ISSN No:-2456-2165

Vendor Lock-In Situation and Threats in Cloud Computing

Purushottam Kumar
Assistant Professor,
Department of Computer Science and Cyber Security
Jharkhand Raksha Shakti University
Jharkhand, India

Dr. Prakash Kumar
Assistant Professor (HOD),
Department of Computer Science and Cyber Security
Jharkhand Raksha Shakti University
Jharkhand, India

Abstract:- Due to the absence of standards, vendor lock-in is a significant obstacle to the adoption of cloud computing. The vendor lock-in issue is now being addressed mostly through technological means. There aren't many studies that analyze and show how complicated the vendor lock-in issue is in the cloud context. As a result, while purchasing services from vendors, the majority of clients are unaware of the proprietary standards that prevent application portability and interoperability. In-depth discussions of cloud concepts are covered in this paper, along with the causes of vendor lock-in problems and some preventative measures that can be taken. This is because many businesses are concerned about the possibility of becoming stuck with a vendor and being dissatisfied with the vendor's services.

Keywords:- *Cloud Computing, Vendor Lock-In, Cloud Models.*

I. INTRODUCTION

Cloud Computing is now a popular paradigm, offering computing resources on a pay-as-you-go basis. It allows a remote and on-demand access to a wide range of services alleviating the need to own and maintain an internal infrastructure. The service model is standardized by the NIST (National Institute of Standards and Technology) and is divided into three major layers. These layers vary in the amount of abstraction they provide to the consumer. The more you climb this service model, the more you will face restrictions. Infrastructure as a Service (IaaS) provides the ability for consumers to provision fundamental computing resources such as processing power, storage capacity or networks. They have control over the operating system and software stack giving them the freedom to deploy any kind of software. Platform as a Service (PaaS) came as an abstraction to the infrastructure layer. Because maintaining and updating a whole infrastructure requires knowledge and time, platform provides with a fully prepared runtime environment to deploy applications. It targets developers to further fasten the development process and to focus on the product features rather than configuring the underlying infrastructure. Software as a Service (SaaS) is the highest level of the Cloud service model. The software itself is provided as a service to the end-user. While Infrastructure as a Service (IaaS) and Software as a Service (SaaS) are still prevalent in the Cloud computing service model, Cloud platforms (PaaS) are becoming increasingly used. According to the recent surveys the use of Cloud Platforms has increased exponentially.

Fig 1: - Split of Management Responsibilities for Cloud Computing Service Models [10]

With a major struggle between cloud providers to dominate the PaaS market, the use case of software migration between providers is to be considered. But this task is far from being easy. Indeed, the platform layer suffers from a well-known issue: the vendor lock-in. Early platforms are providing tools and libraries to use during the development process to access their own features thus locking the application to this platform. The advent of NoSQL solutions with data denormalization makes it even more difficult because of choices made on the program's design to ensure best performance. As a consequence, migrating onto another platform requires tremendous re-engineering effort that a few are able to provide. The will to migrate is explained by several factors. The price is the first one, considering that computers are now a commodity that we need at the lowest price, thus explaining the popularity of the Cloud Computing paradigm.

ISSN No:-2456-2165

Some other factors are the Lock-in avoidance, an Increased Security, a better availability, a Better Quality of Service (QoS guarantee), a Major shift in technology trends or Legal issues (forced to move) among others. As of today, no such tool exists to achieve this migration. In this regard, we present our approach to deal with this major issue of migrations between Cloud Platforms, it shows that, although appearing to be the future of computing, cloud computing is still far from flawless and that researchers and industry professionals are working to improve it. The majority of large enterprises that have adopted cloud computing focus their attention primarily on vendor lock-in notwithstanding all other difficulties encountered in the transition.

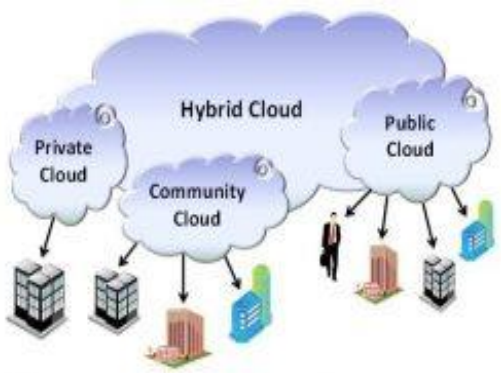

Fig 2: - Cloud deployment models [11]

At first, it was hidden from view, but as more and more businesses migrated to the cloud, they became aware that they were eventually being locked-in. The goal of this research is to assess the numerous problems and facets of various studies pertaining to the vendor lock-in problem. Vendor lock-in problem in cloud computing is characterized by expensive and time-consuming migration of application and data to alternative providers.

Cloud software vendors lock in customers in several ways:

- By designing a system incompatible with software developed by other vendors.
- By using proprietary standards or closed architectures that lack interoperability with other applications.
- By licensing the software under exclusive conditions.

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. According to, 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. 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.

II. VENDOR LOCK-IN

Since the beginning of cloud-based services, the vendor has handled every task and delivered every service. Businesses that currently use cloud-based services may decide to switch to a new Cloud Service Provider (CSP) at some point in the future. This could be because the CSP is no longer able to meet the tenant's needs, there have been changes or updates to the services that the client does not like because they do not meet the client's needs, the CSP has raised its prices, another CSP is offering the same or even better services for less money, there have been agreement breakups, or there could be any number of other reasons that lead the client to switch CSPs but they are unable to get out of this situation, which is known as the Vendor Lock-in.

III. TYPES OF VENDOR LOCK-INS

A. Pricing Locks-ins That Ransoms You

In this type of locks-ins users are charged for the services which they haven't used.

Causes: - Costly Implementations, at the time of procuring a new SaaS, many vendors charge a one-time set-up fee, also called an implementation fee. This setup fee is usually incredibly pricey. So, if you find yourself wanting to change your cloud service provider for any reason, you might go against changing the provider because of the high implementation cost you paid to your current vendor. Non-adherence to usage-based pricing. Usage-based pricing means you pay based on how much you consume. This is the best practice that needs to be followed by cloud vendors. But unfortunately, to make you pay for even the unused and underutilized apps, most of the vendors don't adhere to this practice. They charge you monthly regardless of whether you use their service or not.

Solution: - Finding vendors who provide quick, affordable (or free), and efficient solutions is the first step. Pick suppliers that provide "ready to go" cloud services. You can increase the time to value with a shorter implementation period. An effective software usage monitoring app will examine your usage and assist you in lowering costs associated with inactive and underused apps.

B. Lock-in That keep Your Data as Hostage

Data plays an important role in business. But most of the CSPs providers threatens to destroy your data or keep it as a hostage whenever you wish to change the current CSP.

➢ *Causes*

- Loss of access to your data: - Type of lock-in is when the vendor threatens to destroy your data while holding it hostage. This typically occurs when you fail to make your monthly fare payment, make a late renewal, or switch to a competing product.
- Loss of insights: - While you ask for your data to be transferred when switching services, providers may give you a dump of your data in a CSV (comma-separated values) file. CSV can quickly access your data; however, it loses the context of the data. You must maintain the

context for auditing in specific sectors, such as healthcare and fintech. For example**,** hospitals need to preserve patients' electronic medical records (EMR) for up to 7 years. EMRs may contain the clients' signature which is not possible to transfer in the CSV format.

- Data migration**:** - To avoid wasting your time while getting your data from these providers, make sure they give it to you in a format that your new SaaS application can read. Due to the fact that you are switching to a new cloud service, these vendors charge you a lot to retrieve your data, giving them the opportunity to burn a hole in your wallet. By purposefully raising switching expenses, these suppliers prolong your stay. They are aware of the reasoning behind why you would be less likely to switch to another software provider if switching charges were higher. In some circumstances, the data processing is so complex that you require technical knowledge to fully comprehend the procedure.

Solution: Ask your vendor for the database image if your data is stored in an RDBMS (Relational Database Management System) format so that you can move it without any data loss. Having a backup of all your data is essential, even though you share crucial data on your SaaS applications. You must choose cloud service providers who make the data conversion process quick and straightforward. Additionally, you must be adamant with vendors regarding your data format. For your data, fight.

C. Flexibility: Locks-ins that Handcuffs You

In this type of locks-in your working and approaches towards the data is limited. It will not keep your data as hostage, you can perform basic operations on it but in a limited approach.

➢ *Causes*

- Unable to choose between external and internal databases**:** - You are more locked in the more you lean toward their SaaS stack. Unless you spend twice as much, the majority of SaaS suppliers won't let you run their applications on Amazon AWS, Microsoft Azure, or Google Cloud Platform. They impose a requirement that you use their surroundings. Links to the vendor's website are included in the contract. You must sign an agreement with a cloud provider that gives them the power to unilaterally change the terms and conditions by merely changing the text on a webpage. Because they don't own every component of their system, several cloud service providers do this. They frequently sell third-party solutions that they embed into a solution through a link contained in the vendor's paper. You shouldn't accept a web link in a contract unless absolutely necessary. The terms of service may have said in the original agreement that they wouldn't utilize your data. However, these suppliers may make changes later to sell your data to outside advertising in order to monetize it.
- Add a fee for features based on AI or ML: By automating repetitive operations, artificial intelligence has the ability to improve corporate processes, contribute to productivity growth, and improve your work efficiency. This is frequently exploited by vendors, who charge you extra for features based on these capabilities.

Solutions: Vendors who allow you the choice to host the application are preferable than those who force you to utilize their platform. The opposite should be true as well, since you cannot alter the contract terms without your vendors' approval. Make that the contract is entirely static and that there are no online links or other dynamic parts pointing to the vendor's website, which the vendor may update at any time. Ask for the inclusion of AI, automation, and any other intelligence functionality in the base programme rather than having them packaged and sold separately.

D. Renewal which gives you a lower hand in negotiation

At the time of renewal most of the CSPs will charge you high, as they know that your IT team has got used to, of their services. So, it becomes quite difficult to change the entire CSP and start with new terms and tools of new CSP. This type of locks-ins lowers your hand in negotiation and makes you to accept their renewal conditions.

➢ *Causes*

- Vendors put off discussing a renewal until the very last minute**.** The vendor's sales team forces you to wait until the very last minute to discuss renewals. Therefore, you are unable to switch to a different vendor in time. During this little time, the sellers' end of the price increase is where the majority of it occurs. There is nothing else for it but to keep onto them. Price protection on renewal for a limited period. This is done on purpose to raise the price when the first period ends. Some vendors' agreements compel you to deploy an expensive, ongoing, and sometimes difficult service that could put you out of business. Due to the prohibitive switching prices, their agreement clauses prevent you from changing providers, leading you to second-guess your choice. To increase the price after the initial term has passed, this is done on purpose. You may go bankrupt if you are required by some vendors' agreements to install an expensive, ongoing, and perhaps difficult service. Since transferring to a different provider would incur a significant amount of money, their agreement terms prevent you from doing so.

Solution: Negotiations should begin at least a year before the present service is set to terminate. In this case, you might move to a different solution and take a lot of time implementing it, or you can acquire the finest negotiation options to the agreement. You can gather usage information and use it in talks.

IV. CLOUD VENDOR LOCK-IN FEARS

Many factors contribute to concerns about cloud provider lock-in. The loss of control over the infrastructure and data that underpin commercial applications comes first. It can be unsettling to not have total control over things like security, uptime, and infrastructure management as a whole. The dependence on a single vendor for so many essential requirements is the next issue. Your supplier is heavily dependent on you because they control your servers, data,

ISSN No:-2456-2165

networking, user management, and much more. And if something goes wrong, it could have a serious negative impact on your company. Additionally, you could worry that one cloud provider won't be able to match your needs now or in the future. You might have to reconsider your connection with your CSP if they don't adhere to service level agreements or have a data breach. Even worse, you'll need to take into account the possibility of that vendor ceasing operations. Every IT manager considers the expense and difficulties of transitioning to a new vendor when considering whether to go to the cloud and choosing a cloud service provider.

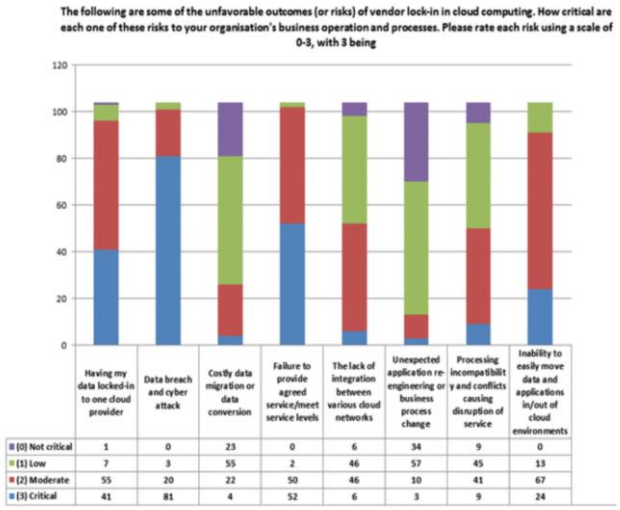

Fig 3: - The potential for vendor lock-in risks is exacerbated in the cloud [14]

V. TYPES OF VENDOR LOCK-IN RISKS

If something goes wrong, it can be challenging to switch to a different cloud service provider due to vendor lock-in. There are four primary lock-in risks that you'll take working with a single cloud provider. These include:

- Data transfer risk
- Application transfer risk
- Infrastructure transfer risk
- Human resource knowledge risk
- Data transfer risk

A. Data transfer risk

Transferring your data from one CSP to another is not simple. During a data migration procedure, a wide range of inquiries will surface, including:

- Who is in charge of removing the data from the data warehouses and cloud databases?
- How will the data be formatted? Will that format work with the new cloud provider, or will the data require significant changes?
- How can the data be moved without affecting the functionality of the application?
- How long will it take and how much will it cost to move all of this data?

Although certain industry bodies have made an effort to develop standards for data exchange, occasionally businesses find it challenging to put those standards into practice because of their particular business needs.

B. Application transfer risk

It can be very expensive and challenging to reconfigure an application to function natively on another provider if it was developed on one CSP and makes extensive use of that provider's features. Let's imagine, for example, that you created a business intelligence platform on Microsoft Azure. You make use of fundamental cloud services, such as computing, storage, databases, and networking. However, the programme also makes use of Azure's bot, data lake, and machine learning capabilities. The absence of open APIs and standard interfaces is one cause of this problem. It is exceedingly difficult to switch from one CSP to another because they all have their own exclusive specs and standards. The quick development in both technology and consumer demands is another factor.

C. Infrastructure transfer risk

Every significant CSP operates slightly differently. It can be challenging to guarantee that you will have the proper resource utilization and cost savings if you transfer providers because virtual machine formats and their associated price differ from vendor to vendor. Different databases may have different offerings and formats. Additionally, one cloud provider might offer more appealing options for some infrastructure components while falling short on other services you might require. Moving from one cloud service provider to another is challenging due to these variations in the underlying architecture.

D. Human resource knowledge risk

Your IT team probably has a lot of institutional knowledge about the tools and configurations of that CSP if you've been dealing with just one. If you have to switch CSPs, it will take some time for your engineers to become proficient with the new cloud platform. They will need to get knowledge about fresh infrastructure formats, implementation procedures, and other topics. Although it is rarely considered, the knowledge risk is just as significant as the hazards mentioned above.

VI. MEASURES TO AVOID VENDOR LOCK-IN

- Exercise due diligence: - Before you select your CSP, you should properly vet that they will give you all that you need to execute your applications reliably. We must ascertain your cloud migration goals before choosing a CSP. Analyze your current IT scenario, taking careful note of your current infrastructure, costs, and resource availability. Choose between a public, private, or hybrid cloud environment depending on your needs. Identify the necessary individual cloud components. In order to reduce the danger of vendor lock-in, it is essential to have a thorough grasp of your possible CSP.

- Plan early for an exit: - It resembles a prenuptial agreement in the cloud. Include an escape strategy and any potential costs when you prepare your implementation approach.

- Design your application to be loosely coupled: - Your applications should be created or moved to be as flexible and loosely connected as possible to reduce the danger of vendor lock-in. The application components that communicate with cloud application components should be only loosely coupled to them. This can be accomplished by decoupling your apps from the underlying proprietary cloud infrastructure by combining REST APIs with well-known industry standards like HTTP, JSON, and OAuth. This will not only lessen the degree of vendor lock-in, but it will also give your application the interoperability necessary for quick workload movement and multi-cloud environments.

- Make your data as portable as possible.: - Data migrations are notoriously difficult since differing models and formats might lead to portability problems. Avoid using proprietary formats if you want your data to be as portable as possible. Clearly describe data models using applicable schema standards to produce thorough documentation that is both computer- and human-readable. Make sure your cloud provider offers a simple and affordable method for you to extract data.

- Adopt multi-cloud strategy: - A multi-cloud environment, where you can use various CSPs to power your apps, is where the majority of organizations are headed. For instance, you might use IBM Bluemix's Watson as your artificial intelligence platform while employing Amazon EC2 for compute capacity and Redshift for your data warehouse. Going multi-cloud reduces your reliance on a single CSP to meet all of your requirements. A multi-cloud strategy has some drawbacks, such as extra work for development teams and increased security risk.

- Use DevOps techniques and tools: - More and more DevOps tools are being used to maximize code portability. Companies like CoreOS and Docker offer container technology, which helps isolate software from its surroundings and abstract dependencies from cloud providers. Since the majority of CSPs offer common container formats, moving your application to a different cloud provider should be simple in such case. By automating the configuration of the infrastructure that supports your apps, you may deploy your application to a variety of IT settings, which can make switching to a new CSP less challenging. Configuration management tools like Chef and Puppet can help you do this.

VII. CONCLUSION

In this paper we have compared how vendors could use the absence of standards in cloud computing to take advantage of customers by making their solutions as proprietary as possible to facilitate lock-in with key interoperability and portability difficulties related to vendor lock in. Our continuing research focuses on finding solutions to the problem of vendor lock-in in the context of cloud computing. We want to research fresh ways to avoid vendor dependence and create a paradigm for cloud computing migration that deals with the problem of vendor lock-in.

REFERENCES

[1]. A. M. Alakeel, "A Guide to dynamic Load balancing in Distributed Computer Systems", International Journal of Computer Science and Network Security (IJCSNS), Vol. 10, No. 6, June 2010, pages 153-160.
[2]. The NIST definition of cloud computing, available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800- 145.pdf.
[3]. W. Kim; Cloud computing architecture, available at: https://www.academia.edu/42414263/Cloud_computing_and_Infrastructure.
[4]. R. Buyya, J. Broberg, and A. M. Goscinski, Cloud computing: Principles and paradigms, vol. 87. John Wiley & Sons, 2010.
[5]. D. Bermbach, ―Quality of Cloud Services: Expect the Unexpected, ‖ IEEE Internet Comput., vol. 21, no. 1, pp. 68–72, 2017
[6]. N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, ―Access control as a service for the Cloud,‖ J. Internet Serv. Appl., vol. 6, no. 1, pp. 1–15, 2015.
[7]. Purushottam Kumar,Dr. Prakash Kumar; A survey on Load balancing in Cloud Computing.
[8]. Cyber Security Issues and Challenges in India Mr. Purushottam Kumar, Dr. Prakash Kumar
[9]. Dr. Prakash Kumar, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.12, December- 2017 | ISSN 2320–088X, pp. 157-163
[10]. https://kinsta.com/blog/types-of-cloud-computing/
[11]. https://www.turningcloud.com/blog/cloud-deployment-models/
[12]. A Review on the Risk and its Countermeasures in Cloud Environment Sourav Kumar Upadhyay , Dr. S.C. Dutta, Dr. Prakash Kumar
[13]. Wang Xiaoyu, Gao Zhengming, Research and development of data security multidimensional protection system in cloud computing environment, international conference on advance in ambient computing and intelligence, 2020, School of Computer Engineering, JingchuUniversityofTechnology,Jingmen448000,China
[14]. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0054-z
[15]. 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
[16]. 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
[17]. Satzger B, Hummer W, Inzinger W (2013) Winds of Change: From Vendor Lock-in to the Meta Cloud. IEEE Internet Comput 1:69–73
[18]. 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