International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V70I9P101

Volume 70 Issue 9, 1-5, September 2022
© 2022 Seventh Sense Research Group®

Review Article

A Brief Study of Risks Associated with Multi-Tenant Software Architecture in Cloud Environment

Praveen Sengar[1], Meetendra Singh Chahar[2], Amit Kohli[3], Abhay Shanker Mudgal[4]

[1,2,3,4]RBS Management Technical Campus, Agra, India

Received: 08 July 2022 Revised: 12 August 2022 Accepted: 23 August 2022 Published: 05 September 2022

Abstract **-** *Cloud computing has acquired a lot of significance in previous years and is growing rapidly. Because of virtual machines, different clients can share one single machine by sharing its database, resources and hardware. Security inside the cloud is of principal significance as the interest and use of cloud computing incrementally. Multi-tenancy particularly acquaints with exclusive security risks with Cloud computing because of more than one tenant using similar actual PC hardware and having similar software and data. Multi-tenancy is a software architecture model which implies a server runs a software instance for each tenant yet serves various tenants. A tenant is an intelligently discrete client or association utilizing a common shared environment. Each tenant has its data access, authorizations, privileges, and permissions. Tenants have imparted admittance to predefined privileges to a particular software occurrence they use. As associations relocate to the cloud and fabricate new cloud-local application stacks, they face numerous accounts and membership tenancies across various cloud suppliers. While there can be security advantages to utilizing separate accounts, such as strong isolation and privilege control capabilities, there are some major Multi-tenancy security issues to know about. The upsides of a multi-tenant software architecture go past productivity and cost savings for your association. Multi-tenant likewise offers significant advantages to clients and end clients. However, gambles, particularly connected with security, should be considered too. This paper examined different risks related to multi-tenant software architecture in the cloud environment.*

Keywords **-** *Multi-tenant, Multi-tenant software architecture, Cloud security, Cloud computing, Virtual machine.*

1. Introduction

Associations and organizations are rapidly embracing cloud computing to assist with expanding net revenues by diminishing IT costs and furnishing clients with quicker execution of services. Multi-tenancy is all about concerned with sharing as far as a cloud environment implies that numerous clients - or tenants - are served by a single instance of an application. While each tenant is physically integrated, they are likewise logically isolated; they share computing resources like configurations, client management rules and data - which the client can somewhat modify. Multi-tenant software architecture is broadly utilized in both public and private clouds. You presumably use or are essentially acquainted with this multi-tenant Software-as-a-Service (SaaS) applications: Google Apps, Microsoft 365, Netflix and Shopify.

Most cloud specialist co-ops offer multi-tenant to exploit the related economies of scale, which converts into reserve funds for the end client. The serious idea of Cloud computing is with the end goal that cloud specialist organizations need to limit the complete expense of responsibility for IT foundation, consequently, presenting multi-tenant is a famous approach to lessening all the cost of proprietorship [7]. Notwithstanding, multi-tenant presents a one-of-a-kind arrangement of safety gambles, which still can't be completely recognized as a difficult issue by strategy creators and cloud specialist organizations [1]. This paper will investigate the risks related to multi-tenant.

2. Related Work

The crucial security issue with Multi-tenancy is the premise on which multi-tenant depend; that is, various tenants have similar PC hardware. To be sure, utilizing a Multi-tenancy approach to improve the public cloud framework presents various difficulties regarding consistency, security and protection. One of the principal difficulties of utilizing this type of different administration is guaranteeing data isolation. The executives' information is basic as a few clients will utilize a similar framework, yet all require security and certainty [1]. To be sure, Multi-tenancy and the absence of organisational detachment among tenants make the public cloud helpless against attacks. The absence of proficient transmission capacity and traffic detachment makes multi-tenant in cloud computing helpless since pernicious tenants might launch attacks on co-resident tenants in similar cloud datacentres [3]. Current ways to deal with cloud access control don't scale well to multi-tenant necessities since they are mostly founded on individual client IDs [4].

In a multi-tenant environment, side-channel attacks present critical risks in a cloud computing environment. Side channel attacks depend on data acquired from transmission capacity observing or other comparable methods. Side channel goes after ordinarily happen because of the absence of approval components for sharing actual resources. The impedance among tenants exists fundamentally due to secret channels with imperfect access control strategies that permit unapproved access [2]. The multi-tenancy architecture has undoubtedly expanded the gamble of data set openness. Subsequently, data protection today is more urgent than at any other time in recent memory. One more security risk related to multi-tenancy is tenants' impedance due to tenant jobs. For instance, an overburden made by one tenant may adversely influence the presentation of another tenant [5]. A third and self-evident chance of Multi-tenancy is resources being relegated to customers whose identities and intentions are obscure.

All virtualization platforms available today have a believed virtualization layer that, whenever split the difference, drives straightforwardly to think twice about any virtual machines running on the actual host [5]. It could bring about the powerlessness to monitor activity on the virtual machine, conceivably permitting a malevolent client to modify the condition of the virtual machine. Virtualization layers are complex software frameworks. This intricacy prompts weaknesses that could permit a virtual machine client to oversee the virtualization layer and, from that point, oversee any remaining virtual machines running on a similar host [6]. The fourth security risk in multi-tenant frameworks is uncoordinated change controls and misconfigurations. When various tenants share the underlying framework, potential changes might prompt a security breach permitting one tenant to access another tenant's information or resources. A fifth security risk might result from co-existed tenant data. Suppliers might store information from various tenants in similar data set table spaces or potentially backup tapes to diminish cost. In this situation, a data detection request might turn into a test on parts of data not being as expected as deleted data.

The resources are ideally utilized in a multi-tenancy cloud; however, it likewise has security challenges; the author has recommended including VM segmentation, database segmentation and VM introspection in a multi-tenant environment to guarantee security [7]. The author examines the security necessities and security issues in medical services multi-tenant cloud framework and recommends upgraded multi-cloud systems will get the vulnerabilities and prevent data loss with access control, audit, flow control, digital signature and numerous others [8]. Multi-tenant presents a security risk in cloud computing specifies hazard and countermeasure related with it sorted into Governance, Control and Auditing Configuration, Design and Change Management, Logical Security, Access Control and Encryption [9]. Approaches, such as Hypervisor and Database segmentation, improve security while getting the multi-tenancy during offering by the cloud service provider [10].

3. Multi-Tenant Software Architecture

Multi-tenancy is a software architecture model which implies that a server runs a single software instance for each tenant yet serves various tenants. A tenant is a legitimately independent client or association utilizing a common environment. Each tenant has its data access, authorizations, privileges, and permissions. Tenants have shared access to predefined privileges to a particular software instance they use. This architecture model is inverse to the single tenant model, which implies that you want to run a different foundation and software instance for each tenant.

Cloud computing uses multi-tenant software architecture to offer a common environment inside public cloud suppliers. The most famous multi-tenant cloud suppliers are Google Cloud, Amazon Web Services (AWS), and Microsoft Azure. The multi-tenant software architecture can be ordered by the level of layers intended to be shared across various tenants. Three key sorts are low, middle, and high degrees.

3.1. High Degree

This multi-tenancy implies that you can share the database and support customized business logic, workflows, and UI layers. Multi-tenant software architecture is presented inside all the sub-layers of SaaS software.

3.2. Middle Degree

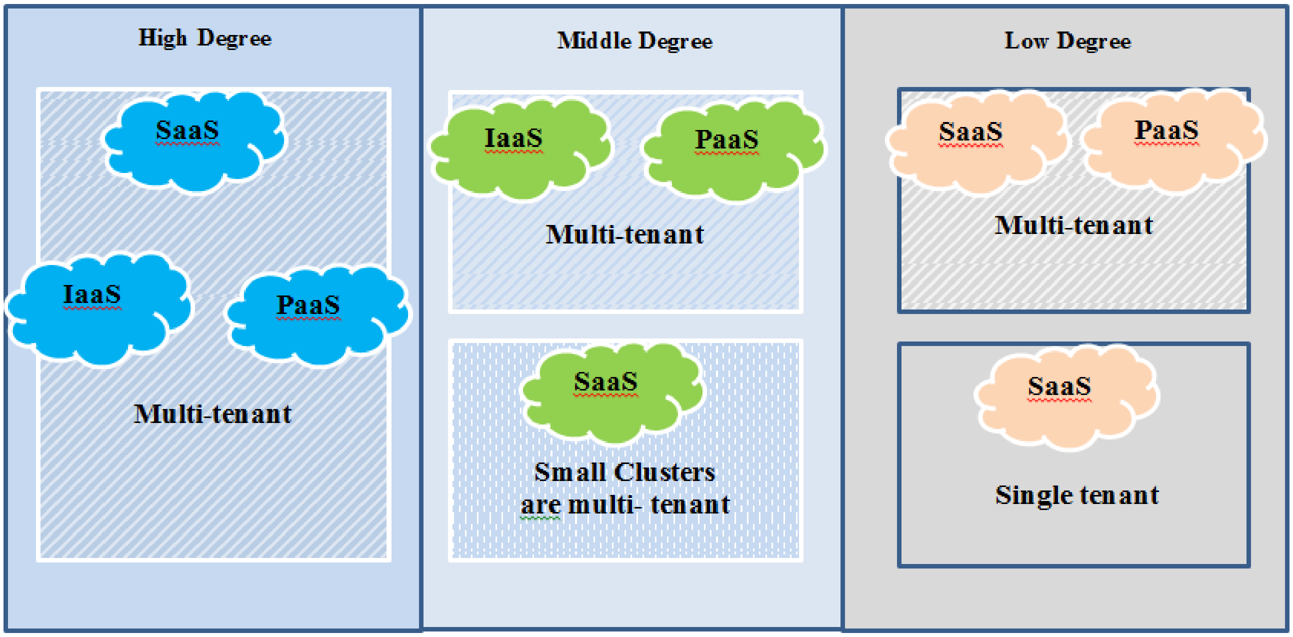
This multi-tenancy in cloud computing suggests that tenants are partitioned into small clusters for application layers and databases. Furthermore, each tenant group has its duplicate of the database and the application instance. As a rule, a middle degree implies that some SaaS clusters are multi-tenant.

3.3. Low Degree

This degree of multi-tenant software architecture is accessible for IaaS and PaaS layers giving devoted SaaS layers to each tenant.

For example, Salesforce.com has above 150,000 clients upheld by 16-24 multi-tenant IaaS/PaaS instances with a 1:5000 proportion. It implies that 5,000 tenants having a similar data set are upheld by a single multi-tenant instance. Thus, it makes Salesforce.com - a high-degree multi-tenant software supplier- a powerful model for the organization as it has cross-industry serviceable workloads. There is nobody size-fits-all methodology when picking the multi-tenant software architecture type for your framework.

Cautiously gain proficiency with the responsibilities, including strategic value, instability, security, etc. Remember that high-degree multi-tenant software architecture is best for cross-industry serviceable workloads.



Source: Ascendixtech.com

Fig. 1 3 Types of Multi-Tenancy in Cloud Computing

4. Risks Associated with Multi-Tenant Software Architecture

In multi-tenant Cloud computing, overseeing and checking information too, as security can represent an extraordinary issue as a similar data set is utilized by different clients. A hacker who gets through the multi-tenant data set would approach every one of the information of numerous businesses who have put away information on it. Next to its downsides, it is profoundly attractive because of its expense-proficient nature. Though in the present time, multi-tenant cloud architecture is the need of great importance to lessen the no. of resources utilized by reusing them. Thus, it helps accomplish usage of the same actual resource, diminishing the expense of cloud service. Notwithstanding, reusable items should be painstakingly overseen and controlled since they can violate confidentiality by the probability of data leaks and prompt different vulnerabilities. Despite data isolation, security breaches like data security, network security, and different issues like customization, reinforcement and reclamation, less transmission capacity and lacking rights to get to the software might prompt sluggish software experience for certain tenants.

4.1. Data Security

A tenant's data should be kept secure from other tenants having a similar shared application. If any tenant's information is hacked, it could also represent a risk to different tenants.

4.2. Network Security

Lack of network isolation among tenants might make the application vulnerable to network attacks like Hacking, DoS (Denial of Service) attack, SQL Injection, and so on.

4.3. Privacy

Each tenant's data should be secret, and only authorised users should have the option to access the data placed with their dataset or table. The current access control methodology is mostly founded on deficient IDs in a multi-tenant cloud. The absence of authorized components can present side-channel attack risks in the multi-tenant cloud environment. Side channel attacks depend on data acquired from power utilization, transmission capacity checking or execution time and other comparative procedures.

4.4. Resource Security

Same resources are utilized by different tenants. Each instance of the resource ought to have the option to play out its work independently and doesn't get to the resource of another tenant.

4.5. Slow Performance

If one tenant utilises more computing power, different tenants will encounter delayed down execution. Utilizing proper tools, one ought to deploy the tenants on the organization wherein they would get the greatest limit and cost decrease. One tenant's heavy service utilisation might affect the quality of service given to different tenants.

4.6. Co-existed Tenant Data

To decrease cost, the Tenants might utilize data storage approaches like the same shared dataset or table divided between numerous tenants. In these cases, deleting or updating the data segments becomes difficult, resulting in data not being deleted or updated appropriately.

4.7. Changing Configurations

Multi-tenant architecture with a single common environment for different tenants might prompt surprising misconfigurations and change management risks. If a single tenant needs setup changes and updates, they might likely cause natural errors for different clients. Due to shared underlying architecture, any changes made by any of the tenants in the arrangements which isn't facilitated among the tenants could prompt a security breach permitting tenant access to other tenants' data.

4.8. Corrupted Data

While multi-tenant clients are isolated from one another at the virtual level, they are genuinely coordinated (sharing hardware, applications and even data). Albeit uncommon, on the off chance that a cloud vendor has an insufficiently designed framework, corrupted data from one tenant could spread to others.

4.9. Co-tenant and External Attacks

Lack of data isolation makes multi-tenant cloud foundations a hands-on target for attacks. A vindictive tenant might send off these attacks - maybe a contender - against co-tenants or by an outside source. Side-channel generally happens due to an absence of authorized controls for sharing actual resources and depends on data gathered from bandwidth monitoring or relative procedures.

4.10. Tenant Workload Interference

If one tenant makes an overburden, it could adversely affect the workload performance for different tenants.

4.11. Mistakenly Assigned Resources

The virtualization layer should become compromised; it gives admittance to any virtual machines running on a similar host and may permit a malicious client to change the setup of the virtual machine. That could bring about a deficiency of observing capabilities.

4.12. Lacking Logical Security Controls

Physical resources are divided among various Tenants. That implies reliance on coherent isolation to guarantee that one tenant purposely can't obstruct the security of different tenants.

4.13. Malicious or Ignorant Tenants

If the supplier has more vulnerable sensible controls between tenants, a malicious or ignorant tenant might diminish the security stance of different tenants. Shared Services can become the cause of failure.

4.14. Uncooperative Change Controls

When various tenants share the basic foundation, all changes should be organized and tested.

4.15. Data Breach Risks

Multi-tenant is about public cloud deployment with a common environment used by different tenants. It implies that every client has explicitly controlled privileges to access a single common dataset with other tenants' data encapsulated. As a matter of fact, this risk is conceivable while using a single common dataset for various tenants. The multi-tenant software architecture prompts higher data breach risks.

4.16. High Downtime Risks

As we've expressed, proficient resource use is one of the multi-tenant software architecture benefits. In any case, this benefit has a possibly basic flipside called downtime. If you haven't laid out an exceptionally versatile architecture, clients may immediately overuse the aggregate sum of resources you give.

5. Conclusion and Future Scope

Multi-tenancy is, to be sure, a twofold edge sword in Cloud computing. The economies of scale acknowledged by multi-tenant frameworks permit the specialist co-op to pass investment funds onto the client, diminishing their generally working expenses. Without a doubt, they are all about the cost of ownership. In any case, by its actual nature, multi-tenant acquaints a remarkable security risk with the cloud computing environment. Multi-tenant design is sought after, and numerous associations utilise it to decrease their endeavours, cost and resources. Security is an extraordinary issue in multi-tenant architecture as services are divided between the customers. It could prompt data loss, misuse or violation and different issues. This paper examined issues like slow performance, privacy, data security, resources divided between tenants, data breaches, etc.

In future, we can diminish data breaches takes a chance by implementing efficient isolation in multi-tenant security models by utilizing data loss prevention systems. Data sharing is likewise a potential weakness of your multi-tenant security model, prompting unauthorized access to delicate information. Implement collaboration controls that empower tracking, controlling, and identifying granular authorizations of shared records. The most common way of overseeing different complex privileges inside your multi-tenant software architecture might become a potential security issue. Bunches of accounts, membership tenures, resources, and service permissions can prompt the over-allocation of privileges across various accounts. AWS organizations and Azure management groups are among the best services.

References

[1] K. Wood, M. Anderson, "Understanding the Complexity Surrounding Multitenancy in Cloud Computing", *Eighth IEEE International Conference on e-Business Engineering*, vol. 1, pp. 119-124, 2011.

[2] A. Abdulrahman, M. Sarfraz, et al., "A Distributed Access Control Architecture for Cloud Computing," *IEEE Soft Ware*, vol. 12, pp. 36-44, 2012.

[3] Z. Feng, B. Bai, et al., " Shrew Attack in Cloud Data Center Networks", *Seventh International Conference on Mobile Ad-hoc and Sensor Networks*, vol. 11, pp. 441-445, 2011.

[4] W. Tsai, Q. Shao, "Role-Based Access-Control Using Reference Ontology in Clouds", *Tenth International Symposium on Autonomous Decentralized Systems*, vol. 11, pp. 121-128, 2011

[5] C. Momm, W. Theilmann, " A Combined Workload Planning Approach for Multi-Tenant Business Applications", *35th IEEE Annual Computer Software and Applications Conference Workshops*, vol. 11, pp. 255-260, 2011.

[6] B. Hay, K. Nance, et al., "Are Your Papers in Order? Developing and Enforcing Multi-Tenancy and Migration Policies in the Cloud", *45th Hawaii International Conference on System Sciences*, vol. 12, pp. 5473-5479, 2012.

[7] Issac Odun-Ayo, Sanjay Misra, Olusola Abayomi-Alli, “Cloud Multi-tenancy: Issues and Developments”, 2017.

[8] R.John Victor and Monisha Singh, “Security Analysis in Multi-Tenant Cloud Computing Healthcare System,” *IJMET*, 2018.

[9] Wayne J. Brown, Vince Anderson, Qing Tan, “*Multitenancy-Security Risks and Countermeasures*”.

[10] C. C. Kalyan Srinivas, S. Sajida, Lokesh, “Security Techniques for Multi Tenanacy Applications in Cloud”, *IJCSMC*, 2013.

[11] [Online]. Available: Ascendixtech.com

[12] Dr. Amit Kumar Chaturvedi, Praveen Sengar, Kalpana Sharma, “Analyzing Resource Allocation Strategies with Elasticity in Multi-Tenant Cloud Environment”, *International Journal of Computer Trends and Technology (IJCTT)* – vol. 67, no. 3, pp. 151-155, 2019.

[13] Mangesh Latekar, Prof. Roshna Ravindran, “Resolving Multi-Tenancy Issues Using Cloud Automation”, *International Journal of Scientific Research & Engineering Trends,* vol. 6, no. 3, pp. 1447-1451, 2020.

[14] Dr. Amit Kr. Chaturvedi, Meetendra Singh Chahar, Dr. Kalpana Sharma, “Analysis on Privacy Preserving and Data Security for Cloud Data Storage”, *International Journal of Computer Trends and Technology (IJCTT),* vol. 60, no. 3, pp. 151-156, 2018.

[15] Vanga Odelu, Ashok Kumar Das, Adrijit Goswami, “A Secure Effective Dynamic Group Password-Based Authenticated Key Agreement Scheme for the Integrated EPR Information System”, *Journal of King Saud University – Computer and Information Sciences,* pp. 68–81, 2016.

[16] Dr.K.Karuppasamy, Ms.F.Margret Sharmila, Tharani .T, "Survey On Cloud Security And Algorithms," *SSRG International Journal of Computer Science and Engineering,* vol. 6, no. 11, pp. 40-42, 2019. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V6I11P108

[17] L. Malina*, J. Hajny, P. Dzurenda and V. Zeman, “Privacy-Preserving Security Solution for Cloud Services”, *Journal of Applied Research and Technology, Science Direct,* vol. 13, no. 1, pp. 20-31, 2015.

[18] D. Chandramohan, T. Vengattaraman, D. Rajaguru, P. Dhavache-lvan, “A New Privacy Preserving Technique for Cloud Service User Endorsement Using Multi-Agents”, *Journal of King Saud University – Computer and Information Sciences,* vol. 28, pp. 37-54, 2016.

[19] Y. A. A. S. Aldeen, M. Salleh, Y. Aljeroudi, “An Innovative Privacy Preserving Technique for Incremental Datasets on Cloud Computing”, *Elsevier, Journal of Biomedical Informatics,* vol. 62, pp. 107-116, 2016.

[20] Jian Wang Yan Zhao Shuo Jiang Jiajin Le, “Providing Privacy Preserving in Cloud Computing”, *IEEE International Conference on Test and Measurement,* pp. 213-216.

[21] N.M. Joseph, E. Daniel, N.A. Vasaanthi, “Survey on Privacy-Preserving Methods for Storage in Cloud Computing”, Amrita International Conference of Women in Computing (AICWIC’13), *International Journal of Computer Applications® (IJCA),* pp. 1-4.

[22] Dr. K. Kartheeban, A. Durai Murugan, “Privacy Preserving Data Storage Technique in Cloud Computing,” *IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing,* 2017.

[23] Mbugua Samuel Thaiya, et al., "On Software Modular Architecture: Concepts, Metrics and Trends," *International Journal of Computer and Organization Trends,* vol. 12, no. 1, pp. 3-10, 2022. *Crossref,* https://doi.org/10.14445/22492593/IJCOT-V12I1P302

[24] Hui Wang, “Privacy-Preserving Data Sharing in Cloud Computing”, Journal of Computer Science and Technology, vol. 25, no. 3, pp. 401-414, 2010.

[25] N. Vurukonda, B.T. Roa, “*A study on Data Storage Security Issues in Cloud Computing*”, Presented in the 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), Published in Elsevier, Procedia Computer Science, vol. 92, pp. 128-135, 2016.

[26] M. B. Jayalekshmi and S. H. Krishnaveni, “A Study of Data Storage Security Issues in Cloud Computing”, *Indian Journal of Science and Technology,* vol. 8, no. 24, pp. 1-5, 2015.

[27] Akhil K.M., Praveen Kumar M, Pushpa B.R, “*Enhanced Cloud Data Security Using AES Algorithm*”, International Conference on Intelligent Computing and Control (I2c2), 2017.

[28] Amit Kumar Chaturvedi, Meetendra Singh Chahar, Kalpana Sharma, “Proposing PDM Model for Securing Data Storage on Cloud Servers”, *International Journal of Engineering and Advanced Technology (IJEAT),* vol. 9, no. 3, pp. 789-793, 2020.