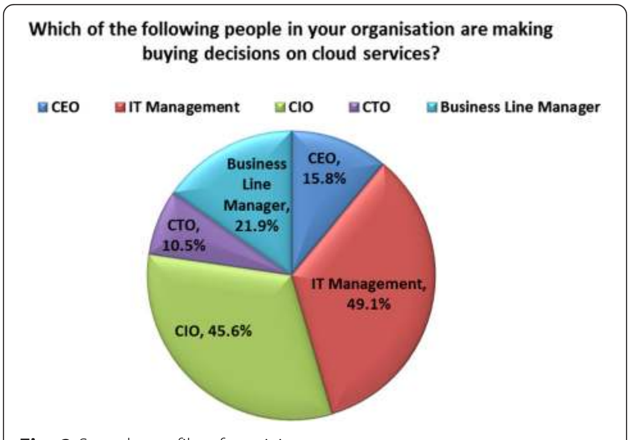


Fig. 2 Sample profile of participants

making buying decisions in the cloud adoption process. This indicates that the role of IT manager in most organisations is still considered paramount as opposed to premise that the advent of cloud computing will make IT management obsolete – that is, some of the existing IT management roles will be moved to cloud providers [39]. Arguably this is not the case today as pointed by [40]. Cloud computing is seen as a viable deployment model within the context of UK organisations IT strategy, but it is not seen as the only viable model. Most organisations foresee the continued use of on-premise IT alongside cloud-based services for the foreseeable future, evolving into a prevalence of hybrid IT estates.

Findings

The analysis of the results show over 49 % of top level IT managers influence the decisions for adopting cloud services. This confirms that cloud computing adoption in the UK is seen as a viable IT deployment model. Moreover, more than half (50.9 %) of the organisations polled in the study are already using cloud services for at least one application domain within their organisation. The higher majority (69 %) utilise a combination of cloud services and internally owned applications (i.e. hybrid IT) for organisation's needs (Fig. 3).

Adoption of cloud computing by UK businesses

The survey affirms that the concept of using cloud computing services to address the business IT needs has established a mainstream deployment across organisations of various sizes. To further substantiate this matter, interestingly about 36 % of participants confirmed using a hybrid (public and private) cloud deployment model as opposed to a private cloud. Only 46 % of UK firms participated in the survey use public cloud services, in spite of the associated security risks (Fig. 4). The rate of adoption has been motivated by numerous indicators for effective cloud deployment decision. The most cited reasons for adopting cloud computing includes better scalability of IT resources (45.9 %), collaboration (40.5 %), cost savings (39.6 %) and increased flexibility (36.9 %). This suggests that organisations are allured to utilising cloud services due to the perceived business benefits of cost savings, IT flexibility and business agility.

The business benefits of cloud migration

In addition to the reasons for why the cloud model has achieved a mainstream deployment status across UK organisations, identifying the actual benefits of cloud computing is critical to further our understanding of motivations to migrate to cloud-based services. As shown in Fig. 5, the majority of the respondents identified capacity and scalability (70.3 %), increased collaboration, availability, geography and mobility as benefits for migration. However, further analysis have shown, from a business stance, that for organisations with more than

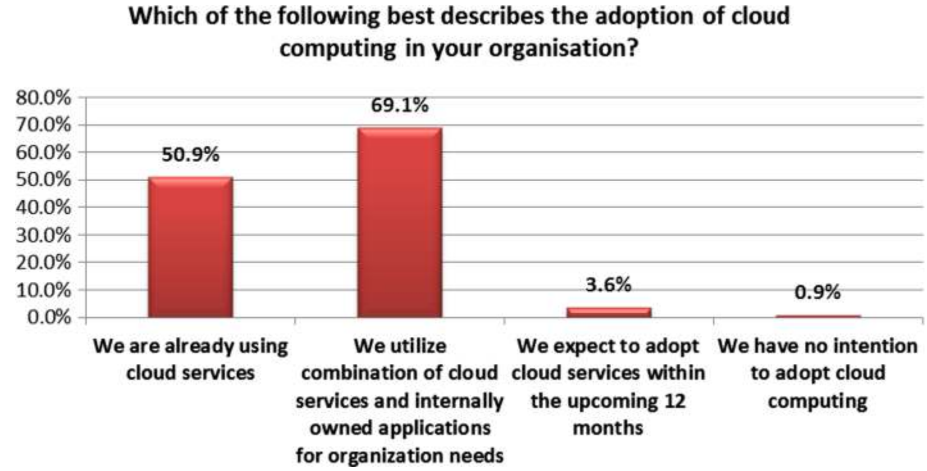


Fig. 3 Cloud adoption maturity in UK

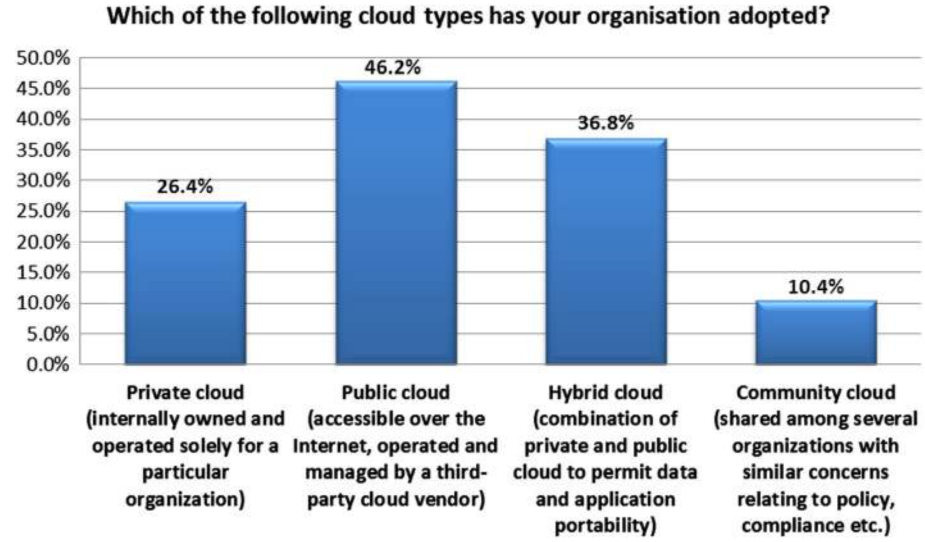
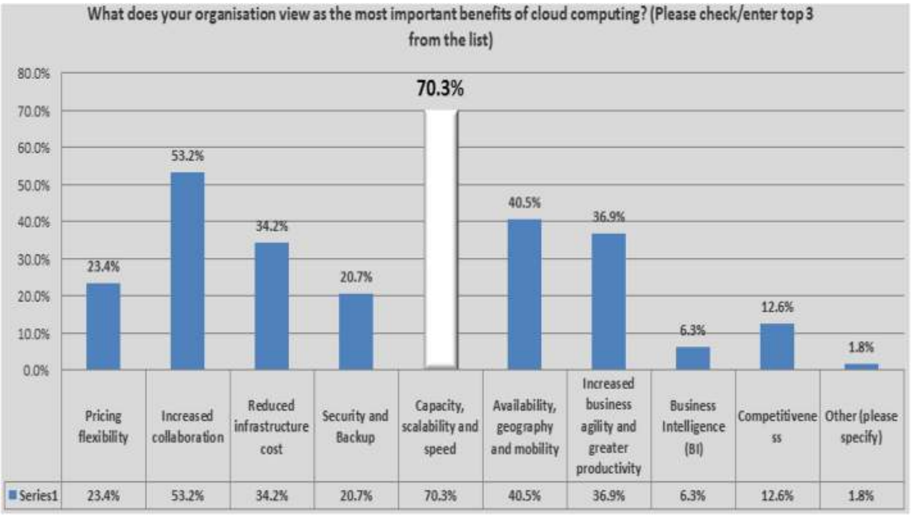


Fig. 4 Service deployed models

250 employees, the three most important realised benefits reported by participants are reduced infrastructure cost, ubiquity, and increased collaboration respectively. This indicates that the business benefits of migrating to the cloud vary across different organisation sizes. Moreover, the results also show slight difference between the motivations for adoption and the actual benefits realised from using cloud services.

Challenges to cloud implementation for UK businesses

In order to identify the factors that have an impact on cloud implementation and purchasing decisions, this study explored "what are the greatest barriers for implementing cloud computing for organisations?" Fig. 6 shows the barriers identified by the participants. Respondents identified systems and data security risks, loss of control and over dependence on a single cloud provider (35.1 %) as core existing barriers to future cloud implementation. To confer from this result, the security is still a major concern for UK businesses in implementing cloud solutions. In fact, this is due to lack of trust [11], often associated with worries about loss of control (i.e. in terms of system availability and business continuity risks), as indicated by (48.6 %) participants in the study. For instance, some organisations are worried about security within the cloud (i.e. data centres), while others feel that moving data into different geographies can have regulatory (compliance) implications. Besides, another barrier to



	Pricing flexibility	Increased collaboration	Reduced infrastructure cost	Security and Backup	Capacity, scalability and speed	Availability, geography and mobility	Increased business agility and greater productivity	Business Intelligence (BI)	Competitivene ss	Other (please specify)
■ Series1	23.4%	53.2%	34.2%	20.7%	70.3%	40.5%	36.9%	6.3%	12.6%	1.8%

Fig. 5 Benefits of cloud computing to UK Enterprises

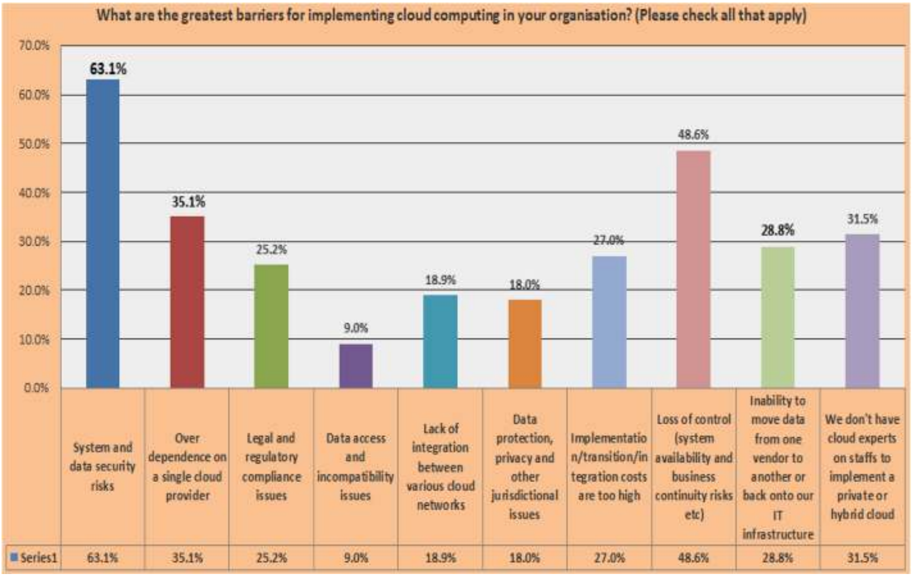


Fig. 6 Barriers to cloud implementation in the UK

cloud implementation evident in Fig. 6 is legal and regulatory compliance issues (25.2 %). Moreover, the findings tie in with a recent study published by [41], of which (57 %) participants identified "the biggest challenge in managing data security and privacy is compliance". However, regarding systems and data security risks (63.1 %), cloud service providers can demonstrate their compliance with, and adherence to, industry-accepted standards for data security and integrity. In essence, this will show transparency in practice and capability, and also assist the establishment of trust for organisations to implement/deploy their most critical, data-intensive functions and processes in the cloud.

Cloud application usage and service adoption among UK organisations

In order to identify the opportunities which may affect stakeholders' and decisions for or against cloud migration, this study explored which applications have adopted from cloud services, which local applications are considered for moving to the cloud. It also explored which applications for whatever reason, were not intended to adopt from the cloud model. The findings presented herein continue to validate cloud solutions as being pervasive options across UK organisations and industry sectors. The results in Fig. 7 suggest that general purpose applications such as email and messaging,

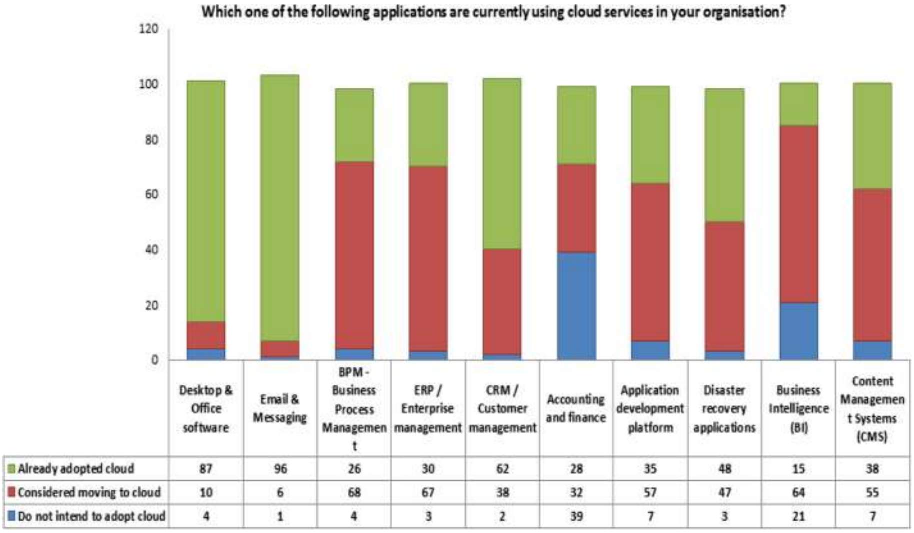


Fig. 7 Cloud-based CRM and ERP service adoption rates soar

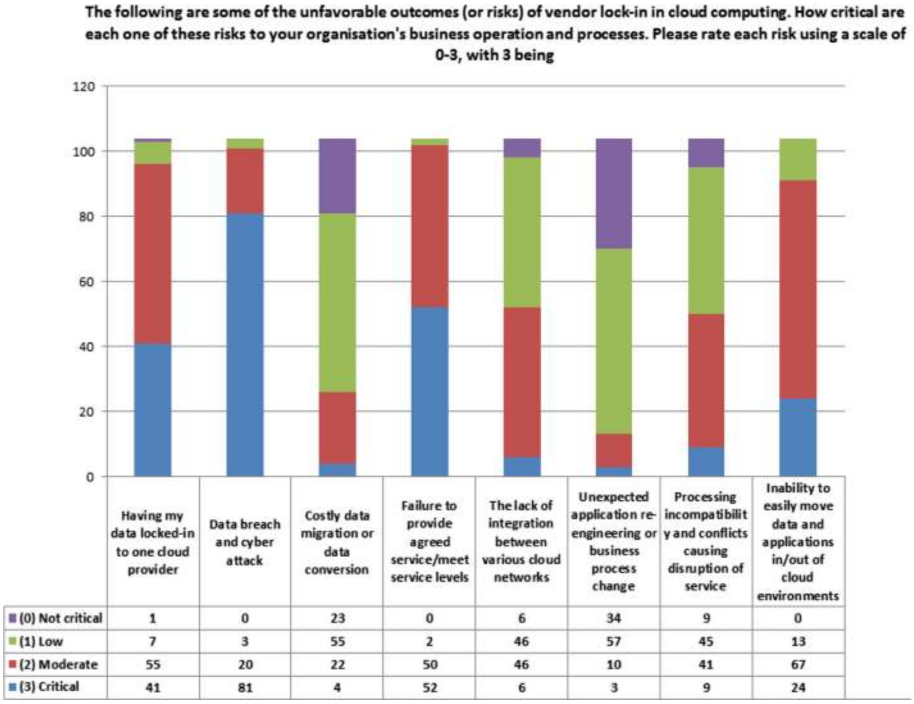
desktop and office software, etc. have all adopted the cloud delivery model. It should be noted that the widespread and reckless sign of adoption could pose significant risks, as the cloud computing era is still evolving. This is further reinforced by respondents who consider moving business process management (68 %), enterprise management (67 %), and business intelligence applications (64 %) respectively to the cloud. This certainly reflects the impact that the cloud has on the delivery and use of enterprise software applications, as identified by respondents.

The one application which is identified by most respondents as not suitable for cloud deployment is accounting and finance (39 %), perhaps due to data security concerns. Moreover, further data analysis in cloud adoption rate across organisations, realised that larger enterprises find disaster recovery, (ERP) and business process management applications (BPM) as the best fit for cloud migration. However, for smaller enterprises, the adoption of (non-mission critical) cloud-based applications mirrors their use of email messaging, desktop hosting and Customer Relationship Management (CRM) applications for collaboration. Remarkably, the lower cost and flexibility that cloud-based applications offer is ideal for small businesses, as they are agile and often run with teams that are spread over wide geographical regions. In essence, these applications are better suited for online delivery [42].

Vendor lock-in concerns and challenges in cloud migration

As cloud computing adoption rate soars across the UK market, the risks of vendor lock-in is also prevalent. How lock-in critically affects an organisations' business application and operation in the cloud cannot be overemphasized or underestimated. For example, Fig. 8 paints a clear admonitory picture of how UK businesses rate the risks of vendor lock-in against the decision to migrate/adopt cloud services. The risks (in Fig. 8) were identified from the initial pilot interviews and also from the literature [9–11, 13]. Moreover, the following risks (i.e. inability to move data and applications in/out of cloud environments, data ownership and cyber breaches) in Fig. 8 were critical themes that emerged from the unstructured interviews with IT practitioners. The results in Fig. 8, highlights that besides the risks of data breach and cyber-attack, or failure to meet agreed service levels, UK businesses are also concerned about having corporate data locked-in to a single cloud provider. These concerns affect the wider business functions where an enterprise is using cloud to perform essential business activities to keep operations running.

In the study it was deemed paramount to first assess participants current perception of the term "vendor lock-in" in the context of cloud computing. As shown in Fig. 9, only 44 % of respondents indicated to have a basic understanding of the term. This indicates that whilst UK



	Having my data locked-in to one cloud provider	Data breach and cyber attack	Costly data migration or data conversion	Failure to provide agreed service/meet service levels	The lack of integration between various cloud networks	Unexpected application re-engineering or business process change	Processing incompatibilit y and conflicts causing disruption of service	Inability to easily move data and applications in/out of cloud environments
🟪 (0) Not critical	1	0	23	0	6	34	9	0
🟩 (1) Low	7	3	55	2	46	57	45	13
🟥 (2) Moderate	55	20	22	50	46	10	41	67
🟦 (3) Critical	41	81	4	52	6	3	9	24

Fig. 8 The potential for vendor lock-in risks is exacerbated in the cloud

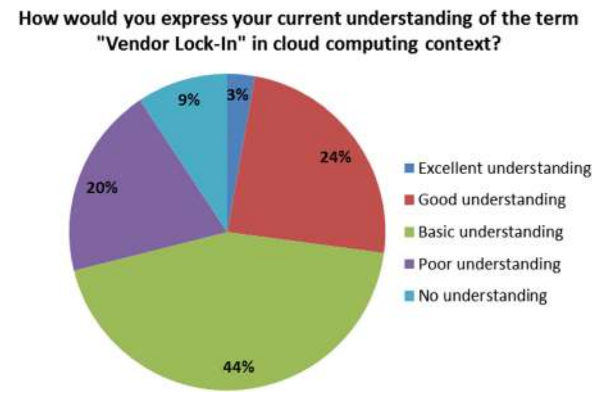


Fig. 9 UK Business perception of vendor lock-in

organisations are rapidly migrating and adopting cloud services, only a few (3 %) had exceptional knowledge. This means the lack of clarity on the problem of vendor lock-in still pervades. In part, this gap of knowledge means that organisations are not aware of the inherent lock-in problem within the cloud environment. However, the result implies that organisations with basic knowledge may not yet have experienced a cloud lock-in situation. A possible explanation for this may be attributed to the immaturity of the cloud computing ecosystem. If organisations' previous experiences in IT are compatible with the existing information and the infrastructure, then the degree of lock-in introduced by service providers will be consistent with the current knowledge and practice. Hence, in order to develop a comprehensive understanding to manage the risks associated with lock-in, organisations must first define what the lock-in means to them. This requires mapping and cross-examining the challenges of lock-in with different cloud service types (i.e. infrastructure, platform and software) and deployment models (i.e. public, private or hybrid). Comprehending the term "vendor lock-in" is critical to further our understanding. In agreement with the definition of vendor lock-in provided in [2] by Armbrust et al., in Table 2 as many as 71 % of the participants claimed vendor lock-in risks will deter their organisations from adopting more cloud services, although some respondents were unsure.

Core risk factors of lock-in

In an effort to highlight factors which may affect future cloud migration decisions, participants were requested to identify practical challenges of lock-in they encountered when using cloud services. These issues relate to lack of integration points between existing management tools (47.7 %), incompatibility issues with on-premise software, and inability to move to another service provider or take data in-house (Fig. 10). Overall, the results indicate that these challenges closely relate to interoperability and data portability issues prevalent in the cloud environment. Moreover further results show that a significant majority (76.6 %) of participants were unsure of relevant (existing or emerging) standards to support interoperability across clouds and portability of data from one cloud provider to another.

Table 2 Response indicator suggest Lock-in is a deterrent to Cloud migration

Definitely yes	Possibly yes	Not sure	No
9 %	71 %	11 %	9 %

To confer from Fig. 10, the main challenges associated with cloud lock-in are integration and incompatibility issues, followed by data portability. However, as shown in Fig. 11, when asked to identify best practices to minimize lock-in risks in cloud migration, most business respondents identified the following as top mitigation strategies: (a) making well-informed decisions before selecting vendors and/or signing cloud contracts (66.4 %); (b) the need for an open environment for continuous competition between providers in the cloud service market (52.3 %); (c) use of standard software components with industry-proven interfaces (39.3 %). Equally, in the case of managing the risks of vendor lock-in, it is encouraging to note that respondents expressed by a substantial majority are slightly (39.4 %), moderately (33.7 %), and quite likely (22.1 %) to use a cloud computing risk management framework to manage vendor lock-in risks and compliance requirements effectively. Furthermore, this indicates that UK businesses require effective and efficient strategies to manage lock-in risk(s) prevailing in the cloud ecosystem.

UK organisations view on cloud lock-in

Business strategies for avoiding vendor lock-in

This section summarises both the desires and experiences of the participants who contributed to this study. Moreover, this section presents strategic approaches for mitigating the risks and challenges of lock-in in cloud migration.

Awareness of the commonalities among cloud providers

To refer back to the first research question of interest to business adopters stated in section 1.1. UK business decision makers are rightly concerned about the risks of being locked into a single cloud service provider and the implications of such a risk including not having a clear exit strategy. There is a need for these organisations to understand what the exit strategy looks like, even if it is unlikely that they will exit in the near future – besides, no company would want to buy into a service where they feel they had no alternative provider. In this

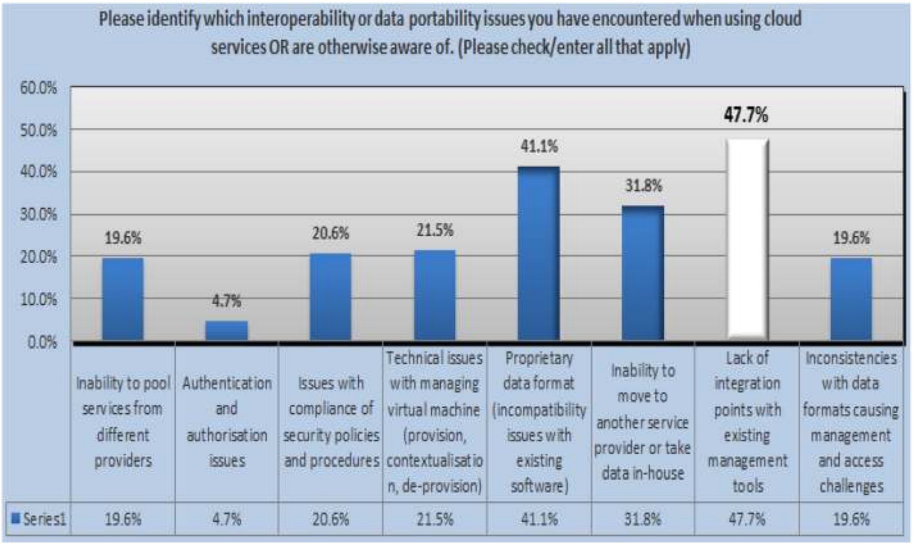


Fig. 10 Practical challenges of vendor lock-in in cloud migration

connection, one possible strategy will require decision-makers to possess a comprehensive understanding of the heterogeneity that exist between cloud semantics and the cloud interfaces. This often requires an awareness of the commonalities (i.e. complexities and dependencies) among services offered by cloud providers and standards used. By clearly understanding this, organisations will realise how the cloud's loose structure can affect data/ application movability and security of data sent in it. This can be done by having an in-depth understanding of how data and application components are handled and transmitted in the cloud environment. When this is well understood and harnessed (at pre contractual phase), the benefits to the organisations become apparent (at post migration phase). Additionally, enterprises can be more interoperable and avoid vendor lock-in strategically by selecting vendors, platforms, or services that support more standards and protocols (as further discussed below in Section 4.1.3). This is essentially important in the vendor selection process as it enables organisations to maintain a favourable mix of cloud providers and internal support. These strategies can help

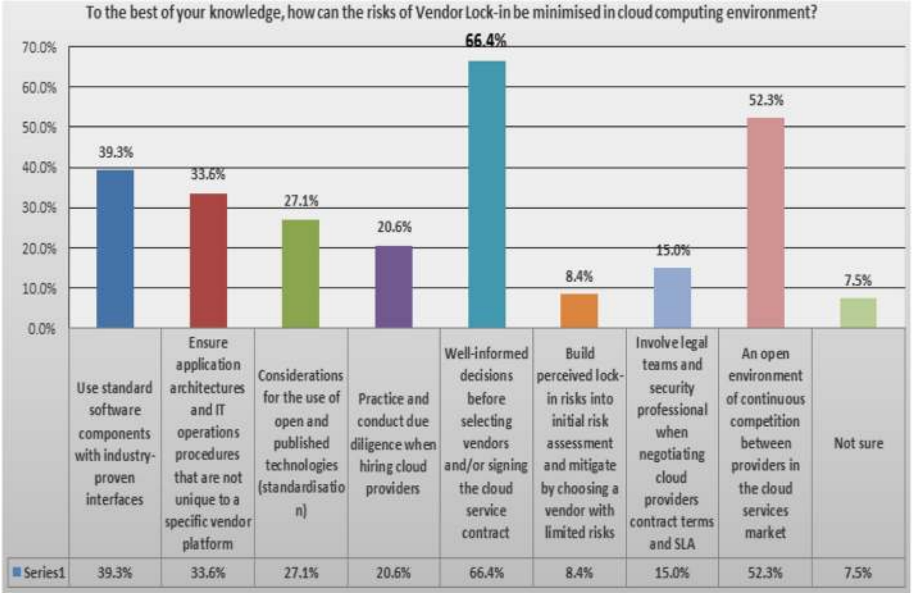


Fig. 11 Current best practice for mitigating cloud lock-in risks

organisations to form a plan for an efficient and effective migration and adoption process. Actually, having a clear understanding of the disparity between cloud semantics and service interfaces offered by different cloud vendors can help significantly to reduce the effects of vendor lock-in.

Substantial training and stakeholder engagement is necessary to develop an understanding and agree solutions on specific lock-in concerns [43–45]. Otherwise, cloud services offered to enterprises may not be properly assessed for potential lock-in risks before decisions are made to use the service [46]. Moreover, the results in Fig. 6 indicate a general lack of understanding and awareness of lock-in problem in the cloud. The low response gained from participants who identified over dependence on a single cloud provider (35.1 %) and difficulty to move data back in-house or across to a different cloud provider (28.8 %) platform illustrates the unawareness of practitioners on the potential effect of cloud lock-in problem. To infer from this result, it appears the risk of dependency is a more significant barrier than data lock-in. This seems counter intuitive considering the practical challenges associated with the data lock-in when extending the use of cloud in the enterprise. However, the probable explanation is that presently most organisations are too reliant on cloud providers for operational and technical support [47], thus they fail to fully prepare to deal with unexpected and undesirable data lock-in issues in the cloud (referring to Fig. 10). As pointed out by Bradshaw et al. [28], lock-in will become more of an issue as the cloud computing market matures. In agreement, Lipton in [48] admits that the complexity and cost of switching (or porting) a cloud service to a different provider is often under-appreciated until it is too late. Therefore it can be claimed that as long as corporate data is not locked-in moving to another cloud provider is just a matter of enduring a switching cost. Such cost can be reduced by employing best practices such as choosing cloud providers that support: (i) the use of standardised APIs wherever possible; (ii) wide range of programming languages, application runtimes and middleware; (iii) as well as ways to archive and deploy libraries of virtual machine images and preconfigured appliances. Overall, these findings suggest respondents do not currently have sufficient understanding on possible technical and non-technical issues of lock-in that can occur in the cloud environment. Thus, it is recommended that organisations remain meticulous when making decisions towards the selection of vendors, taking into consideration potential difficulties associated with switching vendors. However, it is probable for organisations to suffer financial loss if they did not make a strategically correct vendor selection decision from the very onset.

Well-informed decision making

The study has found that for UK organisations, when it comes to evaluating the business risks of vendor lock-in for or against cloud migration, surprisingly, a vast majority (66.4 %) of respondents said making well-informed decisions before selecting vendors and/or signing the cloud service contract is an extremely important part of the decision-making process (refer to Fig. 11). This signifies that as cloud computing becomes more widely used for various applications across different industry sector[s] and size[s], UK businesses are finding it extremely important to understand ways to maximize benefits and minimize the risks of lock-in. In essence, this is particularly important given the plethora of vendors in the market place today, with each offering businesses proprietary cloud-based services and contracts that have different specification (and legal agreements). In regard to the interpretation of this finding, our study suggests that the vetting process for selecting vendors is a critical aspect for effective cloud migration with minimized risk of lock-in. Moreover, such finding exemplify the need for organisations to look beyond the vendor selection phase, and focus on constantly monitoring any development or changes in the cloud that may impact data security or hinder interoperability and portability – thus facilitating a lock-in situation. However, the findings (in Fig. 11) also reveal a gap in understanding, regarding how organisations should manage the risks of vendor lock-in. A sign of lack of understanding is explained by a smaller percentage (8.4 %) of participants identifying the need to build perceived lock-in risks into initial risk assessment. This is quite enlightening, in spite of the relevance of this strategy in the vendor selection phase. Possible interpretation of these may be attributed to the general lack of understanding and experience (on the part of IT and business managers) in respect of technical aspects of complex distributed cloud-based solutions.

Standards and cloud-based solutions

The impact caused by vendor lock-in problem due to lack of standards is what enterprises should be wary about when considering migration to cloud computing [29]. Despite the number of studies in recent years underlining the high relevance of standards in cloud computing, unfortunately this study reveals that most UK organisations still lack a comprehensive understanding on the importance of standards in minimising lock-in risks. In fact, as pointed out by [49], there are two ways a business can achieve the full potential of cloud computing (i) either by changing providers according to their needs (ii) prioritising or simply combining different solutions to get the best of the breed services. However, this will require standards and interoperability to be supported by all providers, but it is often not the case. An informative example in this context is seen in research in [50], arguing that many cloud providers are concerned with the loss of customer that may come with standardisation initiatives which may flatten profits, and do not regard the solution favourable. Based on our research findings, from a business perspective, we suggest the following as key measures to improve customer retention and engender trust in enterprise cloud migration: 1) the quality of service (QoS) guarantee, 2) data protection and metadata ownership, 3) contract termination, as well as 4) data export functionality. Furthermore, as discussed in our previous study [4], in the absence of standardisation, UK businesses willing to outsource and combine a range of services from different cloud providers to achieve maximum efficiency, irrefutably, will experience difficulty when trying to get their in-house systems to interact with the cloud. Likewise, the lack of standardisation also brings disadvantages, when migration, integration or exchange of computer resources is required. This is consistent with the research findings presented in this paper (see Fig. 10). Unsurprisingly these issues were identified from a business perspective, considering the important role of standards in at least mitigating such concerns. Hence, business stakeholders' should be aware that decisions to adopt or move resources to the cloud require adequate risk analysis for potential lock-in. Based on this analysis and the evidence in Fig. 10, we believe there are opportunities that exist for the regulatory and standard bodies to take the necessary action. One potential solution would be to standardise the APIs in such a way that businesses (or SaaS developers for example) could deploy services and data across multiple cloud providers. Thus, the failure of a single cloud provider/vendor would not take all copies of corporate data with it.

Standard initiatives Cloud-specific standards are regularly proposed as a way to mitigate vendor lock-in and achieve portability and interoperability [50]. It is expressed in [51] that many providers are concerned with customer churn rate that may come with standardisation. But according to [52], unless there is a well-accepted and widely used standard, it remains a questionable solution. Therefore as a partially adopted standard would represent a poor solution [53], many cloud vendors now support the creation and adoption of new standards by proposing them to standardisation groups. Clear examples of such cloud-specific standards are OASIS CAMP [54] for PaaS and TOSCA [55] for IaaS. Both specifications aim at enhancing the portability and interoperability of applications across different clouds. We review the two OASIS cloud-specific standards (TOSCA and CAMP) and their potential for dealing with the lock-in problem.

TOSCA The Topology and Orchestration Specification for Cloud Applications (TOSCA) [55], is an emerging standard that enhances service and application portability in a vendor-neutral ecosystem. TOSCA specification describes a meta-model for defining IT services. This metamodels defines both the structure of a service (topology model of a service) and its operational aspects (such as how to deploy, terminate, and manage this service). Service templates are interpreted by a TOSCA-compliant environment (e.g. OpenTOSCA [56]), which operates the cloud services and manages their instances [54].

Managing cloud services requires extensive, mostly manual effort by the customers. Further, important cloud properties (such as self-service and rapid elasticity) can only be realised if service management is automated. In this aspect, TOSCA allows application developers and operators (DevOps) to model management best practices and reoccurring tasks explicitly into so-called plans (i.e. Workflows). TOSCA plans use existing workflow languages such as Business Process Model and Notation (BPMN) [57, 58] or the Business Process Execution Language (BPEL) [59]. To increase portability, TOSCA allows service creators to gather into plans those activities necessary to deploy, manage, and terminate the described cloud service. TOSCA also enables a cloud service creator to provide the same plan or implementation artefact in different languages (e.g. a plan can include the same functionality twice – in BPEL and BPMN). An application ported to the cloud using TOSCA can be composed of services provided by different cloud providers and a user can decide to a specific service with a similar one from a different vendor.

CAMP Cloud Application Management for Platforms (CAMP) is an Oasis cloud-specific standard designed to ease the management of applications across platforms offered as a service (PaaS) [54]. The CAMP standard defines a self-service management API that a PaaS offering presents to the consumer of the platform. The specified CAMP API provides a resource model to describe the main components of any platform offer. For instance, independent software vendors can exploit this interface to create tools and services that communicate with any CAMP-compliant cloud platform via the defined interfaces. Likewise, cloud vendors can also leverage these interfaces to develop new PaaS offerings, or adapt the existing ones, which would be compliant with independent tools. Thus, cloud users save time when deploying applications across multiple cloud platforms.

At present, the effort of deploying applications with vendor-specific tools across multiple PaaS cloud platforms is a non-trivial task. Developers and system operators often face the barrier of redeploying applications to other providers' platform because tools are incompatible. However, this can be simplified using the CAMP interface common to both source and target platforms. To simplify the deployment efforts and support migration across multiple cloud platforms, CAMP defines the Platform Deployment Package (PDP). A PDP is an archive containing a plan file together with application content files such as web archives, database schemas, scripts, source code, localization bundles, icons etc. This archive can be used to move an application and its components from platform to platform, or between a development environment and an operative target platform.

Portable hybrid IT environment

To infer from discussion in the preceding section, the vendor lock-in risk is a valid concern for organisations migrating to the cloud. Considering that lock-in is undesirable, and cannot be eradicated, then how can businesses mitigate its associated risks when migrating to the cloud? From a portability perspective, it becomes critical that organisations' data is sharable between providers, since without the ability to port data or application, it would become simply impossible to switch cloud service providers at all [60, 61]. Cloud portability is a salient consideration to enable organisations migrate a cloud-deployed asset to a different provider and it is a direct benefit of overcoming vendor lock-in [62]. Generally, reconfiguration of systems and applications to achieve interoperability is time/resource consuming and may require a considerable amount of expertise, which could be challenging for some organisations. Therefore, from a business perspective, portability should be seen as a key aspect to consider when selecting cloud providers as it can both help mitigate lock-in risks, and deliver business benefits. This means allowing applications, systems and data components to continue to work correctly when moved between cloud providers' (hardware and/or software) environments [35]. Indeed, the need for organisations to easily switch cloud providers with their data alongside have been a consistent theme throughout the discussion presented hitherto.

To expatiate on the question stated above, it is helpful to view the situation from a business perspective after deploying a SaaS cloud service such as CRM (which according to Fig. 7, 52 % of organisations have already adopted the cloud model). Suppose these organisations use the SaaS CRM and over time, perhaps, the terms of use or the price of the cloud-based CRM service become less attractive, compared to other SaaS providers or with the use of an in-house CRM solution. If the organisation decides to change providers for whatever reason, data portability aspects must be considered. For SaaS cloud services, data formats and contents are handled by the service provider thereby making data portability a major consideration. The issue of importance in a SaaS-level migration is the compatibility of the functional interface presented to end-users and any API made available to other customer applications. In order to alleviate this problem, the APIs made available by the SaaS service should be interoperable with the interface provided by the on-premise application or data that is being replaced. On the other hand, the data handled by one vendor's software should be importable by the second vendor's software, which implies both applications have to support the common format. Standard APIs for various application types will also be required. If the APIs are not interoperable, any customer application or data using the APIs will need to be changed as part of the migration process.

Data portability is usually of most concern in a SaaS, since in these services, the content, data schemas and storage format are under the control of the cloud service provider. The customer will need to understand how the data can be imported into the service and exported from the service. Further, SaaS applications also present interoperability barriers. The lack of adoption of standard APIs for SaaS applications makes switching from one SaaS application to another difficult as it involves a change in the interface. This also applies to any application or system belonging to the cloud service customers that use APIs offered by the SaaS application. Data synchronization is another concern, encountered in cloud interoperability and not in data portability [63]. To further substantiate this argument, we elucidate on the need for a portable hybrid environment by highlighting two main categories of portability scenarios encountered in current cloud service market: 1) porting legacy applications or data; and 2) porting cloud native applications or data. In scenario 1, due to dependence on particular technologies and data organisation, the legacy software assets currently require a significant amount of effort to be invested in porting them into the cloud environment. Whereas in scenario 2, even when applications and data are written from scratch for a cloud environment, they are usually locked and targeted for a specific cloud [63]. Thus, the effort of porting in a different cloud is usually a onetime exercise [63]. However, in both scenarios, the main problem is that there must be a capability to retrieve customer data from the source cloud service and also a capability to import customer data into the target cloud service. Thus, data portability is based on import and export functionality from cloud data services for data structures. This is commonly done through the existence of some API (or web interface) associated with the cloud service – it may be a generic API or a specific API, unique to the cloud service.

In light of such challenges, [64] claims that ensuring data portability is a major challenge for enterprises due to the large number of competing vendors for data storage and retrieval. The ability to move data also emerges as a management issue for cloud computing. Therefore, in response to the question of data movability, it is important to note that the API used for the source service may not be the same as the API used for the target service and that different tooling may be required in each case. The main aspects of data portability are the syntax and semantics of the transferred data. The syntax of the data should ideally be the same for the source service and the target service. However, if the syntax does not match (i.e., the source may use JSON syntax, but the target may use XML), it may be possible to map the data using commonly available tools. If the semantics of the transferred data does not match between the source and target services, then data portability is likely to be more difficult or even impossible. However, this might be achieved by the source service supplying the data in exactly the format that is accepted by the target service. Therefore, on a long term, achieving data portability will depend on the standardization of import and export functionality of data and its adoption by the providers. The aim is to minimize the human efforts in re-design and re-deployment of application and data when moving from one cloud to another. To this end, it becomes vital that any enterprise cloud migration project can be carried out without any disruption to data availability since data is an organisation's most critical, ubiquitous, and essential business asset [29].

Observations

This paper confirms that UK organisations are increasingly adopting cloud services, and it also reveals that they have been progressively migrating services perceived as non-mission critical (i.e. where lock-in and security risks seem lower) such as general purpose applications suites, email and massaging applications. This strategy used allows the organisations to get a feel for how the cloud environment works before fully committing themselves. However, this is generally not the case for organisations surveyed. A lesser minority (see Fig. 7) seem to have adopted core systems in the cloud (e.g. ERP and CRM), including accounting and finance applications. At present, as indicated by the Cloud Industry Forum [39], cloud providers or vendors are better placed, if they ensure such capabilities like the trial or "test and see" strategy (whether completely free or paid for time limited pilot) is made available within their go-to-market strategy. It is worth underlining that, free of charge or low cost does not necessary mean free of lock-in risks or low proprietary lock-in risk. Organisations must be cautious of potential areas of lock-in traps and take adequate measures to mitigate their exposure; e.g. choice of operating environment, programming models, API stack, data portability etc. Further, businesses should take heed of other legal, regulatory, or reputational risks that may exist. This is vitally important if the data involved is not just for testing, but constitutes real corporate data, perhaps even confidential or personal data. It is interesting to note that 28 % of organisations surveyed have already adopted the cloud model for hosting accounting and finance applications (refer to Fig. 7).

On a conclusive note, it is believed that the discussions presented herein, above all, indicate hypothetically that vendor lock-in risks will reduce cloud migration, which in turn affects the widespread adoption of cloud computing across organisations (small or large). Thus an emerging research agenda arises as to investigate: 1) ways to come up with multijurisdictional laws to support interoperability and portability of data across cloud providers platform, along with effective data privacy and security policies; and 2) novel ideas of avoiding vendor dependency on the infrastructure layer, platform, and through to the application layer as lock- cannot be completely eliminated, but can be mitigated. However, these require, not just tools and processes, but also strategic approaches – attitude, confidence, comfort, and enhanced knowledge of how complex distributed cloud-based services work. Sometimes the inhibitor to cloud adoption and migration in most organisations, in principle, are the attitude, knowledge, and confidence of the paramount decision makers. Thus, for most organisations today, the challenge is clear that they simply do not understand potential effect of lock-in to the business. While the business benefits of cloud computing are compelling, organisations must realise that achieving these benefits are consistent with ensuring the risks of vendor lock-in and security implication of such risk is clearly understood upfront. When identified, such risks should be mitigated with appropriate business continuity plans or vendor selection, prior to migration to the cloud.

Potential of DevOps tools for avoiding vendor lock-in

Issues with cloud lock-in surpass those of technical incompatibility and data integration. Mitigating cloud lock-in risks cannot be guaranteed with a selection of individual open (technology-centric) solutions or vendors. Instead, the management and operation of cloud services to avoid lock-in should be addressed at a standardised technology-independent manner. In this respect, we present a concise discussion on the potential of DevOps [65] and of tools (such as Chef, Juju and Puppet) that support interoperable management.

DevOps is an emerging paradigm [66] to eliminate the split and barrier between developers and operations personnel. Automation underlies all the practices that constitute DevOps. The philosophy behind DevOps is to bring agile methodologies into IT infrastructure and service management [65]. This is achieved by implementing the concept of "Infrastructure as Code" (IaC) using configuration management tooling. An automation platform is what provides the ability to describe an infrastructure as code. IaC automations are designed to be repeatable, making the system converge to a desired state starting from arbitrary states [67, 68]. In practice, this is often centred on the release management process (i.e., the managed delivery of code into production), as this can be a source of conflict between these two groups often due to different objectives [68]. DevOps approaches can be combined with cloud computing to enable on-demand provisioning of underlying resources (such as virtual servers, database, application middleware and storage) in a self-service manner. These resources can be configured and managed using DevOps tools and artifacts. As a result, end-to-end deployment automation is effectively enabled by using the DevOps approaches in cloud computing environments [69]. Tools are emerging that address building out a consistent application or service model to reduce the proprietary lock-in risks stemming from customized scripting while improving deployment success due to more-predictable configurations. Today, several applications provisioning solution exists that enable developers and administrators to declaratively specify deployment artefacts and dependencies to allow for repeatable and managed resource provisioning [56]. Below, we review some DevOps tools among the currently available ones that may help enterprises simplify their application release circle.

Chef Chef is a configuration management framework written in Ruby [70]. Chef uses an internal Domain Specific Language or DSL to express configurations. Configuration definitions (i.e. ruby-scripts) and supporting resources (e.g. installation files) in Chef are called recipes. These recipes are basically scripts written in DSL to express the target state of a system [71]. Chef manages so called nodes. A node is an element of enterprise infrastructure, such as a server which can be physical, virtual, in the cloud, or even a container instance running a Chef client [72]. Chef provides APIs to manage resources on a machine in a declarative fashion. Chef recipes are typically declarative (resources which define a desired state) but can include imperative statements as well. Combining a Chef system together with cloud infrastructure automation framework makes it easy to deploy servers and applications to any physical, virtual, or cloud location. Using Chef, an organization can configure IT from the operating system up; applying system updates, modifying configuration files, restarting any necessary system services, applying and configuring middleware and applications.

Puppet Puppet is an open source configuration and management tool implemented in Ruby [47] that allows expressing in a custom declarative language using a model-based approach [73]. Puppet enables deploying infrastructure changes to multiple nodes simultaneously. It functions the same way as a deployment manager, but instead of deploying applications, it deploys infrastructure changes. Puppet employs a declarative model with explicit dependency management. One of the key features of Puppet is reusability. Modules can then be reused on different machines with different operating systems. Moreover, modules can be combined into configuration stacks.

Juju Juju is a cloud configuration, deployment and monitoring environment that deploy services across multiple cloud or physical servers and orchestrate those services [74]. Activities within a service deployed by Juju are orchestrated by a Juju charm, which is a deployable service or application component [75].

In summary, as applications evolve to function in the cloud, organizations must reconsider how they develop, deploy, and manage them. While cloud computing is heavily used to provide the underlying resource, our review shows that DevOps tools and artefacts can be used to configure and manage these resources. As a result, end-to-end deployment automation is efficiently enabled by employing DevOps approaches in cloud environments. But, cloud providers such as Amazon and cloud frameworks such as OpenStack provide cost-effective and fast ways to deploy and run applications. However, there is a large variety of deployment tools and techniques available [76]. They differ in various dimensions, most importantly in the metamodels behind the different approaches. Some use application stacks (e.g., AWS OpsWorks2 or Ubuntu Juju) or infrastructure, others use lists of scripts (e.g., Chef run) or even PaaS-centric application package descriptions such as Cloud Foundry manifests. This makes it challenging to combine different approaches and especially to orchestrate artefacts published by communities affiliated with the different tools, techniques, and providers. Nevertheless, these solutions are highly desirable because some communities share a lot of reusable artefacts such as portable scripts or container images as open-source software [77]. Prominent examples are Chef Cookbooks, Puppet modules, Juju charms, or Docker images. Adopting a configuration management tool implies a significant investment in time and/or money [78]. Nevertheless, before making such an investment, an informed choice based on objective criteria is the best insurance that an enterprise has picked the right tool for its environment, as the focus is on deploying predefined application stacks across several (virtual or physical) machines.

Discussion and conclusion

In this paper a comprehensive analysis of vendor lock-in problems was discussed and the impact to companies as a result of migration to cloud computing was explored. A survey was conducted and revealed that the cloud paradigm has greatly impacted on many organisations subsequent to migrating IT and business applications to the cloud due to vendor lock-in. In fact, the study has shown that, while organisations are eager to adopt cloud computing due to its benefits, there is equally an urgent need for avoiding vendor lock-in risks. Moreover, the results of our study have highlighted customers' lack of awareness of proprietary standards which prohibit interoperability and portability when procuring services from vendors. The complexity and cost of switching providers is often under-appreciated until implementation. Business decision makers are often unaware of how to tackle this issue. Our findings offer cloud computing consumers, service providers, and industry practitioners a better understanding of the risk of lock-in embedded in the complex, technologically interdependent and heterogeneous cloud systems. In this respect, our research points to the need for more sophisticated policy approaches that take a system-wide perspective to alleviate the current vendor lock-in problem which affects interoperability and portability. Furthermore, our findings show that within many organisations in the study, a lack of clarity on the problem space of vendor lock-in still pervades. This lack of knowledge poses a significant barrier to obscure the potential effect the vendor lock-in problem could have on enterprise applications migrated to and operating in cloud platforms. Hence, to be protected against such risks when migrating to the cloud environment, companies require standards, portability, and interoperability to be supported by providers. However, this is currently difficult to achieve as explored in this paper. Fundamentally, the difficulty is attributed to the vendors' APIs which control how cloud services are harnessed, as cloud APIs are not yet standardized, making it complex for customers to change providers. Some cloud providers are concerned with the loss of customers that may come with standardisation initiatives which may then flatten their profits and do not regard the solution favourable. Therefore, we propose the following strategic approaches to address the issues: (i) create awareness of the complexities and dependencies that exist among cloud-based solutions; (ii) assess providers' technology implementation such as API and contract for potential areas of lock-in; (iii) select vendors, platforms, or services that support more standardised formats and protocols based on standard data structures; and (iv) ensure there is sufficient portability. In our future work, we will explore interoperability and portability constraints which affect enterprise application migration and adoption of SaaS clouds.

Additional files

Additional file 1: Questionnaire Survey Questions. (PDF 402 kb)

Additional file 2: Survey Data Analysis. (XLS 283 kb)

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

All listed authors made substantive intellectual contributions to the research and manuscript. JOM was responsible for the overall vendor lock-in research including drafting the manuscript, analysis and interpretation of study results. RS, FT and JOM contributed to the design of methodology used. RS and FT participated in the critical and technical revisions of the paper including editing the final version, also helping with the details for preparing the paper to be published. RS and FT coordinated and supervised the project related to the paper and also gave final approval of the version to be published. All authors read and approved final manuscript.

Authors' information

Justice Opara-Martins is a PhD candidate at Bournemouth University where he graduated with an MSc in Wireless and Mobile Networks. He holds a BSc (Hons.) in Information and Communication Technology. He is a member of the British Computer Society (BCS), IBM Academic Initiative and Association for Project Managers (APM). His research interests include cloud computing, virtualization and distributed systems.

Reza Sahandi completed his PhD at Bradford University in the United Kingdom in 1978. He has been a senior academic at various Universities in the United Kingdom for many years. He is currently Associate Dean at Bournemouth University. His research areas include multimedia and network systems, wireless remote patient monitoring and cloud computing.

Feng Tian received the PhD degree from Xi'an Jiaotong University, China. Currently he is an Associate Professor Bournemouth University (BU), United Kingdom. He was an Assistant Professor in Nanyang Technological University in Singapore before joining BU in 2009. His current research interests include computer graphics, computer animation, augmented reality, image processing and cloud computing.

Acknowledgements

The research leading to these results is supported by Bournemouth University (DEC) Doctoral Scholarship funding. Additionally, the authors would like to thank the Faculty of Science and Technology for providing additional financial support to enhance the quality of this manuscript.

Received: 6 May 2015 Accepted: 5 April 2016
Published online: 15 April 2016

References

1. Andrikopoulos V, Binz T, Leymann F, Strauch S (2013) How to Adapt Applications for the Cloud Environment: Challenges and Solutions in Migrating Applications to the Cloud. Springer Comput J 95(6):493–535
2. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2009) Above the Clouds: A Berkeley View of Cloud Computing. Commun ACM 53(4):50–58
3. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Futur Gener Comput Syst 25(6):599–616
4. Sahandi R, Alkhalil A, Opara-Martins J (2013) Cloud Computing from SMEs Perspective: A Survey Based Investigation. J Inf Technol Manag Publ Assoc Manag XXIV(1):1–12, ISSN #1042-1319
5. Loutas N, Kamateri E, Bosi F, Tarabanis KA (2011) Cloud Computing Interoperability: The State of Play. In: CloudCom., pp 752–757

6. Toosi AN, Calheiros RN, Buyya R (2013) Interconnected Cloud Computing Environments: Challenges, Taxonomy and Survey. ACM Computing Survey 5:Article A
7. Di Martino, B. Cretella, G. Esposito, A. (2015) 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, pp.538–544, doi: 10.1109/FiCloud.2015.119
8. Di Martino, B. Cretella, G. Esposito, A. Sperandeo, R.G., (2014) Semantic Representation of Cloud Services: A Case Study for Microsoft Windows Azure, in Intelligent Networking and Collaborative Systems (INCoS), 2014 International Conference on, pp.647–652, doi: 10.1109/INCoS.2014.76
9. Satzger B, Hummer W, Inzinger W (2013) Winds of Change: From Vendor Lock-in to the Meta Cloud. IEEE Internet Comput 1:69–73
10. Binz T, Breiter G, Leyman F, Spatzier T (2012) Portable cloud services using tosca. IEEE Internet Comput 3:80–85
11. Petcu D, Macariu G, Panic S, Craciun C (2013) Portable cloud applications-from theory to practice. Futur Gener Comput Syst 29(6):1417–1430, https://doi.org/10.1016/j.future.2012.01.009
12. Ardagna, D., Di Nitto, E., Casale, G., Petcu, D., Mohagheghi, P., Mosser, S., Matthews, P., Gericke, A., Ballagny, C., D'Andria, F. and Nechifor, C.S., (2012) 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 (pp. 50–56). IEEE Press.
13. The OpenGroup Consortium. Available from: http://www.opengroup.org
14. Ferry, N. Hui Song Rossini, A Chauvel, F. Solberg, A. (2014) CloudMF: Applying MDE to Tame the Complexity of Managing Multi-cloud Applications, in Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp.269–277, doi:10.1109/UCC.2014.36
15. Silva, G.C, Louis M. R, and Radu, C. (2013) A Systematic Review of Cloud Lock-in Solutions. Cloud Computing Technology and Science (CloudCom), IEEE 5th International Conference on. Vol. 2. IEEE.
16. Edmonds, A. Metsch, T. Papaspyrou, A. Richardson, A. (2012) Toward an Open Cloud Standard, in Internet Computing, IEEE, vol.16, no.4, pp.15–25 doi: 10.1109/MIC.2012.65
17. Toosi, A. Rodrigo N. C, and Buyya, R. (2014) Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey. 47, 1, Article 7 47 pages. http://dx.doi.org/10.1145/2593512
18. Behrens, P, (2015) The Ordoliberal Concept of 'Abuse' of a Dominant Position and its Impact on Article 102 TFEU. Nihoul/Takahashi, Abuse Regulation in Competition Law, Proceedings of the 10th ASCOLA Conference Tokyo 2015, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2658045
19. Leymann F et al (2011) Moving Applications to the Cloud: An Approach Based on Application Model Enrichment. Int'l J Cooperative Information Systems 20(3):307–356
20. Shan C, Heng C, Xianjun Z (2012) Inter-cloud operations via NGSON. IEEE Commun Mag 50(1):82–89, January
21. Toivonen, M., 2013. Cloud Provider Interoperability and Customer Clock-In. In *Proceedings of the seminar* (No. 58312107, pp. 14–19). Available from: https://helda.helsinki.fi/bitstream/handle/10138/42910/cbse13_proceedings.pdf?sequence=2#page=17
22. Moreno-Vozmediano R, Montero R, Llorente I (2012) Key Challenges in Cloud Computing to Enable the Future Internet of Services, IEEE Internet Computing., 18 May, Available from: http://doi.ieeecomputersociety.org/10.1109/MIC.2012.69
23. Michael A, Armando F, Rean G, Anthony DJ, Randy HK, Andrew K, Gunho L, David AP, Ariel R, Ion S, Matei Z (2010) A view of cloud computing. Commun ACM 53(4):50–58
24. Sitaram D, Manjunath G (2012) Moving To the Cloud: Developing Apps in the New World of Cloud Computing. Elsevier, USA
25. Loutas N, Peristeras V, Bouras T, Kamateri E, Zeginis D, Tarabanis K (2010) Towards a Reference Architecture for Semantically Interoperable Clouds. In: IEEE Second International Conference on Cloud Computing Technology and Science., pp 143–150
26. Rodero-Merino L, Vaquero LM, Gil V, Galán F, Fontán J, Montero RS, Llorente IM (2010) From infrastructure delivery to service management in clouds. Futur Gener Comput Syst 26(8):1226–1240
27. Petcu D, Vasilakos AV (2014) Portability in clouds: approaches and research opportunities. Scalable Comput Practice Experience 15(3):251–270
28. Bradshaw D, Folco G, Cattaneo G, Kolding M, (2012) Quantitative estimates of the demand for cloud computing in Europe and the likely barriers to uptake. IDC Interim Tech. Report. SMART 2011/0045. http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf Accessed 29 Dec 2014
29. Opara-Martins J, Sahandi R, Tian F (2014) Critical review of vendor lock-in and its impact on adoption of cloud computing', International Conference on Information Society (i-Society), pp.92-97, doi: 10.1109/i-Society.2014.7009018
30. Badger L, Grance T, Patt-Corner R, Voas J (2011) Cloud Computing Synopsis and Recommendations [draft] (Special Publication 800-146). National Institute of Standards and Technology. http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf Accessed 24 Jan 2015
31. Ahronovitz M et al. (2010) Cloud Computing Use Cases: Introducing Service Level Agreements. Use Cases Discussion Group, White Paper V4.0. http://www.cloud-council.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf Accessed 8 Feb 2015
32. Liu X, Ye H (2008) A Sustainable Service-Oriented B2C Framework for Small Businesses. In 4th IEEE International Symposium on Service Oriented Systems Engineering (SOSE'08), Taiwan, December.
33. Miranda J, Guillen J, Murillo J (2012) Identifying Adaptation Needs to Avoid the Vendor Lock-in Effect in the Deployment of Cloud ServiceBased Applications (SBAs). WAS4FI I-Mashups September 19 Bertinoro, Italy.
34. Petcu D (2011) Portability and Interoperability between Clouds: Challenges and Case Study. In: Towards a Service-Based Internet, vol 6994. Springer, Berlin Heidelberg, pp 62–74
35. Lewis GA (2013) Role of standards in cloud-computing interoperability. In: 46th Hawaii International Conference on System Sciences (HICSS)., pp 1652–1661
36. Hogan M, Liu F S A, Tong J (2011) NIST Cloud Computing Standards Roadmap. NIST Special Publication 500-291, July. http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Jul5A.pdf Accessed 7 Jan2015
37. NVivo qualitative data analysis software; QSR International Pty Ltd. Version 8, 2008.
38. Survey Monkey, (2014) Online Survey Development Tool. https://www.surveymonkey.com Accessed 17 Sept 2014
39. Alkhalil A, Sahandi R, John D (2013) Migration to Cloud Computing-The Impact on IT Management and Security. In 1st International Workshop on Cloud Computing and Information Security, Atlantis Press.
40. Cloud Industry Forum (2014) The Normalisation of Cloud in a Hybrid IT market – UK Cloud Adoption Snapshot & Trends for 2015. Cloud UK, Paper 14. http://www.aspect.com/globalassets/images/uk-documents/aspect—cif-wp.pdf Accessed 17 Nov 2014
41. KPMG (2013) Breaking through the Cloud Adoption Barriers. Cloud Providers Survey https://www.kpmg.com/LU/en/IssuesAndInsights/Articlespublications/Documents/breaking-through-the-cloud-adoption-barriers.pdf Accessed 24 Nov 2014
42. Dubey A, Wagle D (2007) Delivering software as a service. The McKinsey Quarterly (May), pp. 1–12
43. Premkumar G, Michael P (1995) Adoption of computer aided software engineering (CASE) technology: an innovation adoption perspective. SIGMIS Database 26(2–3):105–124
44. Eder L, Igbaria M (2001) Determinants of intranet diffusion and infusion. Omega 29(3):233–242
45. Daylami N, Ryan T, Olfman L, Shayo C (2005) System sciences. HICSS '05, Proceedings of the 38th Annual Hawaii International Conference, Island of Hawaii, 3-6 January.
46. T. Binz, F. Leymann, and D. Schumm (2012) "CMotion: A Framework for Migration of Applications into and between Clouds," Proc. Int'l Conf. Service-Oriented Computing and Applications, IEEE Press, pp. 1–4.
47. Dutta A, Peng GCA, Choudhary A (2013) Risks in enterprise cloud computing: the perspective of IT experts. J Comput Inf Syst 53(4):39–48
48. Lipton P (2013) Escaping Vendor Lock-in with TOSCA, an Emerging Cloud Standard for Portability, CA Technology Exchange 4, 1
49. Leimbach T, Hallinan D, Bachlechner D, Weber A, Jaglo M, Hennen L, Nielsen R O, Nentwich M, StrauB S, Lynn T, Hunt G (2014) Potential and Impacts of Cloud Computing Services and Social Network Websites. Publication of Science and Technology Options Assessment. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf Accessed 14 Nov 2014
50. Govindarajan A, Lakshmanan L (2010) Overview of Cloud Standards. Springer Computer Communications and Networks Journal, London, pp 77–89
51. Petcu D (2011) Portability and interoperability between clouds: Challenges and case study. In: Towards a Service-Based Internet, vol. 6994 LNCS. Springer Berlin Heidelberg, Poland, pp 62–74

52. Lewis, G (2013) Role of standards in Cloud Computing Interoperability. In: 4th Hawaii International Conference on System Sciences Jan, pp. 1652–1661.
53. Shan, C. Heng, and Z. Xianjun (2012) Inter-cloud operations via NGSON. In: IEEE Communications Magazine, vol. 50, no. 1, pp. 82–89.
54. OASIS Cloud Application Management for Platforms, version 1.0. (2012) Available from: https://www.oasis-open.org/committees/download.php/47278/CAMP-v1.0.pdf
55. OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) Version 1.0, Committee Specification Draft 04 (2012).
56. OpenTOSCA (2015) Available from: http://www.iaas.uni-stuttgart.de/OpenTOSCA
57. Breitenbucher, U., Binz, T., Kèpes, K., Kopp, O., Leymann, F., and Wettinger, J. (2014) Combining Declarative and Imperative Cloud Application Provisioning based on TOSCA. In IC2E. IEEE.
58. Business Process Model and Notation (BPMN) Version 2.0. OMG (2011)
59. OASIS (2007) Web Services Business Process Execution Language (BPEL) Version 2.0
60. Parameswaran AV, Chaddha A (2009) Cloud Interoperablility and Standardization. Infosys, SETLabs Briefings 7(7):19–26
61. Cisco Systems, (2010) Planning the Migration of Enterprise Applications to the Cloud. A Guide to your migration Options and Best Practices, Technical report. http://www.cisco.com/en/US/services/ps2961/ps10364/ps10370/ps11104/Migration_of_Enterprise_Apps_to_Cloud_White_Paper.pdf Accessed 1 Dec 2014
62. Mell P, Grance T (2009) The NIST Definition of Cloud Computing, Technical report
63. Petcu D, Vasilakos AV (2014) Portability in clouds: Approaches and research opportunities. Scalable Comput Pract Exp 15(3):251–270. doi:10.12694/scpe.v15i3.1019
64. Buyya R, Ranjan R, Calheiros RN (2010) InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services, Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2010), Busan, South Korea. Springer, Germany, pp 328–336
65. Humble J. and Farley D. (2010) Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation. Addison-Wesley Professional.
66. Wettinger J, Breitenbücher U, Leymann F (2014) DevOp Slang—bridging the gap between development and operations. In: Villari M, Zimmermann W, Lau KK (eds) Service-Oriented and Cloud Computing. Lecture Notes in Computer Science, vol. 8745. Springer, Berlin Heidelberg, pp 108–122
67. Hummer, W, Rosenberg, F., Oliveira, F and Eilam, T., (2013) Automated testing of chef automation script. In: Proceedings of ACM/IFIP/USENIX 14th International Middleware Conference
68. Nelson-Smith, S. (2011) Test-Driven Infrastructure with Chef. O'Reilly.
69. Wettinger J, Gorlach K, Leymann F (2014) Deployment aggregates—a generic deployment automation approach for applications operated in the cloud. In: IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations (EDOCW)., pp 173–180
70. Nelson-Smith, S. (2011). Test-Driven Infrastructure with Chef. O'Reilly Media, Inc.
71. Sabharwal N, Wadhwa M (2014) Automation through Chef Opscode: A Hands-on Approach to Chef
72. Ruby (2016) Available from: https://www.ruby-lang.org/en/
73. Puppet Labs (2015) Open Source Puppet. Available from https://puppetlabs.com/puppet/puppet-open-source
74. Ubuntu Juju (2015) Available from: https://juju.ubuntu.com
75. Wettinger, J., Breitenbücher, U., Leymann, F (2014) Standards-based Devops automation and integration using tosca. In: Proceedings of the 7th International Conference on Utility and Cloud Computing (UCC 2014), pp. 59–68. IEEE Computer Society
76. Gunther, S., Haupt, M., and Splieth, M. (2010) Utilizing Internal Domain-Specific Languages for Deployment and Maintenance of IT Infrastructures. Technical report, Very Large Business Applications Lab Magdeburg, Fakultat fur Informatik, Otto-von-Guericke-Universitat Magdeburg
77. J. Wettinger, V. Andrikopoulos, S. Strauch, and F. Leymann (2013) "Enabling Dynamic Deployment of Cloud Applications Using a Modular and Extensible PaaS Environment," in Proceedings of IEEE CLOUD. IEEE Computer Society, pp. 478–485.
78. Delaet T, Joosen W, Vanbrabant B (2010) A Survey of System Configuration Tools. In: Proceedings of the 24th Large Installations Systems Administration (LISA) conference

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Immediate publication on acceptance
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com