

# Transforming the Data into Virtual Set-Up Segmented usage and Adoption

Dr. R. Poorvadevi

Assistant Professor, CSE Department, SCSVMV University, Kanchipuram, Tamil Nadu, India

**How to cite this paper:** Dr. R. Poorvadevi "Transforming the Data into Virtual Set-Up Segmented usage and Adoption" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-3, April 2019, pp.856-858, URL: <https://www.ijtsrd.com/papers/ijtsrd23094.pdf>



IJTSRD23094

## ABSTRACT

In digitalized environment, heterogeneous users are host and deploy their applications as a digital transformation. As the growing of dynamic business requirements, the operational values of service level agility, scaling and availability of resources are the more focusing components. However, enterprises are needed to deliver the data with utmost desired security value to its genuineness users. All the client level processes are initiated by verifying the strong security level access parameters. So, it is important to process the data migration with the adopted cloud vendors. Lots of security breaches are causing the data level protection in the service access environment. The proposed work will implement the secured transformation user's data, applications, and resources to the desired virtual set-up in order to strengthen the customer's application. The approach will be used to finding the service adoption by verifying the level of service guaranty with the cloud vendor adoption.

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (<http://creativecommons.org/licenses/by/4.0>)



**KEYWORDS:** Data migration, Cloud adoption, cloud vendor, data segmentation, cloud service provider, Virtual set-up, cloud client, Security breaches.

## 1. Introduction

Cloud framework has the challenges for fundamentals of security which are isolation and segmentation. Moving applications and data from fully self-controlled to third party-controlled realms poses a significant cyber security concern to most enterprises. IT and security teams rigorously assess applications on a case by case basis before they are moved to the cloud – especially applications which create, process, and store sensitive data. As a best practice for cloud adoption, the less critical applications are moved to the cloud first, with the assumption that this reduces the security risk and allows gaining experience.. Attackers today use sophisticated techniques, not only to steal data, but also to compromise the systems to create bot networks. This eventually robs the enterprise with excessive cloud billing and potentially opens the door to access more sensitive applications which are on-premise. These are some of the reasons why cloud adoption is a slow and careful process for most enterprises.

## 2. Literature Study

An author Paulo Rupino da Cunha, et.al, "Avoiding Lock-In: Timely Reconfiguration of a virtual cloud Platform on Top of Multiple PaaS and IaaS Providers". This paper has mainly focused on virtual cloud platform creation for multiple level of PaaS and IaaS service provider. All the lock-in controls are reconfigured with cloud underlying architecture. [1]

Zhengping Liang et.al, "Security of virtual working on cloud computing platform". This paper has implemented the security metrics for the various cloud user applications. Determined the virtual set-up process for all the cloud service provider data sources. [2]

Pongsakorn U-chupala et. al, "An implementation of a multi-site virtual cluster cloud". This paper proposed a novel approach of multi site user application transformed to the virtual cluster groups by specifying the access level policies, data protection in the service platform.[3]

So, from the analysis of background work all the security level implementations were considered and processed into the different cloud adoption. There are no specific standards, access policies are formed for the data migration.

## 3. Proposed Work

Accelerating the cloud application to the micro segmentation will process the application, data level functions the digital transformation level to mitigate the security policies with the compromising security parametric values. The various client service specific applications were examined under the machine –critical applications and finding the enterprises to secure the entire client level resources to be segmented with the cloud user adoption level. External threats also to be

notified with the security perimeter control to process and regulate the traffic between the access policies. Internal networks, technologies are combined with the data segmentation policy level to produce the application migration and content specific process over the transformation levels.

The following are the needs for transforming data to the virtual setup for the cloud user and enterprise applications which is listed below:

- Modernize Current IT asset base
- Prepare for future needs
- Lower infrastructure costs
- Increase Business agility
- Disaster Recovery Security

The major concern for transformation of data to the virtual setup is data gravity. The cloud infrastructure will explicitly specify the data abstraction for the user applications. Integration of business segments to the various user groups. It also finds the customized time factor for transforming of any client level resources to the virtual environment.

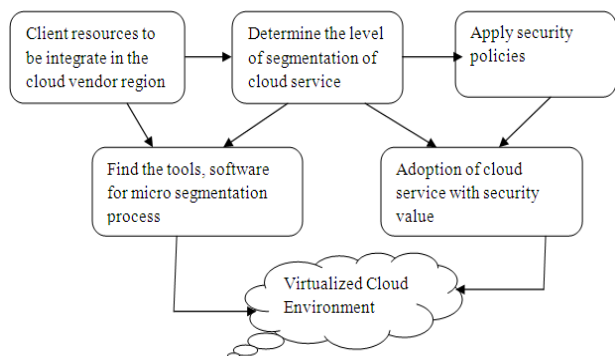


Fig: 1 proposed system architecture

An above diagram will (fig1) depicts the functional process of iterating the applications and client’s data in the virtualized environment. All the generic process will analyze the micro level segmentation task in the cloud infrastructure platform to specify the level of segmented data usage.

**4. Implementation Work**

Customizing the data integration among the cloud vendors will specify to locate the users application in the secured platform by maintaining the data management policies and application mobility and also improving the governance.

The main issue is that every application complicates data management by introducing elements of application logic into the data management tier, and each one is indifferent to the next data use case. Business processes use data in isolation and then output their own formats, leaving integration for the next process. Therefore, application design, data architecture, and business processes must all respond to each other, but often one of these groups is unable or unwilling to change. This forces application administrators to sidestep ideal and simple workflows, resulting in suboptimal designs. And, although the workaround may have been necessary at the time, this technical debt must eventually be addressed during data migration or integration projects

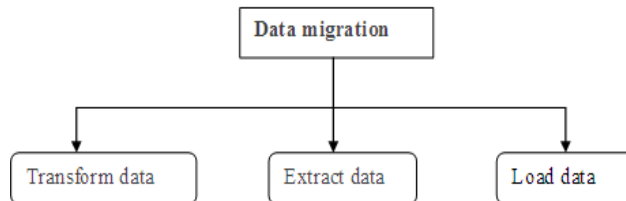


Fig: 2 Process of Data migration in Virtual set-up

All the generic process is built on the application environment and identification of client level security parameters are evaluated with the virtual key ID values. However, entire transaction of client’s information is also migrated with the specific cloud vendor platform. The following are the various strategic processes are verified and demonstrated in the virtualized environment. The key logger’s data has been identified by encrypting the correct key values in the client access platform. The following table shows the sample identified results for the application transformation to the virtual setup which is listed below:

Service Process ID	Migrated Environment	Cloud adoption status	Process efficiency (%)
ID -709	AWS	Processsd	89.23
ID - 15.267	GAE	optimizd	94.3
ID - 53.083	Sales force	verified	97.16
ID -67.1	Microsoft Azure cloud	processsd	99.03
ID -48.2	EC2	Processsd	99.42

Table: 1 depicting the migration process outcome

The above table process the significant role of application migration to the requested user access zone. All the generic processes are evaluated under the desired service environment. This table show that, how the migration has taken place for the various service access platforms.

**5. Experimental Results**

The user application process is demonstrated for the various migration policies to evaluate the service migration process. Segmented data has been adapted to the cloud vendor location and process the migration level access constraints along the service environment. To enable the service process for the various cloud user applications virtualized environment credentials are investigated with the specific user level access information.

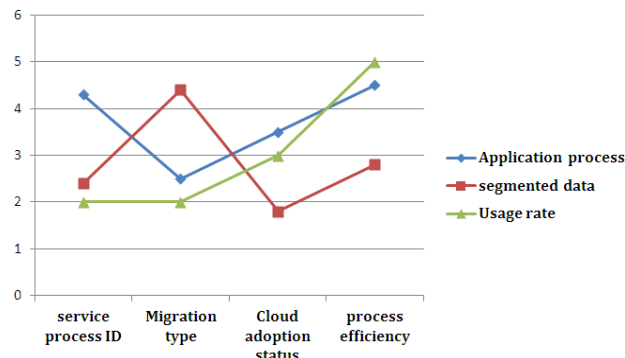


Fig: 3 Process of Transformation of user application to the virtual environment

## 6. Conclusion

From the migration perspective all the user access level constraints are verified for the applications transformation to the virtualized environment. All the security components are iterated with the specific functional parameters for segmenting the data into the concern and schematic cloud adoption mechanism.

### References:

- [1] Paulo Melo ; Catarina Ferreira da Silva , : Avoiding Lock-In: Timely Reconfiguration of a virtual cloud Platform on Top of Multiple PaaS and IaaS Providers", International conference on Cloud Computing, Year: 2013, Pages: 970 - 971
- [2] Zhengping Liang ; Songsong Jia ; Jianyong Chen ; Pengfu Chen, "Security of virtual working on cloud computing platform", 2012 IEEE Asia Pacific cloud Computing Congress (APCloudCC), Year: 2012, Pages: 72 - 75
- [3] Pongsakorn U-chupala ; Putchong Uthayopas ; Kohei Ichikawa ; Susumu Date ; Hirotake Abe, "An implementation of a multi-site virtual cluster cloud ", The 2013 10th International Joint Conference on Computer Science and Software Engineering (JCSSE), Year: 2013, Pages: 155 - 159
- [4] Qi Zhang ; Ling Liu ; Calton Pu ; Qiwei Dou ; Liren Wu ; Wei Zhou, "A Comparative Study of Containers and virtual Machines in Big Data Environment", 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), Year: 2018, Pages: 178 - 185
- [5] Subhadra Bose Shaw ; Jay Prakash Kumar ; Anil Kumar Singh, "Energy-performance trade-off through restricted virtual machine consolidation in cloud data center", 2017 International Conference on Intelligent Computing and Control (I2C2), Year: 2017, Pages: 1 - 6
- [6] Fanqiang ; Xiaoxia Xu ; Libo cui, "The research about modeling technology of irregular virtual reality scene based on point cloud data", 2010 International Conference on Computer Application and System Modeling (ICCSM 2010), Year: 2010, Volume: 6 Pages: V6-538 - V6-541
- [7] D. Maria Manuel Vianny ; M. Aramudhan ; G. Ravikumar, "Effective binary cuckoo search optimization based cloud brokering mechanism on cloud", 2017 International Conference on IoT and Application (ICIOT), Year: 2017, Pages: 1 - 8

