THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Layered Framework of Multi-Tenancy in Enterprise Level of Cloud Computing For Distribution Access Control

Dr Santosh Kumar Henge
School of Computer Science and Engineering, Lovely Professional University, Punjab, India.
Email: santosh.24372@lpu.co.in, hingesanthosh@gmail.com

Abstract:

The cloud environmental computing will intensely transformed the conveyance of technology based groundwork along with their supportive possessions to the enterprises. The end-users will get the benefits with the cloud based individualities such as on-request based nature-provision, resource-assembling, elasticity-provision along with dynamicity based scaling by the implication of their own enterprise based multi-tenants. Cloud implicated provision suppliers isolate the possessions and end-client's facts into tenants which are used to shield data confidentiality and truthfulness. The maintenance and implication of distribution of secure access control is most priority and complex task in enterprise based multi-tenant cloud environment. The multi-tenancy is the key factor of both public-private-private spaces of secure cloud by implicating with the any one of the cloud service models. This single model cannot be fit into in every environment of enterprise based cloud security. This paper is proposing the three layers framework of multi-tenancy in enterprise level in cloud computing. The three layers considered as Infrastructure based Environmental Service (IaSE), Platform based Environmental Service (PaSE) and Software based Environmental Service (SaSE). This three layer architecture of multi-tenancy has showing the many benefits over multi-instance of environment. This approach is showing many technical feasibilities which can be useful to avoid secure and privacy problems in enterprise based multi-tenant environment.

Keywords: Infrastructure as Service Environment (IaSE), Platform as Service Environment (PaSE) and Software as Service Environment (SaSE), Three Layers Framework (TLF), Enterprise based Multi-Tenancy (EbMT), Multi-Tenancy (MT), Authorization Credentials (AC), Cloud based Service Providers (CbSP).

1. Introduction:

The cloud environmental computing will intensely transformed the conveyance of technology based groundwork along with their supportive possessions to the enterprises. The Tenants are secluded data-containers by implicating with the cluster based precise cybernetic computing settings. Apiece tenant relates to an enterprise, domain of an enterprise and discrete end-users who routines with cloud based facilities by implicating with the confidentiality, truthfulness along with security. It emphasis on-tenant segregation moderates the possibility for association crossways occupants. Which regarded as one of the most important features of cloud computing, The multi-tenancy is an architectural methodology which is implicating by empowering a solitary instance of solicitation to be shared among multiple enterprises or end-users which are considered as tenants. These tenants can primarily implicated with the Software as Service Environment (SaSE). Multi-Tenancy (MT) base applications are principally clustered into three type of end-users. The first clustered is framed with the administrators to end-site clients: the administrators are treated as top-level access controls and the end-site clients treated as the owners of the site. The second clustered is framed with the enterprise-managers level to projects co-ordinators along with end-users at the enterprise level.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Here the enterprise-managers are treated as priority resource persons of the enterprise. The third cluster is framed with the number of end-users whose are more depended on cloud services with or without enhancing the complete secure based knowledge for implementing their technical transactions. In the Enterprise based Multi-Tenancy (EbMT) environment, every technical transactions can be accessible and viewable by the provided secure access controls. The access controls are defer person-to-person, role-to-role, enterprise-to-enterprise and even through cloud-cloud when the data is accessing through distributed cloud environment. The accessible credentials (CAs) will change depends on situation of tenant demands and the time-plan. The cloud based secure pages can be accessible to tenants or end-users depending on their CAs. The tenants are holding their internal capabilities and permissions to modify certain parts of the application such as log-rules, internal tenant access modes and so on. The end-users will get the benefits with the cloud based individualities such as on-request based nature-provision, resource-assembling, elasticity-provision along with dynamicity based scaling by the implication of their own enterprise based multi-tenants [3-4].

2. Paper Objectives:

The Cloud service providers-CSPs isolate possessions in customer's data into occupants to shield their data confidentiality along with truthfulness [4]. The maintenance and implication of distribution of secure access control is most priority and complex task in enterprise based multi-tenant cloud environment. The multi-tenancy is the key factor of both public-private-private spaces of secure cloud [2] by implicating with the any one of the cloud service models. This single model cannot be fit into in every environment of enterprise based cloud security. This paper is proposing the three layers framework of multi-tenancy in enterprise level in cloud computing. The three layers considered as Infrastructure based Environmental Service (IaSE), Platform based Environmental Service (PaSE) and Software based Environmental Service (SaSE).

3. Cloud Computing Environment (CCE) characteristics for Implication of Cloud based Data Access Control Replicas:

In present life scenarios, the CbSPs are using solitary sign-on procedures to attain authentication and modest consent in associated cloud settings but in this type of scenarios the fine-grained consents are characteristically not reinforced. The NASA assimilated RbAC into Nebula [11] a private clustered based cloud systems.

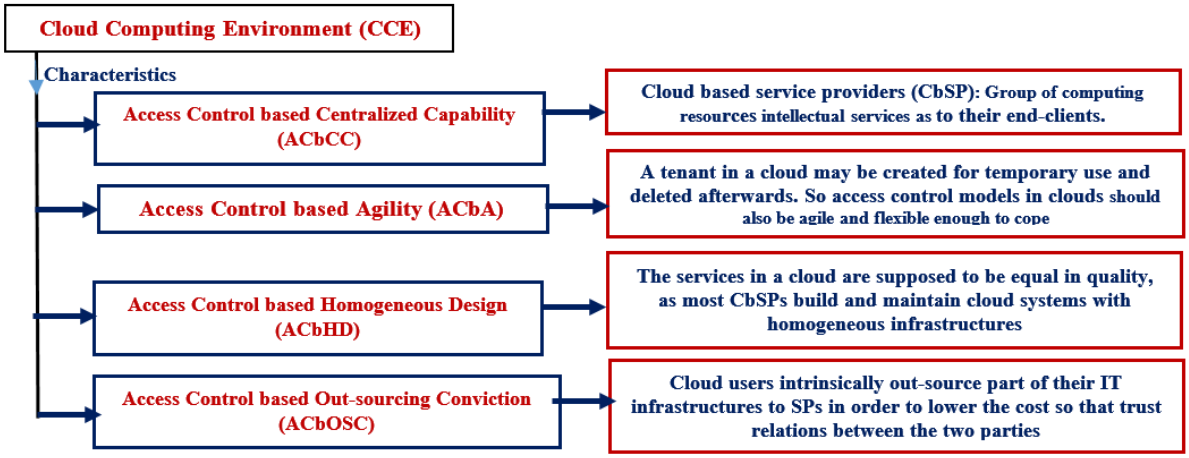


Fig.1 : Cloud Computing Environment (CCE) characteristics for Implication of Cloud based Data Access Control Replicas

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

The traditional environmental RbAC will empowers the fine-grained AC mechanisms (FGACM) in distributed clouds. But, it has deficiencies the capability to achieve secure-associations. The IBM[12] and Microsoft[13] were projected a resource-distribution methodology in data-centric clouds with the implications of database schemas. But this methodology is dedicated to databases and it cannot be flexible to directly apply to supplementary sorts of services. The collaboration implicated models in traditional environmental ACM: RT [14] and dRBAC [15] which are utilize the identifications to steadily transfer between the technical-data-collaborators. Cloud based Data Access Control Replicas will be implicated with the characteristics of CCE such as Access Control based Centralized Capability (ACbCC), Access Control based Agility (ACbA), Access Control based Homogeneous Design (ACbHD) and Access Control based Out-sourcing Conviction (ACbOSC) as shown in the fig.1.

4. Layered based Multi-Tenant testing through Application as Service Environment (AaSE), Software as Service Environment (SaSE), Infrastructure as Service Environment (IaSE) and Network as Service Environment (NaSE):

The software vendors building SaSE applications using a multi-tenant architecture is not at all an easy undertaking. It has holding the many advantages. Multi-tenancy testing is one such highly challenging area. The Multi-Tenant Environment test cases are mainly focuses over the components of Application, Infrastructure and Network.

4.1. Layer1: Software as Service Environment (SaSE):

The SaSE is well-defined as “the capability provided to the consumer to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser and web-based email or a program interface (PI) [5]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings”[5]. The SaSE will be executed with help four levels in Multi-Tenant environment, which are concerning to how the SaSE solicitation is transported to numerous tenants, here the tenants are considered as customers [5-6].

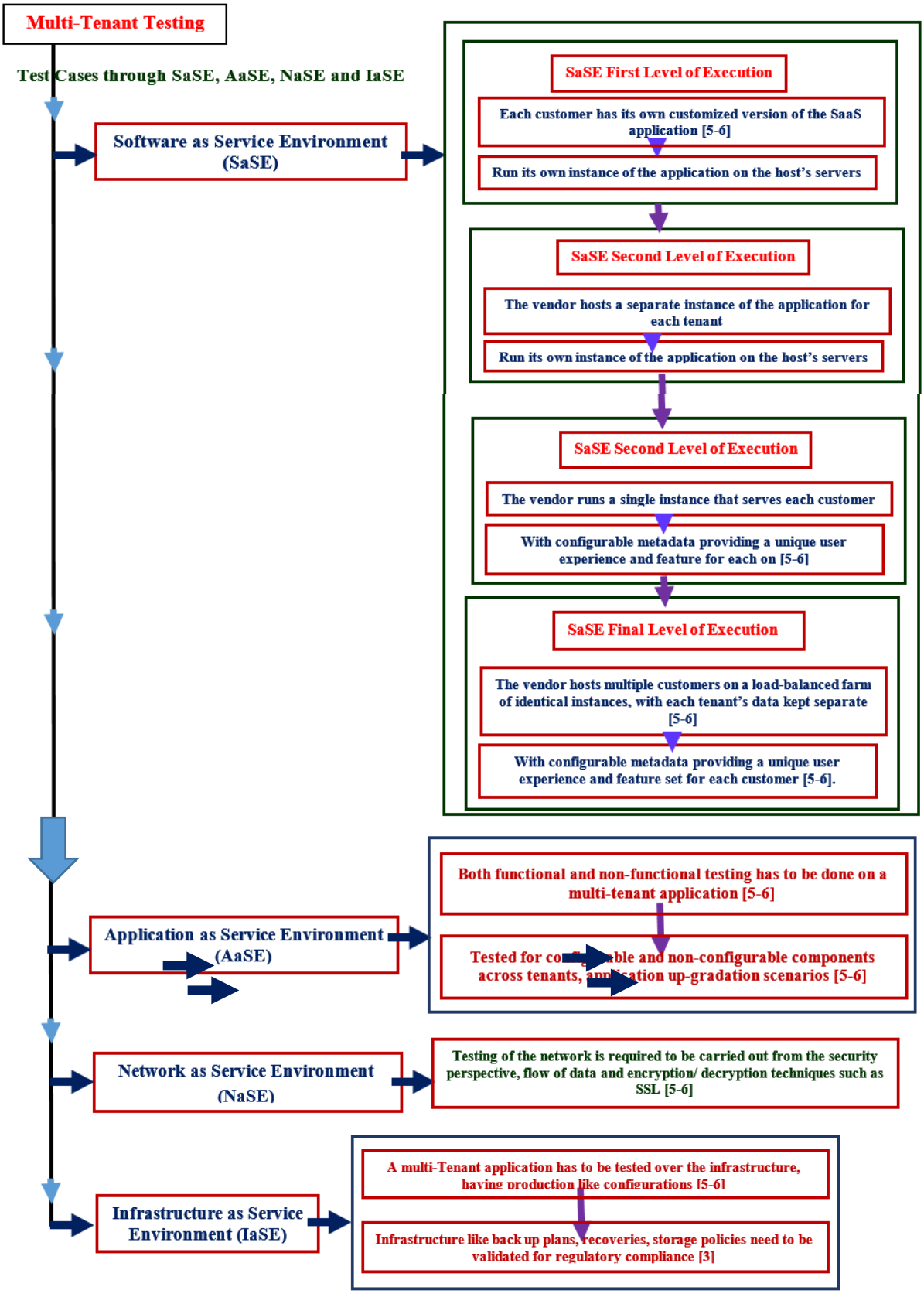
4.2. Layer2: Application as Service Environment (AaSE):

The functional and non-functional testing cases are to be done on MTA. But moving beyond functional and non-functional, a multi-tenant application has to be tested for configurable and non-configurable components across tenants, application up-gradation scenarios. Interface testing, is also essential to perform, as being a MT, it is important to measure the change done for one tenant over other tenants. Multi-tenant application also requires security testing in the form of MT isolation and access privilege, validation for roles and application data.

4.3.Layer3: Network as Service Environment (NaSE):

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Testing of the network is required to be carried out from the security perspective, flow of data and encryption/ decryption techniques such as Secure Socket Layer. The testing also desires to be approved out over different bandwidths to ensure the accessibility of data and its transfer.



ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Fig.2 : Multi-Tenant testing through Application as Service Environment (AaSE), Software as Service Environment (SaSE), Infrastructure as Service Environment (IaSE) and Network as Service Environment (NaSE)

4.4. Layer4: Infrastructure as Service Environment (IaSE):

A multi-Tenant application has to be tested over the infrastructure, having production like configurations, as it is likely to impact the end user experience. Infrastructure like back up plans, recoveries, storage policies need to be validated for regulatory compliance. [3] A foremost fence to the acceptance of cloud IaSE is association which can the numerous tenants involve in collaborative responsibilities necessitating possessions to be collective transversely tenant restrictions [3]. Presently IaSE based CSP emphasis on multi-tenant isolation which can compromised with the imperfect cross-tenant access proficiencies in their APIs of IaSE [3].

5. Conclusion:

The multi-tenancy is the key factor of both public-private-private spaces of secure cloud by implicating with the any one of the cloud service models. This single model cannot be fit into in every environment of enterprise based cloud security. This paper is proposing the three layers framework of multi-tenancy in enterprise level in cloud computing, the considered three layers are IaSE, PaSE and SaSE. The three layer architecture of multi-tenancy has showing the many benefits over multi-instance of environment. This approach is showing many technical feasibilities which can be useful to avoid secure and privacy problems in enterprise based multi-tenant environment.

References:

1. Vivek, Senior Testing Quality Assurance (STQA) resource, net-solutions, last accessed on 20th Aug 2018 https://www.netsolutions.com/insights/multi-tenancy-testing-top-challenges-and-solutions/

2. Daniel Price, "The Challenges of Multi-tenancy" last accessed on 20th Aug 2018 https://cloudtweaks.com/2014/03/challenges-multi-tenancy/

3. Navid Pustchi and Ravi Sandhu, "MT-ABAC: A Multi-Tenant Attribute-Based Access Control Model with Tenant Trust", Springer International Publishing Switzerland 2015 M. Qiu et al. (Eds.): NSS 2015, LNCS 9408, pp. 1–15, 2015. DOI: 10.1007/978-3-319-25645-0 14.

4. Mell, P., Grance, T.: The NIST definition of cloud computing (2011)

5. Avneesh Vashistha, Pervez Ahmed, "SaaS Multi-Tenancy Isolation TestingChallenges and Issues", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-5, pp:49-50, November 2012.

6. 20 F. Chong and G. Carraro, "Architecture Strategies for catching the Long Tail", Microsoft Corporation, http://blogs.msdn.com/gianpaolo,April 2006.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

7. L. Tao. Shifting paradigms with the application service provider model. Computer, 34(10):32–39, 2001.

8. S.Merkel, "Parallels Software as a Service(SaaS)," p.2.

9. Guo C.J. Sun W., Huang Y., Wang Z.H., and Gao B., " A Framework for Native Multi-Tenancy Application Development and Management" proceeding of 9th IEEE International Conference on E-Commerce Technology and the 4th IEEE Conference on Enterprise Computing, E-Commerce and E-Services, 2007, pp. 1-8

10. Mell P, Grance T. The NIST definition of cloud computing. Special Publication 800-145, 2011.

11. McKenty J. Nebula's implementation of role based access control (RBAC). (Available from: http://nebula.nasa.gov/blog/2010/06/03/nebulas-implementation-role-based-access-control-rbac/) [Accessed on 3 June 2010].

12. Chong RF. Designing a database for multi-tenancy on the cloud. (Available from: http://www.ibm.com/developerworks/data/library/techarticle/dm-1201dbdesigncloud/index.html) [Accessed on 26 January 2012].

13. Chong F, Carraro G, Wolter R. Multi-tenant data architecture. (Available from: http://msdn.microsoft.com/en-us/library/aa479086.aspx) [Accessed on June 2006].

14. Li N, Mitchell JC,Winsborough WH. Design of a role-based trust-management framework. Proceedings of the 2002 IEEE Symposium on Security and Privacy, IEEE, Oakland, California, USA, 2002; 114–130.

15. Singhal M, Chandrasekhar S, Ge T, Sandhu R, Krishnan R, Ahn G-J, Bertino E. Collaboration in multicloud computing environments: framework and security issues. IEEE Computer 2013; 46(2):76–84.

16. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. Above the clouds: a Berkeley view of cloud computing. Technical Report, EECS Department, University of California, Berkeley, 2009.