

# VENDOR LOCK-IN SITUATION IN CLOUD COMPUTING

Naseer Ahmad Shinwari<sup>1</sup>, Nasrullah<sup>2</sup>, Abhishek Saxena<sup>3</sup>, Dr Neeta Sharma<sup>4</sup>  
M.Tech Pursuing<sup>1, 2</sup>, Noida International University, Greater Noida, (U.P.)  
Assistant Professor<sup>3, 4</sup>, Dept of CSE, Noida International University, Greater Noida, (U.P.)

**Abstract:** *Cloud computing is a big technological advancement now days and everyone in the industry are either intentionally or unintentionally using it to some extent. Since Cloud Computing is in its growing phase hence it has some pros and cons, like it is helping the IT departments in efforts deduction and C level managers from paying the upfront cash all at ones, but had certain issues also, like security, privacy and dependency on someone else's services, which might be a big concern for some organizations dealing with critical data. Researchers and industry experts are working a lot on resolving many critical issues of cloud computing, but beside all the other issues one of the major problem that arises with the cloud users is the vendor lock-in problem which should be kept in mind before moving to the cloud.*

*This paper discusses & reviews the concepts of cloud in depth, causes, and some avoidance suggestions of vendor lock-in problem, which if prevented will result in increasing clients and cloud based services, since a huge number of organizations are afraid what-if they are stucked and not satisfied with services of the vendor.*

**Keywords:** Cloud computing, vendor lock-in, distributed servers, cloud service providers, migration, interoperability, meta cloud.

## 1. Introduction

These days, Cloud computing is the most adopting computing paradigm, after all the traditional computing mechanisms, offering resources on “pay-per-use” basis. Since it is in the evolving phase, hence if you ask ten professionals to define cloud computing, you will get ten different definitions. The (NIST) US National Institute of Standards and Technology's [1] definition covers the most important aspects of the cloud:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

This cloud model promotes availability and is composed of five essential characteristics:

- (i) On-demand self-service,
- (ii) Broad network access,
- (iii) Resource pooling,
- (iv) Rapid elasticity,
- (v) Measured Service;

Cloud computing has three service models, Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS) and along with four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud).

Cloud computing is the beginning of new era in the world of computing, which is quite easy to adopt and fair to use because of its “Pay-per-use” nature. By this you only pay for what you use, and hence brings advantages by simply cut off most of the overhead of buying your own servers, configuring them, cooling them, and hiring IT staff, to make sure that your servers are all properly configured and running.

With cloud computing you can get all of the required services without any upfront payment which ensures high availability, performance, on-demand self-service, and most importantly no worries about the servers break down,

hard drive crashes, power supply fails and all other issues which would keep the IT department busy and causes delay in services. By the use of cloud computing it is the sole responsibility of the cloud service provider to make sure you and your clients are getting all the services by providing best performance and high availability.

But with all the best features, cloud tenants/clients have some concerns as well which comprises of security, privacy, service availability, data replication, vendor bankruptcy and vendor lock-in, which are also known as risks or challenges in the cloud.

The recent technical report of European Commission[2] aims to outline that Cloud models & technologies have yet not received their full potential, and many of the capabilities associated with clouds are not yet developed and researched to extent that allows their exploitation to the full degree, respectively meeting all potential circumstances of usage, which gives us the indication that cloud is yet not perfect and researchers and industry experts are trying to make it, as it seems to be the future of computing.

With all other challenges & issues being faced in moving to cloud, the major attention of most of the big organizations, who adopted cloud, is on the vendor lock-in. It was out of the sight at first, but as more and more organizations moved to the cloud they noticed that they are being locked-in at some point. This paper tries to analyze the various issues and aspects of various work related on the vendor lock-in issue.

## 2. Vendor Lock-in

### 2.1. What is vendor lock-in?

Since the inception of Cloud-based Services everything is being done and provided by Vendor. The business organizations who are using cloud based services at some point in time, might want to change their Cloud Service Providers (CSP) and move to a new one. This could be due to any reason, as the CSP can no longer answer the needs of the tenant, or there are changes or updates in the services which are not welcomed by the client as it is unable to suit clients needs, or the CSP raises the price, or some other CSP is providing same or even better services at least price, or there are agreement breakups, or any other cause which makes the client move to a new CSP but they can't come out of this situation, which is known as the vendor lock-in state in terms of cloud computing.

### 2.2. Causes of Vendor lock-in

A client might be locked-in with a vendor for any of the following reasons:

(a) **Cost:** It is the basic concept of the cloud based computing which is meant for "pay for what you use", means that pay for the services which CSP provides, which includes the inbound and outbound bandwidth use for data transmission and storage space your data occupies on the CSP's data centers.

This simple rule can get you locked-in with a vendor, if you have stored huge amount of data on the cloud, and when moving to a new CSP, firstly download all of your data from the previous CSP, for which you will be charged, and then upload all of your data to a the new CPS for which again you will be charged.

Some cloud service providers don't charge their customers for the inbound bandwidth, but might lead to huge data uploads which will lead to lock-in when you are downloading all your data back.

Another issue is the migration cost, which is applied on customers for migrating their data to another CSP which is agreed upon in the agreement. This migrations cost could be a huge amount since they charge with per unit of data, as per GB, which again increases the migration cost relatively if the data is huge in the volume.

Due to such issues, of the data transmission costs plus migration cost, it becomes unbearable for customer and hence remained locked-in with the vendor.

(b) **Time:** It is another important aspect required for switching between CSPs. Nasuni's (2014) [3] data migrations test shows that to transfer 12 TB data from one cloud to another could take from few hours to several days. It is due to the write capability of the cloud, or some CSP may have limitations of bandwidth which slows down the migration process. For real time applications and enterprises it obviously is catastrophic to have no access to their data for days.

(c) **Software Migration:** It is another type of lock-in which is usually experienced in the PaaS model. It is applications lock-in which occurs when we cannot move our application to another CSP because every cloud service provider has its own set of features, framework and language support. Applications developed over a CSP platform

using their specific API will lock-in with that vendor as there are no standard APIs in the world of cloud that every CSP must follow.

This is the worst type of lock-in since we have to redesign or reengineer our whole applications on the new CSP's platform which is time, effort and cost consuming. It also creates extra effort if ties are broken with new service provider in the near future by creating same over head again and again which is not acceptable for every client and remains locked-in with the vendor.

These are the most known reasons for vendor lock-in which make it harder for a client to switch between CSPs and become dependent on the vendor after each day and is left to the mercy of the vendor.

### 2.3. Who benefits from vendor lock-in?

Obviously, the vendor is benefited from the vendor lock-in situation. Moving to cloud is made much easier than getting out of the cloud. As an example, Amazon S3 provides a free trail and all the data uploads are made free. But it won't get all these friendly features and support while getting out of someone's cloud as no one desires you to leave their cloud and move to their competitors.

## 3. Literature review

Vendor lock-in is a major concern for organizations while adopting cloud services. Many researchers are working and had given solutions to address the problem.

Justice Opara-Martins and Reza Sahandi, et al. (2017) [4] worked on avoiding vendor lock-in for cloud SaaS Migration under title "A holistic decision framework to avoid lock-in for cloud SaaS migration". They proposed a holistic six step decision framework for avoiding risks in cloud SaaS migration. They identified 12 challenges while switching between cloud SaaS vendors, which are (a) Technical Challenges (b) Business Challenges and (c) Legal Challenges. For tackling mentioned challenges the six steps which are organized in three phases namely Selection, Provision and Management are better illustrated in figure 1 which is the overview of their proposed work.



Figure 1. Cloud Decision Framework Overview[9]

Peter-Christian Quint and Nane Kratzke (2016)[5] worked on a solution by integrating already available container technologies towards transferability in cloud computing for small and medium enterprises (SMEs) to avoid vendor lock-in. They are introducing C<sup>4</sup>S which is an acronym for Container Cluster in Cloud Computing Systems (C<sup>4</sup>S). This tool, parts of which are developed, will help SMEs to use cloud computing without the fear of vendor lock-in. They further stated that C<sup>4</sup>S is designed to handle high complexity of a container cluster with benefits like elasticity, auto scaling and transformability.

Justice Opara-Martins, et al. (2016)[6] did a survey entitled "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective" to identify the main risk of vendor lock-in and its impact on cloud adoption. Their survey had two phases (1) Pilot Interview Study: where they collected qualitative data using open-

ended interviews with IT practitioners and (2) Quantitative Survey Questionnaire: with the goal of identifying and evaluating the risks and opportunities of vendor lock-in. Our area of interest in their survey is the vendor lock-in, to better understand the findings, you can visualize the graphical representation of the numbers in figure 02 and come to know how the lock-in situations affects the cloud adoption.

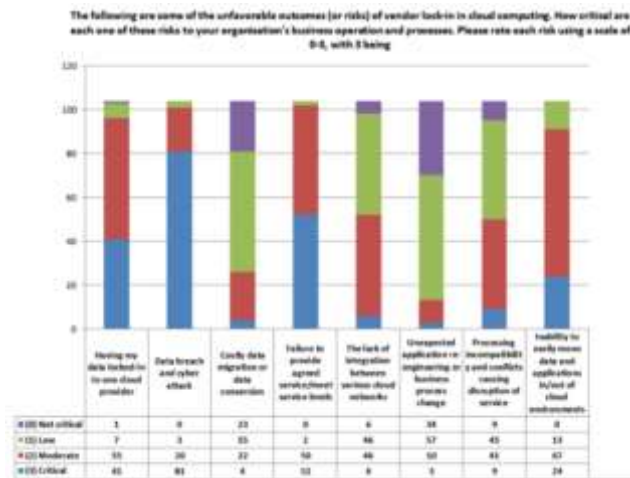


Figure 2 The potential for vendor lock-in risks is exacerbated in the cloud[12]

In the paper “vendor lock-in problem in cloud storage” (2015) Pekkala and Ville[7] stated about storage lock-in problems in cloud and addressed the Abu-Libdeh[8] paper’s statistics to show how the customer is locked-in with the vendor. As customer’s data size increases, the cost and time required for switching between vendors as well increase. Their provided solutions to vendor lock-in in cloud storage services are:

(a) Precaution: which states that firstly, ask the vendor, questions about the storage and extraction of data, data migration tools that make cloud-to-cloud transfer possible and whether they are pledged to support cloud computing standards, before adopting their services.

(b) The distributed cloud method: which mentioned that having data in multiple locations instead of only one CSP is more intuitive and protects against vendor lock-in. Replications of data provides redundancy and market mobility but on the other hand also increases bandwidth and storage costs.

Grace A. Lewis (2013)[9] talked about the roles of standards in cloud computing in his paper “Role of standards in cloud-computing interoperability”. He mentioned how standardization is important in cloud for solving many issues specially for data migration, workload migration, workload management and many other challenges which ultimately leads to the lock-in situation. He has named many projects undertaken for the purpose of developing standards for the cloud community. He has compared the current standardization efforts of cloud computing to that of web standards in 2006 where there were more than 250 standards. He believes that the efforts taken for the cloud standardization would finally be fruit full but we have to wait for it as we did for web standards. His paper shows that cloud standards is the answer for most of cloud challenges specifically the lock-in issue.

Another researcher Benjamin Satzger, et al. (2013) [10] gives the solution of Meta cloud to the vendor lock-in problem in the paper “winds of change: from vendor lock-in to the meta cloud”. They suggested that, once an application is developed using one particular CSP’s API that application is bound to that vendor only, and moving to the new provider will require completely redesigning the application using new provider’s API, which will again be dependent on that specific vendor’s particular API. Their suggestions of the Meta cloud comprises of two main goals:

- Find the optimal combination of cloud services for a certain application with regards to QoS(Quality of Service) for users and price for hosting; and
- Develop a cloud-based application once, and then run it anywhere, including support for runtime migration.

They introduced the meta cloud API. Customers can build their application using meta cloud API which provides a unified programming interface to abstract from the differences among provider’s API implementation. And there must be the meta cloud proxy which will act as a mediator between application and cloud provider. This proxy will transform application request to CSP’s specific requests. And there are some other components of the meta cloud as

Resource Templates, Knowledge Base, Resource Monitoring, provisioning Strategy and Migration/deployment recipes which together service the mentioned purpose.

Another researcher Alexandre Beslic, et al. (2013)[11] introduced a three step re-engineering approach to deal with software migration problem between cloud platforms in the paper called “Towards a solution avoiding vendor lock-in to enable migration between cloud platforms”. Their approach consists of Discovery, Transformation and Migration phases. The first step is the discovery of a cloud software deployed on a platform using MoDisco, second step is the transformation on the program structure/layout using model transformation on the discovered model, and the final step is the migration on the targeted platform with tests suites validation to make sure that software runs as usual. They found that re-engineering is a better and flexible approach than the middleware approach which could be harmful in the long run.

Kevin Xiaoguo Zhu, et al. (2011)[12] have found for low-reservation-utility customers, describing that lock-in is beneficial instead of hurting. They used lock-in strategy in software competition, using two-period duopoly model and illustrated that not every type of customer is in the loss due to the lock-in strategy. In their work they compared proprietary software with open source software by taking into account the two periods of licensing namely the current period and the future period and found that the total subsidies used to capture customers in the first period is so large that the lock-in strategy hurts the proprietary software vendor. They also found that lock-in strategy works differently for different type of customers i.e. when customers are myopic and not foresighted the lock-in strategy is likely to benefit the proprietary software vendor.

## 4. Conclusion

As a conclusion after literature review of many papers, we can say that Vendor lock-in is a major issue in the cloud which is under hard focus of the researchers and industry experts and also effecting the adoption of cloud. Some of the existing solutions for lock-in problem are Cloud standards but we don't have these standards which should be embraced by all cloud service providers and having such standards will be a matter of time, we can go for technical solutions to the problem.

An approach to cloud storage lock-in that we can do in the absence of standards are precautions and distributed cloud methods.

For application lock-in or application migration in PaaS model, meta cloud is useful suggestion. Which if developed and adopted, will vanish the dependency on a particular vendor's API and platform. Using meta cloud would affect the cloud experience but is best solution up to date.

There is future work and serious concern to provide a complete prevention of the lock-in situation.

## 5. References

- [1] The NIST Definition of cloud computing (2011) by Peter M. Mell, Timothy Grance. see [https://www.nist.gov/publications/nist-definition-cloud-computing?pub\\_id=909616](https://www.nist.gov/publications/nist-definition-cloud-computing?pub_id=909616)
- [2] The European Commission technical report. <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>
- [3] Nasuni (2014), “Bulk Data Migration in the Cloud [White paper]”, Nasuni press release: <http://www.nasuni.com/resource/white-paper-bulk-data-migration-in-the-cloud/>
- [4] Justice Opara-Martins, Reza Sahandi & Feng Tian, “A Holistic Decision Framework to Avoid Vendor lock-in Cloud Saas Migration”, Computer and Information Science, Vol.10, No.3, 2017. pp.29-53.
- [5] Peter-Christian Quint, Nane kratzke, “Overcome Vendor Lock-in by Integrating Already Available Container Technologies Towards Transferability in Cloud Computing for SMEs”, the seventh international conference on cloud computing, GRIDs and virtualization, IARIA, 2016, pp 38-41.

- [6] Justice Opara-Martins, Reza Sahandi and Feng Tian, “Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective”, Opara-Martins et al. Journal of Cloud Computing: Advances, Systems and Applications,2016, p 18.
- [7] Pekkala, Ville, “Vendor Lock-in problem in cloud storage”, Jyväskylä: University, 2015, pp. 22.
- [8] Hussam Abu-Libdeh, Lonnie Princehouse, Hakim Weatherspoon, “RACS: a case for cloud storage diversity”, Proceedings of the 1st ACM symposium on Cloud computing,2010, pp. 229-240.
- [9] Grace A. Lewis, “Role of Standards in Cloud-Computing Interoperability”, HICSS '13 Proceedings of the 2013 46th Hawaii International Conference on System Sciences, IEEE Conference, 2013, pp 1652-1661
- [10] Benjamin Satzger, Waldemar Hummer, Christian Inzinger, Philipp Leitner, and Schahram Dustdar, “Winds of Change: From Vendor Lock-In to the Meta Cloud”, IEEE Internet Computing, Vol. 17, Issue. 1, Jan.-Feb. 2013 , pp. 69-73.
- [11] Alexandre Beslic, Reda Bendraou, Julien Sopena, Jean-Yves Rigolet, “Towards a solution avoiding vendor lock-in to enable migration between cloud platforms”, 2<sup>nd</sup> international workshop MDHPCL 2013, pp. 5-14.
- [12] Kevin Xiaoguo Zhu, Zach Zhizhong Zhou, “Lock-In Strategy in Software Competition: Open-Source Software vs. Proprietary Software”, Articles in Advance,2011, pp.1-10,ISSN 1047-7047.

