International
Journal
Of Advanced Research in Engineering & Management (IJAREM)

A solution for minimizing Vendor Lock-In problem in Cloud Computing

Gajawada Sai Pranay Gupta, Abinaya G, Pavithra M
M.S Software Engineering
VIT University, Vellore.

***Abstract*—**Cloud computing has evolved a lot and it is being extensively used. There are various drivers which make people to choose cloud but at the same time there are a number of problems. One such important issue is Vendor Lock-In. In this paper we are going to discuss about vendor lock-in problem, causes for this problem and propose a solution for this problem. We also discuss the limitations of proposed solution.

***Keywords*-**Vendor Lock-In, Encryption, Data Sanitization, Customer Management Layer(CML)

1.INTRODUCTION

Cloud computing is a model for enabling convenient on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In another context cloud computing is a delivery of computer services over the internet. Cloud provides on demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

Cloud computing is widely used now a days, but shifting to cloud computing means giving up control over your data to some extent and there are a lots of issues related to security, privacy and monitoring of data. One such issue faced is the vendor lock-in issue.

1.1VENDOR LOCK-IN

The term vendor lock-in means that the user and the provider of cloud services become dependent on each other. And this dependency is the result of diversity of the service types offered by various cloud providers. There are three solutions to overcome this issue and they are, following standards, using adapters and abstraction layers, adopting model based solutions and semantics to reduce the complexity.

The primary problem faced by the customers is the inconvenience of shifting their data and applications from one cloud to another[1]. Different cloud vendors offer cloud based services with different specifications that vary from each other because, presently each service provider has its own set of software technology, remote API's and in some cases they have their own separate programming language which makes the cloud users to be highly dependent on one particular service provider, and forcing them not to shift to another cloud vendor. This condition is defined as the locked in situation. If the customer still wishes to shift to another service provider then he has to face all the troubles that arises due to technical incompatibilities and the other related expenses[2]. In fact many customers remain with the same vendor to save themselves from these expenses. This attitude of customers has two important impacts.

First, it gives inefficient service providers with power over the market, second it may influence the consumer and vendor choices among the available alternate technologies.

As of cloud computing is concerned, vendor lock-in is the result of present variation between separate vendors based on non-compatible underlying technologies[3]. To totally eradicate vendor lock-in or to minimize its efficacy, consistent effort to ensure interoperability and portability across cloud computing services and systems is necessary. Cloud service vendors lock the consumers in many ways like, developing a system that is incompatible with the system developed by other vendors. Using standards that lack or have lesser interoperability with other soft wares. By using certain licensing terms and conditions vendor lock-in issue deters the growth of the organizations that use cloud computing technology.

2. THE PROBLEM

Vendor lock-in occurs when an organization becomes overly reliant on a single vendor for too many solutions and/or services.

There are many reasons which cause the vendor lock-in problem such as:

1. Use of proprietary APIs provided by the Cloud Service Provider
2. Heavy cost of migration
3. Improper Data Sanitization

The first reason is that if a customer is using all the proprietary APIs provided by CSP then during migration customer needs to change all their applications based on the APIs of new CSP.Even if the customer uses Open Source APIs, this problem cannot be solved as there are a wide range of open source for cloud.

Vendor lock-in exists when the cost of switching from one vendor's technology platform to another is so material that the customer is effectively unable to migrate from the vendor's offerings. This is the problem of heavy migration cost.

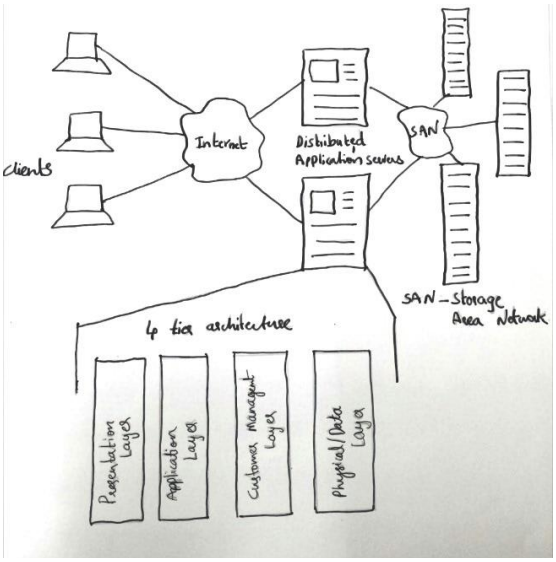
Improper Data Sanitization is a critical issue. Customer stores their data on the cloud.In order to provide reliable service the Cloud Service Provider will back up the data in various locations.This helps in events such as disaster recovery.This location information of data is hidden from client.Client doesn't know if the data is properly sanitized when they are moving from one Cloud Service Provider to other Cloud Service Provider.This will cause the client to stay with the same vendor as some sensitive data is locked within the existing CSP.

3. PROPOSED SOLUTION

We have proposed a solution by slightly modifying the cloud architecture.We are adding a new layer – Customer service/management layer, in the distributed application servers. Thus the new architecture has four layers on the server. They are:

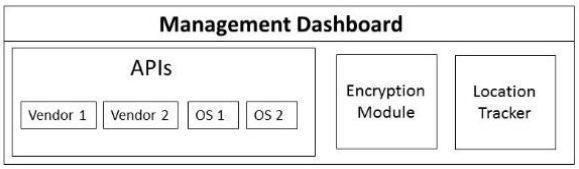
- Presentation Layer
- Application Layer
- Customer Management Layer

Physical/ Data Link Layer



3.1 CUSTOMER MANAGEMENT LAYER

Customer management layer is a cloud platform agnostic layer.This layer consists of management dashboard. This is a GUI for accessing various services provided by customer management layer.This can be an independent service also. Such as management services can be a separate cloud service provided by a CSP.



Customer management layer consists of three modules:

1. API Implementations
2. Location Tracker
3. Encryption Module

In API Implementation module various Application Programming Interfaces of various Cloud Service Providers which are very popular are implemented.Also most common Open Source APIs are also implemented in this module.This helps to modify the client application to suit any of the APIs provided by different CSPs. Thus preventing one of the cause of vender lock-in problem.
Location Tracker will keep track of all the locations where a particular customer's data is stored.This location information is visible to customer.Customer can use this information to monitor their data. It also helps to ensure proper sanitization when the customer is moving to other CSP.
Encryption Module consists of the encryption algorithm using which the customer data is encrypted.Each customer has a unique encryption/decryption key.This key is not stored in any place in cloud.Based on this key the customer will encrypt the data and store it in cloud so that it cannot be interpreted by the CSP. When the customer needs the data he will decrypt the information using same key. Thus achieving security to information.The client has the right to delete all his data on the cloud. Thus preventing improper data sanitization which is one of the driver for Vendor lock-in.

Customer management layer consists of three modules:

1. API Implementations
2. Location Tracker
3. Encryption Module

In API Implementation module various Application Programming Interfaces of various Cloud Service Providers which are very popular are implemented.Also most common Open Source APIs are also implemented in this module.This helps to modify the client application to suit any of the APIs provided by different CSPs. Thus preventing one of the cause of vender lock-in problem.
Location Tracker will keep track of all the locations where a particular customer's data is stored.This location information is visible to customer.Customer can use this information to monitor their data. It also helps to ensure proper sanitization when the customer is moving to other CSP.
Encryption Module consists of the encryption algorithm using which the customer data is encrypted.Each customer has a unique encryption/decryption key.This key is not stored in any place in cloud.Based on this key the customer will encrypt the data and store it in cloud so that it cannot be interpreted by the CSP. When the customer needs the data he will decrypt the information using same key. Thus achieving security to information.The client has the right to delete all his data on the cloud. Thus preventing improper data sanitization which is one of the driver for Vendor lock-in.

4. LIMITATIONS OF THIS SOLUTION

This may result in some regulatory issues such as FBI/CBI should be able to access all the data on cloud. But if the customer data is encrypted then it cannot be interpreted.Since the Location Information is open to customer, this results in greater potential for hackers to attack data centers.More overhead in processing even if a client is using standard API.

5. CONCLUSION

We have seen in detail about Vendor Lock-In problem in cloud. It is clear that this problem is an important security aspect to be considered in cloud. We have also seen the solution which slightly modifies the cloud architecture. This new solution has its own pros and cons. Limitations of the solution are also discussed.

REFERENCES

[1]. 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.
[2]. M. Toivonen, "Cloud Provider Interoperability and Customer Lock-in" Dept. of Computer Science, University of Helsinki, Research Paper 2013.
[3]. 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.