RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

# An Overview on Benefits, Applications and Problems in Multi-Tenancy Techniques in Cloud Computing Models

[1]A Yashwanth Reddy and [2]Dr. M.Upendra Kumar

[1]*Research Scholar, Sri SatyaSai University of Technology*
[2]*Professor CSE, St.Peter's Engineering College (SPEC)*

**ARTICLE DETAILS**

**Article History**
*Published Online:* 25 May 2019

**Keywords**
*IAAS, SAAS, PAAS*

**ABSTRACT**

The word Cloud is utilized as an analogy for the internet, based on standardized utilization of a cloud like shape to signify a network. Cloud Computing is trend setting innovation for resource sharing through network with less cost as contrast with different advances. Cloud infrastructure bolsters different models IAAS, SAAS, PAAS. The term virtualization in cloud computing is exceptionally valuable today. With the assistance of virtualization, more than one working system is upheld with all resources on single H/W. We can likewise say that we procured single server yet we utilized it for multiple functions (Web Server, database server, Application Server, DNS Server, and DHCP Server). One more asset of cloud computing is Multi Tenancy. Security inside the cloud is of foremost significance as the interest and without a doubt use of cloud computing increment. Multi-tenancy specifically acquaints one of a kind security risks with cloud computing because of more than one tenant using the equivalent physical PC equipment. Cloud Computing is the most slanting Information Technology computational model. This environment is empowered with an Internet to give computing resources involved software, servers, Storages and applications that can be gotten to by a customer. Cloud computing is the crucial model to give the services like Infrastructure as a Service, Platform as a Service and Software as a Service. Larger part of these services are offered based on pay per use rent style speculation with low or no startup costs to buy all equipment or software segments. The element gives economic advantages to the two users and service suppliers since it decreases the management cost and in this way lowers the membership cost. Numerous users are, be that as it may, reluctant to buy in to cloud computing services because of security concerns. To empower organization of cloud computing, we have to progress new techniques like secure multi-tenancy, resource isolation should be progressed further.

## 1. Introduction

Cloud Computing is rapidly being embraced by organizations and businesses alike to enable increment to profit edges by diminishing generally speaking IT costs and furnish customers with quicker usage of services. Most of the cloud service suppliers offer multi-tenancy to exploit the related economies of scale which likewise converts into investment funds for the end user. Indeed the aggressive idea of cloud computing is with the end goal that cloud service suppliers need to limit the aggregate cost of ownership of their IT infrastructure, along these lines presenting multi-tenancy is a well-known approach to diminishing aggregate cost of ownership. Nonetheless, multi-tenancy presents an interesting set of security risks, which still can't seem to be completely acknowledged as a major issue by policy creators and cloud service suppliers. This paper will investigate the risks related with multi-tenancy and measures which can be taken to conquer them. Multi-tenancy is the act of putting multiple tenants on the equivalent physical hardware to diminish costs to the user by utilizing economies of scale. Tsai characterizes a tenant as a user in the cloud or a human being [1].

Multi-tenancy has made cloud computing famous by allowing businesses to profit by decreased costs yet keep on accessing data and applications inside a cloud environment. Multi-tenancy is comparable in nature to multiple families in a similar apartment suite. Generally every ha their own space; anyway there is a risk that one family may approach another family's space or information. Wood and Anderson portray multi-tenancy as the capacity to run multiple customers on a solitary software occurrence introduced on multiple servers. In the multi-tenancy model, numerous users' data and resources are situated in a similar computing cloud, and are controlled and recognized using labeling for the extraordinary ID of resources possessed by individual user. In an average multi-tenancy circumstance, the users are the tenants and are furnished with a dimension of control so as to tweak and tailor software and hardware to accommodate their particular needs.

## 2. Multi-Tenancy

Multi-Tenancy is a characteristic consequence of attempting to accomplish economic gain in Cloud Computing by using virtualization and allowing resource sharing. AS characterized before, Multi-Tenancy alludes to resource partaking in Cloud Computing, yet such a definition is as yet general with regards to Cloud Computing, where Multi-Tenancy is seen uniquely in contrast to various service models. In Software as a Service (SaaS), applications are given as a service by the Cloud Service Provider (CSP) where the customer can't screen or control the basic infrastructure; here, Multi-Tenancy implies that at least two customers use a similar service or application given by the CSP paying little mind to the hidden resources. In Infrastructure-as-a-Service (IaaS), where

the customer is fit for provisioning computing, putting away and networking resources and can control yet can't manage the fundamental infrastructure, Multi-Tenancy happens when at least two virtual machines (VMs) having a place with various customers share the equivalent physical machine (PM). Multi-Tenancy has gotten diverse contentions Cloud Computing. While software designers consider it to be a chance, security experts consider it to be vulnerability [2].

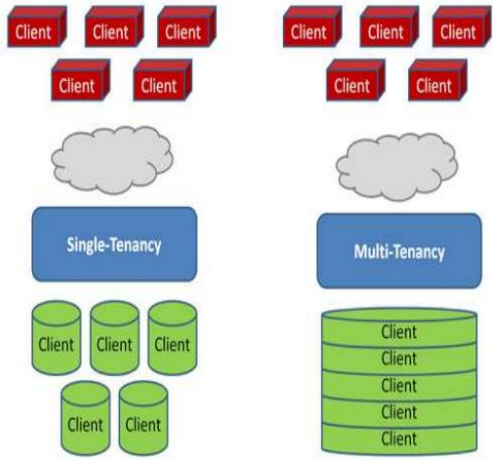


**Figure 1: Single and Multi-tenancy Techniques**

Despite the fact that security experts concur that Multi-Tenancy is a vulnerability that could prompt secrecy being uncovered, they change in giving the answer for such vulnerability. While proposes the end of the virtualization layer so as to avoid multi tenancy, recommends that the supplier should uncover the risk of Multi-Tenancy to the customer and do nothing about it (i.e. give them the choice of paying additional to maintain a strategic distance from Multi-Tenancy). The main strategy appears to be exceptionally powerful, yet would wipe out imperative advantages for Cloud suppliers, for example, VM versatility and monetary benefit because of resource sharing [3]. VM portability is one of these advantages where suppliers can without much of a stretch reallocate VMs to accomplish better use and spare power utilization. Then again, the second strategy won't upgrade the Cloud security and customers particularly undertakings are keeping down interest in Cloud Computing due to security issues. In addition, current routine with regards to UK undertakings is to send Private Clouds so as to cut costs and protect touchy data. We subsequently recognize that an answer anchoring Multi-Tenancy yet keeping its advantages is needed. In this way, a profound understanding of Multi-Tenancy is required so as to recognize all the conceivable advantages conveyed to Cloud Computing as a result of Multi-Tenancy.

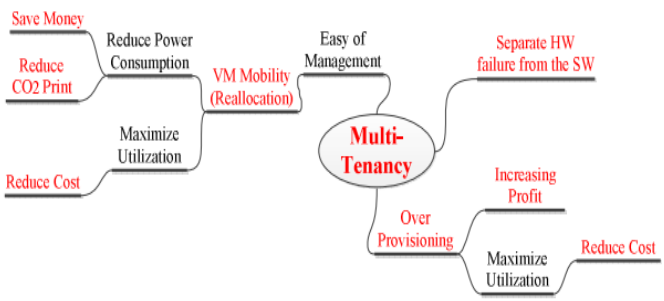


**Figure 1: Multi-Tenancy Benefits' Tree.**

There are basically two type of Multi-tenancy Techniques like:

1. **Virtual Multi-Tenancy:**In this Computing and storage resources are shared among multiple users. Multiple tenants are served from virtual machines that execute simultaneously over a similar computing and storage resources [4].

2. **Organic Multi-Tenancy**: In organic multi-tenancy each part i.e., hardware and software resources in the system design is shared among multiple tenants. In the cloud multi-tenancy ideas are executed in three unique levels of customer incorporation. They are:

- Data centre layer
- Infrastructure layer
- Application layer

### 3. Multi tenancy Security Threats

The essential security issue with multi-tenancy is the specific introduce in which multi-tenancy is based upon; that is, multiple tenants sharing a similar PC hardware. Without a doubt, utilizing a multi-tenancy methodology for the improvement of open cloud infrastructure displays various difficulties as far as consistence, security and protection. One of the principle difficulties of utilizing this type of multiple services is guaranteeing data isolation. Data management is basic as a few users will utilize a similar system however all require security and unhesitatingly. Without a doubt multi-tenancy and absence of network isolation among tenants make the general population cloud powerless against attacks.

Absence of productive bandwidth and traffic isolation makes multi-tenancy in cloud computing helpless, since vindictive tenants may dispatch attacks towards co-inhabitant tenants in a similar cloud data focus. Current approaches to get to control on clouds don't scale well to multi-tenancy prerequisites since they are for the most part based on individual user IDs. By its exceptionally nature multi-tenancy has expanded security risks because of the sharing of software and data by multiple tenants. As these arranged tenants might be contenders, if the hindrances between tenants are separated, one tenant may get to another tenant's data or meddle with their applications. In fact, cloud suppliers are in charge of guaranteeing that one customer can't break into another customer's data and applications [5]. In a multitenant environment side-channel attacks present significant risks in a cloud computing environment. Side channel attacks are based on information got from bandwidth-observing or other comparative techniques. Side channel attacks regularly happen because of absence of approval systems for sharing physical resources. The impedance among tenants exists basically as a result of incognito channels with imperfect access control policies that allow unapproved get to.

To be sure the multi-tenancy design has expanded the risk of database introduction and in this manner, data assurance today is more significant than any other time in recent memory. Another security risk related with multi-tenancy is impedance between tenants on account of tenant outstanding burdens. For instance an over-burden made by one tenant may negatively affect the performance of another tenant. A third, and self-evident, risk of multi-tenancy is resources being doled out to buyers whose personalities, and aims, are obscure. For all intents and purposes all virtualization platforms available today have a trusted virtualization layer that, whenever bargained,

 

drives straightforwardly to full trade off of any of the virtual machines running on the physical host. This could result in the powerlessness to screen activity on the virtual machine, and potentially allowing a vindictive user to adjust the condition of the virtual machine. Virtualization layers are unpredictable software systems. This complexity definitely prompts vulnerabilities, vulnerabilities that could allow a virtual machine user to pick up control of the virtualization layer, and from that point gain control of all other virtual machines running on the equivalent physical host. A fourth security risk natural to multitenant systems is ungraceful change controls and mis-designs. At the point when multiple tenants are sharing the hidden infrastructure it is conceivable that changes may prompt a security rupture allowing one tenant to access another tenant's data or resources. A fifth security risk may result from blended tenant data. To decrease cost, suppliers may store data from multiple tenants in a similar database table-spaces and/or reinforcement tapes. In this situation a data cancellation demand may turn into a test coming about on segments of data not being legitimately erased[6].

**4. Multitenancy Vs Virtualization**

A large portion of the people are accept that the both multi-tenancy and virtualization ideas are same and each can be supplanted in the place of the other. Multi-tenancy is at times confused with virtualization on the grounds that the idea of multiple tenants is like the idea of virtualized examples. The distinctions lie in what is increased inside a physical server going about as a host.

✓ Multi-tenancy: In a multi-tenancy environment, multiple customers share a similar application, running on the equivalent working system, on a similar hardware, with similar data-storage component. The refinement between the customers is accomplished amid application structure, subsequently customers don't share or see each other's data. It empowers every customer application to seem to keep running on a different virtual machine. A physical or virtual server hosting an application is intended to allow usage by multiple diverse users. Every user feels as if they have elite usage of the application [7].

✓ Virtualization: Multiple virtual duplicates of the server environment can be hosted by a solitary physical server. Each duplicate can be given to various users, can be arranged autonomously, and can contain its very own working systems and applications. It empowers every customer application to seem to keep running on a different virtual machine.

**5. Applications Of Multitenancy**

SaaS applications that are intended for the cloud with roots as accomplice database applications normally are multitenant applications. In multitenant applications, data and remaining task at hand can be effortlessly partitioned. You can partition data and outstanding task at hand along tenant limits in light of the fact that most demands happen inside the bounds of a tenant. These SaaS applications deliver a particular software application as a service to their tenants. Tenants can get to the application service and have full ownership of related data put away as a major aspect of the application. Be that as it may, to exploit the advantages of SaaS, tenants must surrender some control over their very own data [8]. They trust the SaaS service supplier to keep their data sheltered and detached from other tenants' data. Instances of this sort of multitenant SaaS application are MYOB, SnelStart and Salesforce.com. Every one of these applications can be partitioned along tenant limits. Applications that give an immediate service to customers or to employees inside an organization (regularly alluded to as users, instead of tenants) are another class on the multitenant application range. Customers buy in to the service and don't claim the data that the service supplier gathers and stores. Service suppliers have less stringent prerequisites to keep their customers' data detached from one another past government-mandated security directions. Instances of this sort of customer-facing multitenant application are media content suppliers like Netflix, Spotify, and Xbox LIVE. Different instances of effectively partition capable applications are customer-facing, Internet-scale applications, or Internet of Things (IoT) applications in which every customer or device can fill in as a partition. Partition limits can isolate users and devices. All applications can't be partitioned along a single property, for example, tenant, customer, user or device. A mind boggling endeavor resource arranging (ERP) application, for instance, has items, requests, and customers. It more often than not has a mind boggling construction with thousands of highly interconnected tables. No single partition strategy can apply to all tables and work over an application's [9].

**6. Benefits Of Multi-Tenancy**

**Lower cost of ownership:** Because all users get to their services from a similar technology platform it is a lot less demanding to get to automatic and incessant updates. Never again need to pay for report customizations or to include new functionalities.

**Effortless limit:** Multi-tenancy gives organizations of all sizes the capacity to live in a similar infrastructure and data focus

**Programming interface Integration versatility:** The integration of Web API is accessible in single-occasions, however in the multi-tenancy environment, explicit solicitations for integrations will presently go into our item guide, and as they wind up accessible, they'll be taken off to all customers [10].

**Access to the latest discharges:** Before, when we wanted to reveal another refresh, it was a protracted procedure since we needed to code the change independently for every customer example to guarantee that it was perfect with their customizations, perform QA, and then put the change into generation. Within excess of 100 customers, it was a tedious errand for our help group. Presently with our multi-tenant environment, on the grounds that each customer's occurrence has a similar base code, the takeoff of new discharges will be exceptionally consistent and give quicker access to imaginative highlights to manage IT and correspondence costs [11].

**Configurable to your own needs:** This capacity gives our customers the capacity to meet their prerequisites and correspondence styles to manage all IT and correspondence costs.

**7. Multi-Tenancy Problems**

**Security:** There is likewise the risk of programmers – regardless of how secure an encryption is with the correct knowledge. A programmer who breaks the encryption of

 

multitenant database will have the capacity to take the data of several businesses who have data put away on it.

**Capacity optimization:** Database managers need the apparatuses and the knowledge to understand which tenant ought to be conveyed on which network so as to expand capacity and diminish costs.

**Service delivery and high accessibility:** When failures happen or when certain services generate anomalous burdens the service delivery can be hindered – yet business customers will regularly ask for high-accessibility. In this way, checking the service delivery and its accessibility is basic to guarantee that the service is appropriately delivered [12].

**Rigid:** Using multi-tenancy qualities of cloud computing, customers can store the data must be put away in servers situated inside France, German customer data inside Germany etc.

## 8. Conclusion

Multi-tenancy is a promising worldview which empowers sharing of a single service case among multiple tenants and additionally leverages benefits for service supplier. Anyway in this procedure of sharing, a few open issues needs to be tended to identify with resource sharing, versatility and security. This proposed overview gives researchers the thought on ebb and flow multitenant systems, promotion and difficulties. In present days all applications are actualized with Multi-tenancy techniques and these applications are utilized in a large portion of the business applications. In this paper we have talked about various type of multitenancy, applications, advantages, advantages and disadvantages of multitenancy in various cloud based service models like SaaS, PaaS and IaaS. In this quickly creating world, cloud technology is exceptionally effective for the advancement of cutting edge software applications. Software as a service (SaaS) is the cloud model for giving applications as a service.

## References


1. Bhaskar Prasad Rimal,Enumi Choi, Ian Lumb, “A Taxanomy and Survey of Cloud Computing System”, Fifth International Joint Conference on INC, IMS and IDC 2009.
2. K. Wood, M. Anderson, " Understanding the complexity surrounding multitenancy in cloud computing ," 2011 Eighth IEEE International Conference on e-Business Engineering, Vol. 1, no. , 119-124, 2011.
3. Abdulrahman, M. Sarfraz, et al, " A Distributed Access Control Architecture for Cloud Computing ," IEEE SOF T WARE, Vol. 12, no. , 36-44, 2012.
4. Z. Chaczko, S. Aslanzadeh, 1st Initial. , " C2EN: Anisotropic Model of Cloud Computing ," 2011 21st International Conference on Systems Engineering, Vol. 11, no. , 467-473, 2011
5. Tim Mather, SubraKumaraswamy, ShahedLatif; , Cloud Security and Privacy, O’Reilly Press, 2009
6. J. Franklin, et al., “Remote detection of virtual machine monitors with fuzzy benchmarking,” SIGOPS Oper. Syst. Rev., April 2008.
7. T. Garfinkel, et al., “Terra: a virtual machine-based platform for trusted computing,” in SOSP, 2003.
8. Stefan Walraven, Tanguy Monheim, Eddy Truyen, WouterJoosen ,Towards Performance Isolation in Multi-tenant SaaS Applications ACM, (2012).
9. Muhammad FahadKhan,etc. An Approach towards Customized MultiTenancyI.J.Modern Education and Computer Science, 2012, 9, 39-44 Published Online September 2012 in MECS www.ramayantiwari.com/wpcontent/uploads/2011/./MultiTenancy.ppt.
10. Scott Chate , Convert your web application to a multi-tenant SaaS solution ,Copyright IBM Corporation 2010.
11. Ahmed E. Youssef ,Exploing Cloud Computing Services and Applications Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 6, July 2012 ISSN 2079-8407
12. The MITRE Corporation, “Common Vulnerability and Exposures (CVE),” http://cve.mitre.org/, Mar. 2011.


 