Critical Review of Vendor Lock-in and its Impact on Adoption of Cloud Computing

Conference Paper · November 2014

DOI: 10.1109/i-Society.2014.7009018

3 authors, including:

Justice Opara-Martins
Bournemouth University
25 PUBLICATIONS **353** CITATIONS

SEE PROFILE

R. Sahandi
Bournemouth University
39 PUBLICATIONS **546** CITATIONS

SEE PROFILE

Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing

Justice Opara-Martins, Reza Sahandi, Feng Tian
Faculty of Sciences and Technology, Bournemouth University
Bournemouth, United Kingdom
{joparamartins, rsahandi, ftian}@bournemouth.ac.uk

Abstract—**Cloud computing offers an innovative business model for organizations to adopt IT services at a reduced cost with increased reliability and scalability. However organizations are slow in adopting the cloud model due to the prevalent vendor lock-in issue and challenges associated with it. While the existing cloud solutions for public and private companies are vendor locked-in by design, their existence is subject to limited possibility to interoperate with other cloud systems. In this paper we have presented a critical review of pertinent business, technical and legal issues associated with vendor lock-in, and how it impacts on the widespread adoption of cloud computing. The paper attempts to reflect on the issues associated with interoperability and portability, but with a focus on vendor lock-in. Moreover, the paper demonstrates the importance of interoperability, portability and standards applicable to cloud computing environments along with highlighting other corporate concerns due to the lock-in problem. The outcome of this paper provides a foundation for future analysis and review regarding the impact of vendor neutrality for corporate cloud computing application and services.**

Keywords-cloud computing; vendor lock-in; enterprise migration; data; API's; interoperability; portability; standards;

I. INTRODUCTION

The introduction of cloud computing as a new information technology (IT) paradigm, offers unprecedented scalability to an organization's business processes and business operations [1]. The cloud technology allows organizations to expand or reduce their computing facilities very quickly. This concept is attracting public and private companies, as well as small to medium-sized enterprises (SMEs), who consider cloud computing model an opportunistic business strategy to remain competitive and to meet business needs [2] [3] [4]. Larger enterprises are exploiting the benefits of this platform by taking business continuity into account, while SMEs to the contrary are enhancing their ability to meet computing resource demands, while eschewing consequential investment in over provisioned infrastructure, maintenance, training etc. [5]. However as reported by [6], cloud computing is still in its early stage of maturity, thus suffers from lack of standardization. In essence, what actually happens is that most new and existing cloud providers propose their own solution and proprietary interfaces for access to resources and services. This heterogeneity is a crucial problem as it raises barriers to the path of the ubiquitous cloud realization. And the main barrier is vendor lock-in which is unavoidable at this stage [7] [8].

Vendor lock-in problem in cloud computing is characterized by expensive and time-consuming migration of application and data to alternative providers [9]. Cloud software vendors lock in customers in several ways: (1) by designing a system incompatible with software developed by other vendors; (2) by using proprietary standards or closed architectures that lack interoperability with other applications; (3) by licensing the software under exclusive conditions [10]. Vendor lock-in deters organizations adopting cloud technology. It is a challenging issue that requires substantial efforts to overcome the existing barriers it erects for organizations [11].

According to [11], market demand and the ability to attract more customers are creating more pressure on cloud providers to support interoperability – a direct benefit of avoiding vendor lock-in. Previous studies have focused on interoperability issues or concerns of vendor lock-in. Various standardization solutions have been developed for increasing interoperability [7], [8]. However, very little research solely investigated the review of vendor lock-in and its impact on adoption of cloud computing. The contribution of this paper provides a foundation for future analysis and review regarding the impact of vendor lock-in for corporate cloud computing application and services.

The rest of this paper is structured as follow. **Section II** presents related research in this field. **Section III** explores vendor lock-in problem in-depth. **Section IV** discusses major considerations for organizations regarding the impact of vendor lock-in due to lack of standards for cloud application programming interfaces (APIs) and data models, pointing out why this is a major problem for enterprises considering cloud migration. Finally **Section V** concludes this paper by summarizing the findings herein presented respectively, and presents directions for future work.

II. RELATED WORK

Vendor lock-in problem has been identified as one of the most widespread and crosscutting problems related with cloud computing adoption [12]. The risks posed by vendor lock-in can inhibit organizations from switching cloud providers [13, 14]. In [15], Razavian et al. conducted an analysis on how vendor lock-in prevents enterprises from migrating towards cloud storage. The outcome of their study proposed a solution that uses erasure coding as a method of distribution, to

distribute redundant data across multiple cloud providers in order to increase the probability of access to data.

In [16], Bhavya et al discuss challenges concerning vendor lock-in problem in cloud computing and presents new ways of overcoming them. In addition, they addressed user concerns in portability and interoperability in the migration of cloud services providing security. With respect to cloud computing, vendor lock-in is the direct result of the current difference between the individual vendor paradigms based on non-compatible underlying technologies, and implicit lack of interoperability. Avoiding vendor lock-in or minimising its impact is consistent with ensuring interoperability and portability across cloud computing systems and services.

Toivonen in [11], describe interoperability issues that lead to vendor lock-in and present a very brief overview on current standardization efforts to address the problem. Whereas, Pahl et al. in [17] analysed several standards for cloud architecture interoperability, and introduced a number of different concerns that will help to assess the state of standardization and its impact on interoperability.

A vendor locked cloud environment can be encouraged, from a cloud provider perspective, through the implementation of proprietary or non-standard APIs and data storage methods. In fact, in this case the main obstacle to a vendor-neutral environment is the lack of industry standards to support interoperability and portability across multiple cloud providers. In [18], Govindarajan and Lakshmanan investigated solutions covering interoperability, security, portability and governance in cloud. For interoperability, they classified the approaches in three groups: standardization bodies, industry solutions, and brokering and management. However in [19] Panhelainen explored current advancement on standardization, and proposed a migration strategy for portability and interoperability between different cloud platforms. Petcu in [9] identified and classified several issues of cloud portability and interoperability. For each issue identified, Petcu surveyed concepts such as requirements, evolution stages, and types of portability and interoperability.

Cloud computing services have made it easier for organizations to rapidly deploy and de-provision IT applications on-demand as business needs evolve. Thus, it becomes important from a cloud provider perspective to focus on building and retaining consumer trust. According to [20], an effective way to engender consumer trust in cloud adoption and prevent vendor lock-in risks is to make it easy for users to switch cloud providers with their data alongside. Even if organizations have copy of their data with them in tow when switching providers, it can still be locked in if the cloud provider stored data in their own proprietary format. Hence, it becomes important not only to have access to data, but also to have it in a format that has a publicly available specification. Further, giving organizations control over their data and the ability to easily switch cloud providers is an important part of establishing trust and is paramount for creating a vendor-neutral cloud environment.

III. VENDOR LOCK-IN PROBLEM

An IDC executive insight research confirmed, while cloud providers are eager to migrate customers onto their platform and readily provide tools to do so, customers have voiced their concerns about the inconvenience of moving applications and data from one cloud to another [21]. Cloud vendors offer enterprises proprietary cloud-based services that have different specifications from one vendor to another. The main problem is attributed to the fact that currently each provider develops its own specific technology solutions, remote APIs, and some even create new programming languages [9]. As a consequence of this, cloud users become dependent (i.e. locked-in) on a certain vendor's services and are unable to switch to different vendor–due to technical incompatibilities–without undertaking substantial switching costs [12]. To further substantiate a lock-in situation, for instance switching between alternative vendors, of essentially the same product, without paying substantial switching cost is not possible as argued by [22]. In other words, the substantial cost associated with switching between incompatible software systems can force a customer to use the same products and services [ibid]. And often this means that these customers will also be reluctant to switch to incompatible vendors. This reluctance has two important consequences as pointed out by [23]. First, it potentially provides incumbent suppliers with market power. Second, it may influence consumer and provider choices among alternative technologies for a product.

In [24], Sheth and Ranabahu claim that, existing cloud computing solutions for enterprises have not been built with interoperability and portability in mind–hence; applications are usually restricted to a particular enterprises cloud or a cloud service provider. In reality, this claim is somewhat correct because existing cloud solutions are tightly coupled to the proprietary technology they were designed for, consequently, locking customers into a single cloud infrastructure, platform, or service preventing interoperability and portability of data or software created by them [12]. Therefore on this note it is worth underlining that, selecting a cloud platform that is built on proprietary formats means that businesses can face a lock-in situation which will make it more difficult for them if they change service provider at some point in the future; either because they want to bring processes back into their premises or maybe they want to select another service provider. Quite clearly, this may constrain the cloud ecosystem growth by limiting cloud service choice, because business applications and data will remain locked in cloud silos. Issues associated with vendor lock-in have been identified and discussed below.

A. Lack of Interoperability Makes it Difficult to Consolidate Enterprise IT Systems in the Cloud

Enabling cloud infrastructure to evolve into a transparent platform while preserving integrity raises interoperability issues [2]. Interoperability of information between multiple clouds is a critical enabler for broad adoption of cloud computing by enterprises [25]. Interoperability in cloud computing has many definitions from different points of view, and is often misused to include the term portability, as evident in [9]. To clearly enunciate for the sake of clarity, we employ the distinction made by the National Institute for Standards and

Technology (NIST) between interoperability and portability by defining interoperability as, "the ability of cloud computing services, from different providers, and other applications or platforms that are not cloud dependent to seamlessly exchange assets [24]." In a cloud environment, consumers favor greater interoperability as it allows them to customize their own solutions by purchasing "best of breed" services from multiple cloud providers and to move easily between providers. Governments, on the other hand, also favor interoperability as a way of driving competition and increasing resilience of the cloud system as a whole, especially where the market consists of only a few providers [26]. Further, another interoperability advantage for consumers (besides avoiding vendor lock-in risks) is that they would be able to compare and choose between providers. Also the use of multiple clouds or hybrid clouds becomes possible when interoperability is supported.

However, interoperability concerns arise in different situations. For example, interoperability between cloud layers needs standardized APIs to allow higher cloud layers to link, exchange and interact to a range of services provided at the lower layers e.g. platform implementations to uniformly link to Infrastructure-as-a-Service (IaaS) offerings. Although it is worth underlining that various cloud service models might have different requirements regarding interoperability. Therefore, fostering cloud interoperability is multi-faceted and is likely to extend to a broad range of ecosystem players, including providers of connectivity and application developers. To this end, we suggest standards bodies, industry players, academia, practitioners etc. should pursue the evolution of cloud offerings with the goal of facilitating interoperability among multiple clouds. In fact, this will undeniably accelerate the maturity and growth of the overall cloud ecosystem.

B. Lack of Portability Hinders Enterprises from Migrating

Portability defines the ease of ability to which application components are moved and reused elsewhere regardless of provider, platform, operating system, infrastructure, location, storage, data format, or API's. Cloud portability is defined as the ability to migrate a cloud-deployed asset to a different provider [27], and it is a direct benefit of overcoming vendor lock-in. Petcu in [9] identified the following as the main kinds of cloud computing portability to consider; data portability, application portability, and platform portability. Whereas in [28], they distinguish the different levels of portability within the cloud service models: IaaS portability involves the migration of virtual machines, whereas Platform-as-a-Service (PaaS) portability is the migration of code and data. While SaaS portability is the migration of data and content [29]. Data being an organization's most critical, ubiquitous and essential business asset, it is vital that any enterprise data migration be carried out without any disruption to data availability. Considering the different attributes of each cloud service model, the idea of data portability will depend on the model adopted. For this reason, organizations are interested to know whether they can move their data and applications across multiple cloud environments at low and minimal costs.

Portability is the key aspect to consider when selecting cloud providers as it can both help prevent vendor lock-in, and deliver business benefits. This means allowing identical cloud deployments to occur in different cloud provider solutions [30]. Portability in cloud computing is a desirable expectation by organizations as they mitigate cloud outages and supports pursuing new business opportunities (e.g. better price, better service quality etc.). [31] believe that the first and foremost step required to ensure cloud service portability is the standardization of the data formats used by service providers. In contrast, industry stakeholders are concerned that an excessive focus on ensuring portability in cloud computing will limit the incentive to innovate by making it harder to differentiate between different architectures and offerings [26]. While on the other, organizations wish to have the capability to move applications across platforms and data across applications, but they are hindered due to the disparity in cloud APIs provided by different vendors. Nevertheless, organizations planning to adopt cloud computing services must realize that moving business IT applications and (sensitive) data beyond the corporate firewall into the cloud environment is a form of outsourcing. And the golden rule of outsourcing is to understand up-front and plan for how to exit the contract. In this case, portability should therefore be a key criterion of any organizations strategy to move into cloud services, allowing for a viable exit strategy to be developed.

C. Lack of Standards Creates Barriers to Cloud Entry

Standards are necessary to consolidate efforts in a technology domain and to enable interoperability and portability. The fields of standardization can be security, interoperability and portability, but the latter two are in the focus despite the importance of security. Standards are regularly proposed as a way to mitigate vendor lock-in. However in [18], they argue that many cloud providers are concerned with the loss of customers that may come with standardization initiatives and do not regard this solution favorable. In agreement with [32], we suggest that standards shared among cloud providers do not need to be identical (i.e. in terms of differentiation advantage), although the greater the uniformity between them, the easier it will be to evaluate potential liabilities in choosing among the services offered by different providers. Moreover, any inconsistency could hinder a user's ability to move data or applications between providers, and might also limit an organization's ability to draw on the resources of multiple providers.

Standardization strives to support applications by different service vendors to interoperate with one another, exchange traffic, and cooperatively interact with data as well as protocols for joint coordination and control [33]. According to [34], cloud users would particularly welcome standards that address workload migration and data migration use cases because such standards would mitigate vendor lock-in concerns. This requires virtual-machine (VM) image file formats and APIs for cloud storage [35]. In the absence of standards for cloud APIs and data models, companies willing to outsource and combine range of services from different cloud providers to achieve maximum efficiency will experience difficulty when trying to get their in- house (legacy) systems to interact with the cloud providers system. Likewise, the lack of standardization may also bring disadvantages, when migration, integration, or exchange of resources is required. The main negative aspect in

this case would be the necessity of factoring applications to comply with other cloud APIs, which can possibly lead to higher costs, project delays, and other related risks. Thus, opposing agility, efficiency, and low cost that often comes with utilizing cloud-based services [36]. The impact caused by lock-in problem due to lack of standards is what enterprises should be wary about when considering migration to cloud computing.

D. Technical Barriers

1) Integration Challenges: According to [37], cloud adoption will be hampered if there is not a good way to integrate data and applications across clouds. In [12] it is argued that the cost and complexity of developing and maintaining integrations between heterogeneous platforms with disparate interfaces and protocols can quickly erase the economic and efficiency gains the cloud delivers. Moreover, a survey by [38] of business managers around the world on their experiences with cloud applications, revealed that companies have abandoned the use of roughly one departmental cloud application a year due to integration problems. It is anticipated that standardization of API's will significantly help to resolve this issue. However, initiatives by multiple standard bodies, forum and consortiums could indirectly lead to the possibility of multiple standards emerging with possible lack of consensus – thereby deteriorating the problem even further. But as advised by [39], it is important for standard bodies, vendors, and users to sit together, discuss and arrive at a consensus on the standards and API's in different areas.

2) Data Portability Issues: Ensuring data portability within the cloud is a major challenge for enterprises due to the large number of competing vendors for data storage and retrieval [40]. Suppose an enterprise uses SaaS product for Customer Relationship Management (CRM), and over time the terms of use of the cloud service become less attractive compared to other SaaS providers or perhaps with the use of an in-house CRM solution. If the business decides to change providers due to unacceptable increase in cost at contract renewal time, breached SLA etc. The key issue of concern for the organizations in this case is basically how easy will it be to move their data to another CRM solution or back in-house? In many cases it will be very difficult because the data structure for cloud computing is not yet standardized. Quite often it is designed to fit a particular form of application processing logic, thus a significant amount of transformation is needed to produce data that can be handled by a different product. In this case, lock-in can be a deliberate strategy as it benefits vendors because it reduces the bargaining power for the enterprise and increases that of the vendors by gaining them a competitive advantage. From a portability perspective it becomes critical that organization data is sharable between providers since without the ability to port data it would become simply impossible to switch cloud service providers at all [38].

IV. Impact of Vendor Lock-in to Enterprise Adoption

From a historical viewpoint, many enterprise organizations fail when it comes to implementing new and transformational technologies. The following were identified as the main causes of failure: lack of understanding and interest in embracing new technologies; early rush into development mode without proper understanding of architecture and design steps; and unrealistic expectations like too-aggressive due dates, too large of a scope and many other reasons [39]. A common misconception about cloud computing is the notion that migrating existing enterprise IT applications to the cloud is a simple solution that reduces cost. But in reality, this is usually the complete opposite. In fact, very few applications are good candidate to move to the cloud in their current architecture. The architecture of an application will affect how an application can be migrated to the cloud environment and sometimes whether it is suitable for migration. Cloud architectures, however, require loosely coupled application architectures – since it allows one to replace components, or change components, without having to make reflective changes to other components in the architecture/systems. This means enterprises can change their business systems as needed, with much more agility than if the architecture/systems were more tightly coupled [40]. Therefore, in agreement with the recommendation by [41], to identify business processes, application and data for operation in the cloud environment, it is mandatory to first develop and understand the technical, business and legal factors that might affect the migration process. Therefore, below we will look at the impact of vendor lock-in on adoption of cloud computing services from a business and legal viewpoint.

A. Business Challenges

From a business perspective many cloud providers seek to make their offerings to consumers as proprietary as possible to facilitate cloud vendor lock-in on the product, as well as at the contract level. There is more than one way to get locked into a cloud vendor's system; an often overlooked method is through a contract. To substantiate further, a joint survey by Cloud Security Alliance (CSA) [31] and Information Systems Audit and Control Association (ISACA) [42] identified exit strategies, contract lock-in and data ownership as core enterprise concerns. While another study conducted by Constellation Research Group found that many cloud contracts come with all the rigour and due diligence of on-premise licensed software. In this connection, according to [32], there are three reasons why consumers face vendor lock-in; have limited rights and controls for users, ambiguous and ultimately expensive switching costs and vendor complacency. Vendors use the key selling point of cloud services (i.e. benefits of moving from capital expenditure to operational expenditure model) to significantly reduce the upfront costs for companies looking to implement new IT services and software. However, to minimise the risk of customer churn eroding their margins, vendors seek to create 'lock-in' through contractual terms, or through the physical holding of the customer's data. In this regard, there is an economic benefit to the vendor in the form of a regular revenue stream, but not so much of a business benefit to the consumers. From a commercial perspective, this puts the vendor in a position of strength when it comes to renegotiating the commercial terms of the agreement. For this reason, it is crucial to carefully review the contract before signing. Considering the negative impact that these issues can have on a business operation, it is worth mentioning that when enterprises opt-in to use any cloud-based solution, the cloud

service should at least provide tools to ensure the consumer can extract, access and interchange data if such a need arises.

B. Legal and Jurisdictional Challenges

A key advantage of utilizing enterprise cloud-based IT solutions from a cloud provider perspective is the flexibility and movement of data between servers that may be located in various parts of the world. Further, data maintained in a cloud environment may contain personal, private or confidential information such as intellectual property (IP) etc. that requires proper safeguards to prevent disclosure, compromise or misuse. An enterprise or SME organization using cloud based IT services is likely to have processing performed in, and data moved between, different jurisdictions. As a result, this may place constraints on the processing that can be performed, on the movement of data, and on the degree of control that the organization has. Furthermore, it is observed that existing laws and governance are insufficient to keep pace with cloud computing service development [42]. Thus, the potential for legal disputes is considerable. In addition, legislative and jurisdictional challenges may also arise due to the possibility of data centers located in areas with different jurisdiction. Bear in mind that many jurisdictions will have specific requirements and regulations regarding the location of data. Therefore such requirements should be carefully considered by enterprises before a decision on adopting the cloud service model is made.

We believe there are opportunities for lawmakers to come up with useful multi-jurisdictional regulations that will help in determining the applicable legislation in cases where data is located in different jurisdictions. Policies need to be crafted around data interoperability related issues to ensure that data interchanged between cloud services is un-hindered, as most enterprise users are likely to use heterogeneous cloud service providers for their business needs. So policy makers will have to focus on data ownership and control issues to ensure that enterprises continue to control the destiny of their data. It is important for cloud providers to put mechanisms in place to ensure that whatever enterprise data they put in the cloud service can be easily and securely taken out, for reasons such as integration with another cloud service, or a move to another cloud service vendor etc.

V. Conclusion and Future Work

In this paper we have presented a critical review and impact of vendor lock-in for enterprise adoption from a technical, business and legal viewpoint. In particular, we have examined key interoperability and portability issues associated with vendor lock-in, and in contrast show how vendors could leverage the lack of standards in cloud computing to exploit customers by making their offerings as proprietary as possible to facilitate lock-in. Interoperability among cloud providers, and portability which facilitates users from migrating their application and data to a different cloud offering, are the possible ways to avoid this lock-in situation and open the way toward a more competitive market for cloud providers and consumers. However, while vendor lock-in cannot be completely eradicated, we believe enterprises can somewhat mitigate its impact – with the right knowledge and research, planning, strategy, technical know-how and vendor selection.

The focus of our ongoing research is to tackle the challenge of vendor lock-in in the context of cloud computing. We would like to investigate novel approaches to avoid vendor dependency, and develop a cloud computing migration framework that addresses the issue of vendor lock-in

References

[1] D. Sitaram, and G. Manjunath, “Moving To the Cloud: Developing Apps in the New World of Cloud Computing” Elsevier, USA 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems, vol. 25, no. 6, pp. 599-616, 2009.

[4] V. Andrikopoulos, T. Binz, F. Leymann and S. Strauch, "How to Adapt Applications for the Cloud Environment: Challenges and Solutions in Migrating Applications to the Cloud," Computing, vol. 95, no. 6, pp. 493-535, 2013.

[5] P. Jamshidi, A. Ahmad, and C. Pahl, “Cloud Migration Research: A Systematic Review” IEEE Transactions on Cloud Computing 2013. Available from: http://doras.dcu.ie/19636/1/TCC-AcceptedVersion.pdf [Accessed on the 5th March 2014].

[6] A. N. Toosi, R. N. Calheiros, and R. Buyya, “Interconnected Cloud Computing Environments: Challenges, Taxonomy and Survey,” ACM Computing. Survey. Vol. 5, Article A, 2013.

[7] X. Liu, and H. Ye, “A Sustainable Service-Oriented B2C Framework for Small Businesses” 4th IEEE International Symposium on Service-Oriented Systems Engineering (SOSE'08), Taiwan, Dec 2008.

[8] D. Petcu. “Portability and Interoperability between Clouds: Challenges and Case Study,” In Towards a Service-Based Internet. Vol. 6994. Springer Berlin Heidelberg, 62–74, 2011.

[9] R. Wang, “Adopting Cloud Computing: Seeing the Forest for the Trees” 2013 [online]. Available from: http://www.forbes.com/sites/oracle/2013/09/20/adopting-cloud-computing-seeing-the-forest-for-the-trees/ [Accessed on 12th February 2014].

[10] J. Miranda, J. Guillen, and J. Murillo, “Identifying Adaptation Needs to Avoid the Vendor Lock-in Effect in the Depolyment of Cloud Service-Based Applications (SBAs)” 2012.

[11] M. Toivonen, "Cloud Provider Interoperability and Customer Lock-in" Dept. of Computer Science, University of Helsinki, Research Paper 2013.

[12] K. Stravoskoufos, A. Preventis, S. Sotiriadis, and E.G.M. Petrakis, "A Survey on Approaches for Interoperability and Portability of Cloud Computing Services" 2013.

[13] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing,” in University of California, Berkeley, Technical Report No. UCB/EECS-2009-28. 2009.

[14] Pearson, S. and A. Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, in IEEE CloudCom, 2010. p. 693-702.

[15] S. M. Razavian, H. Khani, and N. Yazdani, "An Analysis of Vendor Lock-in Problem in Cloud Storage" 3rd International Conference on Computer Knowledge Engineering (ICCKE), 2013.

[16] K. Bhavya, K. Yamini and V. Sreenivas, "Cloud Services Portability for Secure Migration" International Journal of Computer Trends and Technology (IJCTT), Vol 4, Issue 4, 2013.

[17] C. Pahl, L. Zhang, and F. Fowley, "A Look at Cloud Architecture Interoperability through Standards" 2013.

[18] A. Govindarajan, and L. Lakshmanan, "Overview of Cloud Standards in Cloud Computing" London: Springer London, 2010 pp. 77-89.

[19] A. Panhelainen, “Interoperable and Portable Cloud Services” Aalto University School of Chemical Technology, Spring 2012

[20] B. W. Fitzpatrick and JJ. Lueck, “The Case Against Data Lock-in,” ACM Queue, 2010.

[21] J. Bozman, “Cloud Computing: The Need for Portability and Interoperability,” 2010 [online]. Available from: http://delimiter.com.au/wp-content/uploads/2010/10/The-need-for-portability-and-interoperability-IDC.pdf [Accessed on 6th March 2014].

[22] K. X. Zhu and Z. Z. Zhou, "Lock-in Strategy in Software Competition: Open-Source Software vs. Proprietary Software," Information Systems Research, 2011

[23] P. David, and S.M. Greenstein, "The Economics of Compatibility Standards: An Introduction to Recent Research," Economics of Innovation and New Technology, Vol. 1, 1990, pp. 1-29.

[24] A. Sheth and A. Ranabahu, "Semantic Modeling for Cloud Computing, Part I & II," IEEE Internet Computing Magazine, vol. 14, pp. 81-83, 2010.

[25] J. Pooyan, A. Aakash and P. Claus, "Cloud Migrattion Research: A Systematic Review," IEEE Transactions on Cloud Computing, [online] 2013.Available from: http://doras.dcu.ie/19636/

[26] World Economic Forum (WEF), "Advancing Cloud Computing: What to do now?" Priorities for Industry and Governments, WEF in Partnership with Accenture, 2011.

[27] P. Mell, and T. Grance, "The NIST Definition of Cloud Computing." Technical report, 2009.

[28] T. Dillion, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," Advanced Information Networking and Application (AINA), 24th 2014 Conference, pp. 752-757, 2010.

[29] JISC Legal Information, "Report on Cloud Computing and the Law for UK FE and HE (An Overview)," 2011.

[30] G. A. Lewis, "Role of Standards in Cloud-Computing Interoperability," IEEE, 46th Hawaii International Conference on Systsem Sciences, pp. 1652-1661, 2012.

[31] Cloud Security Alliance (CSA), "Security Guidance For Critical Areas of Focus in Cloud Computing," V3.0, 2011.

[32] R. R. Wang, “The Enterprise Cloud Buyer’s Bill of Rights: SaaS Applications,” How to maximize your investment an d avoid potential Vendor lock-in, Best Practices Report, 2012.

[33] Ahronovitz, Miha, et al. for the Cloud Computing Use Cases Discussion Group. Cloud Computing Use Cases White Paper (Version 4.0) [online].

[34] G. S. Machado, D. Hausheer, and B. Stiller,“Considerations on the Interoperability of and between Cloud Computing Standards,” [online]. Available from: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.155.51, 2010 (Accessed on 17th May 2014).

[35] C. S. Yoo, “Cloud Computing: Architectural and Policy Implications," [online]. Available from: http://techpolicyinstitute.org/files/yoo%20architectural_and_policy_implications.pdf, 2010 (Accessed on 27th April 2014).

[36] Cisco, "Planning the Migration of Enterprise Applications to the Cloud," A Guide to your migration Options: Private and Public Clouds, Application Evaluation Criteria, and Application Migration Best Practices, 2010.M. Kavis, “Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS),” John Wiley & Sons, 2014.

[37] R. Buyya, R. Ranjan, and R. N. Calheiros. “InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services.” In Proceedings of the 10th InternationalConference on Algorithms and Architectures for Parallel Processing (ICA3PP ’10), Vol. 6081 Busan, South Korea, 13–31. 2010.

[38] A. V. Parameswaran and A. Chaddha, "Cloud Interoperablility and Standardization," Infosys, 2013.

[39] M. Kavis, “Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS),” John Wiley & Sons, 2014.

[40] D. Linthicum, “The API Is Everything for Cloud Computing.” InfoWorld [online] Available from: http://www.infoworld.com/d/cloud-computing/the-api-everything-cloud-computing-481?source=IFWNLE_nlt_cloud_2010-06-07 (2010). [Accessed on 6th April 2014]

[41] Information Systems Audit and Control Association (ISACA), "Cloud Computing Market Maturity," Study Results, 2012. Available from: https://downloads.cloudsecurityalliance.org/initiatives/collaborate/isaca/2012-Cloud-Computing-Market-Maturity-Study-Results.pdf [Accessed 19th May 2014].

[42] M. G. Avram, “Advantages and challenges of adopting cloud computing from an enterprise perspective,” The 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013).