

Resolving Multi Tenancy Issues Using Cloud Automation

Scholar Mangesh Latekar, Prof. Roshna Ravindran

Master of Computer Application
SIES College of Management Studies, Mumbai University
Navi Mumbai,
India mlatekar@gmail.com, roshna.ravindran@siescoms.edu

Abstract – Cloud Computing has gained much importance in past years, and is growing further rapidly. Due to use of virtual machines (virtualization), multiple customers can share one single machine by sharing its hardware, resources and database. This paper discusses the issues involved in multi tenancy cloud environment and suggesting if it can be resolved by using cloud automation.

Keywords – Cloud computing, Multi-tenancy, tenant, security, cloud automation.

I. INTRODUCTION

Cloud Computing can be defined as hosting the servers on internet which can help to better manage the data storage and their processing and decreasing the workload on local server by transferring the workload over the internet.

Cloud Service Providers (CSP) makes the applications and services available online for the customers.

The customers (companies) can access these services of cloud as and when needed by paying for the service for a certain period of time.

Before cloud the companies had to construct and maintain the information management technology and infrastructure. But now, due to cloud companies can use servers, applications etc. according to their needs and hence easily manage and afford them.

Virtual machines are software which provides same functionalities as of physical computers and behaves like a physical computer by running applications and operating system.

Cloud computing is classified into 3 cloud models they are PaaS, IaaS and SaaS.

IaaS (Infrastructure as a Service) provides storage and compute services on demand. It includes services such as operating system, servers and storage.

PaaS (Platform as a Service) provides tools and software for developers to speed up the development, testing and deployment of the application. This includes shared processes, APIs, database management etc.

SaaS (Software as a Service) provides the software application as a service to customers on license. It provides configuration options as well as development environment.

Cloud deployment models include private, public, community and hybrid cloud models.

Private cloud is used by a single organization and is considered to be the most secure model. It is used by

organizations where high data security, management and availability is required.

Public cloud unlike private, is used by multiple organizations and hence it is useful for organizations to store non-sensitive or fluctuating data. Organizations have no control on the location of the infrastructure. Thus, public clouds are considered as less secure than private clouds.

Community Cloud are mutually shared between organizations belonging to particular community. This model is managed and hosted by third party vendor.

Hybrid cloud is combination of private and public clouds .It helps organization to use private cloud for sensitive data and public cloud for non-sensitive data.

II. OBJECTIVE

The primary objective of this study is to gain information about multi tenancy and the issues faced in multi-tenant cloud architecture.

Secondly it sheds light on how cloud automation can help to overcome some of the multi tenancy issues and thus enhance the multi-tenant architecture.

The study aims to project the use of cloud automation to improve the multi-tenant cloud architecture.

III. RELATED WORK

In Reference [1] the author discusses about multi-tenant cloud and suggest using encryption and cryptographic algorithm such as RSA algorithm. It shows how the cloud security is solved by providing an RSA algorithm and also providing security service such as key generation encryption and decryption.

In Reference [2] according to author the resources are optimally used in multi tenancy cloud but it also has security challenges .The author has suggested including VM segmentation, database segmentation and VM

introspection in multi-tenant environment to ensure security.

In Reference [3] the author discusses about the security requirements and security issues in health care multi-tenant cloud system. The author suggested enhanced multi cloud framework will secure the vulnerabilities and prevent data loss. The author suggest framework with access control, audit, flow control, digital signature and many others.

In Reference [4] the author put forward that multitenancy introduces security risk in cloud computing. The author mentions risk and countermeasure associated with it. The counter measure is categorized into Governance, Control and Auditing Configuration, Design and Change Management, Logical security, Access Control and Encryption.

In Reference [5] the author suggests securing the multi tenancy during offering by cloud service provider. The author suggest approaches such as Hypervisor and Database segmentation to enhance security.

IV. SINGLE TENANCY VS MULTI TENANCY

Tenants are group of users or customers sharing the same view of application, including the data they access, configurations, user management and other functions. For example, AWS (Amazon Web Services) offers services or products such as storage and backup, database, website hosting and many others. Companies such as Netflix, LinkedIn, and Facebook are some of the tenants of AWS that is they use AWS services to meet their business needs. In case, if a tenant host their website or online business they too will have no. of tenants.

Thus, tenants must have isolated spaces from other tenants to achieve privacy and security among the individual tenant's data or information.

Single tenancy is providing services to a single customer where only a single customer can have access to the application and the database.

Single tenant cloud computing provides more secure ,reliable set of data as it gives single tenant the access to a single database ,hence it is much flexible to adapt to changes made in its environment. Multi tenancy refers to sharing hardware infrastructure, resources by various tenants belonging to same or different organizations. It provides shared instance of the application to multiple tenants by providing different views to each tenant according to their needs.

In multi tenancy the services are provided to multiple customers wherein multiple customers use the same application instance and also share the same database.

Though separate part of the database is allocated to each customer in multi tenancy, thereby following data isolation and clients may have different levels of access

privileges. In SAAS, multi tenancy is implemented by providing same service or application to multiple customers.

In IAAS, multi tenancy occurs when a same physical machine is shared among two or more virtual machines belonging to different users.

In PASS, multi tenancy is implemented by providing tools and software such as database management, operating system and development tools.

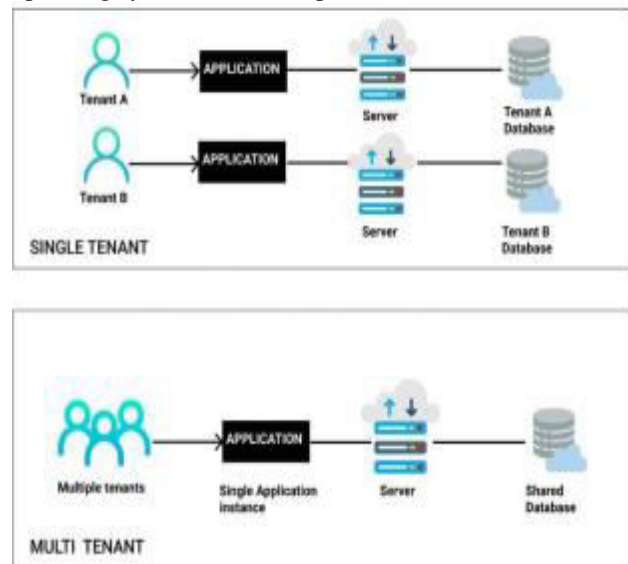


Fig.1. Single tenant vs Multi tenant.

V. MULTI TENANCY IN DIFFERENT KINDS OF CLOUD COMPUTING AND DATA STORAGE

Multi tenancy in public cloud computing is sharing software instance, they store metadata about each tenant and alter the software instance according to tenant's needs. In public cloud multi tenancy Company A shares infrastructure with Company B, that is tenants can share software instance and infrastructure with external organizations. Containers includes everything an application needs in order to run including software, system libraries, system settings, etc.

Multi tenancy in container architecture is obtained by running multiple containers created by different customers in a single host machine.

Server-less computing is a model where the application broken into functions which runs on demand. This model is also called as FAAS (Function as a service).

In multi tenancy server-less provider will be running the code from several customers on a single server at any given point, as tenants are not assigned discrete physical servers.

In private cloud computing, multi tenancy is obtained by sharing applications, software instance, and infrastructure within the organization. For example, various

departments, teams or branches of an organization shares the same infrastructure.

1.Data Storage in Multi tenancy

There are several choices to share storage among the tenants. The following are ways data can be stored in multi-tenant architecture

1.1Separate database server for every tenant:

Every user in this model has its own database server and hence the tenants are isolated from each other. This approach is expensive and is not practical because for 1Lakh tenants 1 lakh database server is impractical.

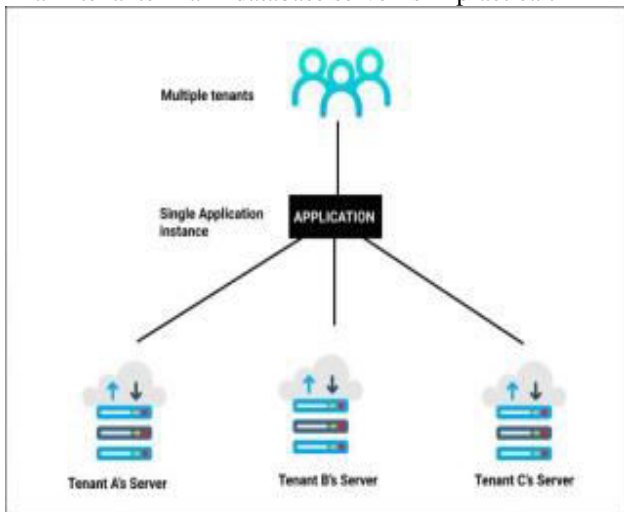


Fig.2.Separate database server for every tenant.

1.2Separate database per tenant:

Separate database is given to each tenant on same server, that is same sever is shared by multiple tenants. This approach is also impractical and expensive.

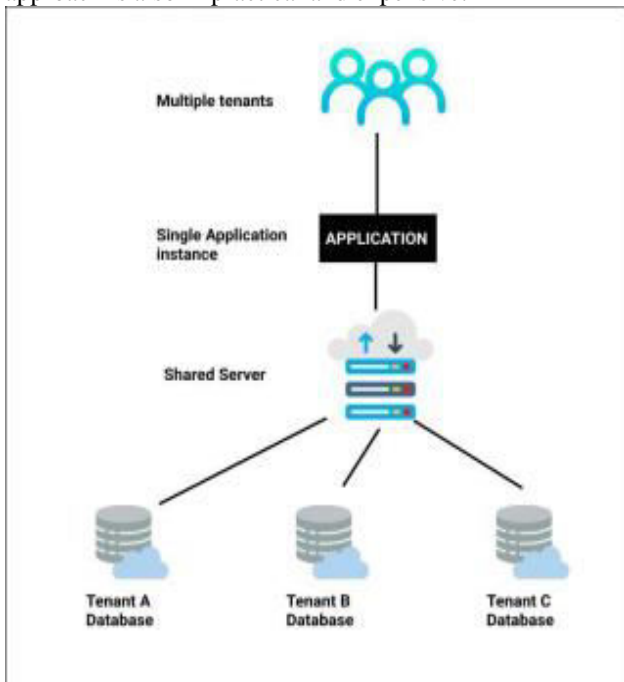


Fig.3.Separate database per tenant.

1.3Table per tenant:

This approach is better than previous approaches and is cost efficient. Each tenant has a separate table shared on common database though separate schemas are created for every tenant. Factors such as data isolation and security must be of more focus in this approach. However large number of tables must be kept and managed.

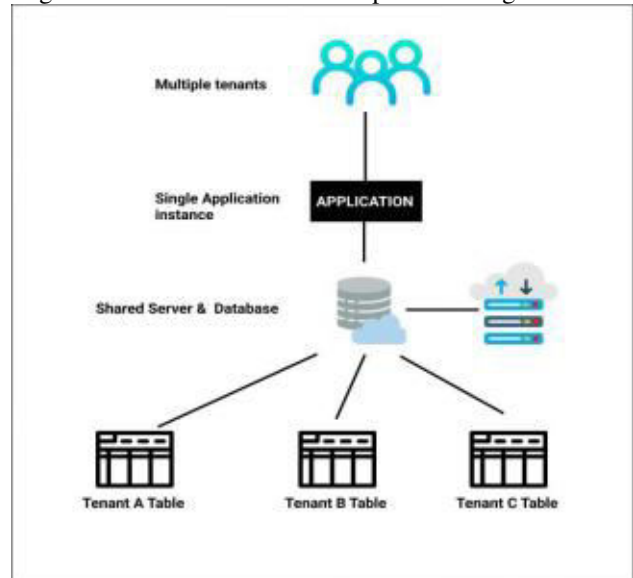


Fig.4.Table per tenant.

1.4Table shared among tenants:

In this approach there is a common table shared among multiple tenants. This model provides common schema for all the tenants. It is efficient approach in terms of cost and hardware use. Disadvantage of this schema is sharing same schema among tenants may pose security issues.

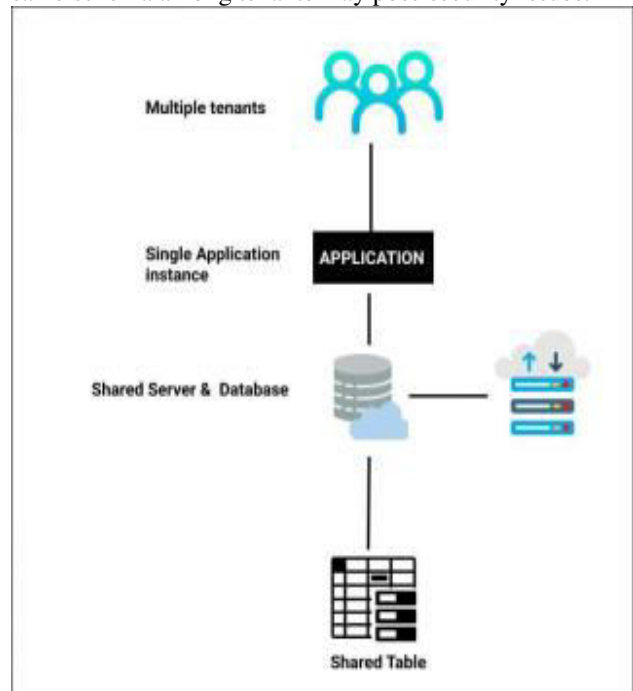


Fig.5.Table shared among tenants.

VI. MULTI-TENANT CLOUD ISSUES

In multi-tenant cloud computing managing and monitoring data as well as security can pose a great problem as the same database is used by multiple customers. A hacker who breaks through the multi-tenant database would have access to all the data of multiple business who have stored data on it.

Beside its drawbacks it is highly desirable due to its cost efficient nature. Whereas in today's era, multi-tenant cloud architecture is the need of the hour to reduce the no. of resources used by reusing them. Hence, it helps achieving utilization of same physical resource, reducing the cost of cloud service.

However, reusable objects must be carefully managed and control since they can violate confidentiality by possibility of data leak and can lead to other vulnerabilities.

Despite data isolation, security breach such as data security, network security, and other problems such as customization, backup and restoration, less bandwidth and insufficient rights to access the software may lead to slow software experience for some tenants.

1. Data Security

Data of a tenant must be kept secure from other multiple tenants sharing the same application. If any one of the tenant's data is hacked then it might pose a risk to other tenants also.

2. Network Security

Lack of network isolation among tenants may make the application vulnerable to network attacks such as Hacking, DOS (Denial of service) attack, SQL Injection, etc.

3. Confidentiality

Data of each tenant must be confidential and only the authorized person should be able to access the data belonging to their database or table. Current approach for access control are mostly based on IDs which are insufficient in multi-tenant cloud.

Lack of authorization mechanism can pose side channel attack risks in multi-tenant cloud environment. Side channel attacks are based on information gained from power consumption, bandwidth monitoring or execution time and other similar techniques.

4. Resource Security

Same resources are been used by multiple tenants and each instance of the resource should be able to perform its work independently and does not access the resource of other tenant.

5. Slow Performance

If one tenant is using more amount of computing power, the other tenants would experience slow down performance. Using appropriate tools one should deploy

the tenants on the network in which they would get maximum capacity and cost reduction

6. Comingled Tenant Data

To reduce cost, the tenants may use data storage approaches such as using same shared database or table shared among multiple tenants. In these cases, deleting or updating on requested portions of the data becomes challenging thus resulting in data not deleted or updated properly.

7. Changing Configurations

Due to shared underlying architecture, any changes made by any of the tenants in the configurations which is not coordinated among the tenants could lead to security breach allowing tenant to gain access to other tenant's data.

Cloud Automation can help provide solution and security to the multi-tenant architecture.

VII. CLOUD AUTOMATION

Cloud automation is reducing the manual efforts and automating tasks such as managing and deployment of workloads, creating storage unit, server and Virtual machine configurations, scaling of resources, etc.

Cloud automation enables cloud service providers to automatically create, modify and distribute resources. Cloud automation is not build on top of cloud it requires use of specialized tools.

Cloud automation can be achieved by using orchestration and automation tools that run on top of virtual machines.

Orchestration is converting steps and processes of managing and deploying of workload in coded form and automation is implementing this steps automatically without human intervention.

Using cloud automation helps improve security by minimizing human errors and automating sensitive tasks.

It also automates the backup process to improve organization's resistance to disaster, equipment failure or cyber-attack. Hence cloud automation helps to better control the infrastructure and resources of the organization. These benefits of cloud automation could also be useful in multi-tenant cloud environment.

Some of the Cloud automation features which can improve multi-tenant performance

1. Workload Management

Cloud Automation helps in workload management and their deployment automatically by adding or removing the containers to balance work load which can be used in multi-tenant architecture to remove issue such as slow down performance.

2. Access Management

Using automation tools to manage user permissions, passwords and roles, configuring access permissions

based on roles and regular password expiration would act as barrier to access sensitive data.

3. Monitoring

Using automated tools to monitor your application working and network traffic, to find and log suspicious activity, detect vulnerabilities, network configuration flaws, adding random check points in the application and alert the tenant about it. Automated tools can help to monitor the application 24X7.

4. Resource Management

Cloud automation tools provides container resource management solution, optimizing resources, allows application to find cloud resources that match their resource needs.

5. Drift Detection

Automation tools helps to detect drift in the configurations and prevent them automatically by restoring the suspicious changes made in the configuration.

VIII. CONCLUSION

Multi-tenant architecture is in demand and many organizations are using it to reduce their efforts, cost and resources. Security can pose a great issue in multi-tenant architecture as services are shared among the consumers. It could lead to data loss, misuse or violation and other issues. Cloud automation can help to overcome these security issues by automating them. Issue such as slow performance cloud be solved by automation of workload management. Confidentiality and data security issues can be solved to some extent by implementing automation tools for monitoring, access-management and drift detection to find any suspicious changes. Resources shared among multiple tenants can be better managed by using automation tools for resource management. Thus, Cloud automation could provide solutions to overcome issues in multi-tenant architecture.

REFERENCES

- [1]. Manjinder Singh, and Charanjit Singh, "Multi tenancy Security in Cloud Computing," IJESRT, March
- [2]. Issac Odun-Ayo, Sanjay Misra, Olusola Abayomi-Alli, "Cloud Multi- tenancy: Issues and developments", Dec 2017.
- [3]. R. John Victor and Monisha Singh "Security Analysis in Multi tenant cloud computing healthcare system," IJMET, March 2018.
- [4]. Wayne J. Brown, Vince Anderson, Qing Tan, "Multitenancy-Security risks and countermeasures".
- [5]. C.C. Kalyan Srinivas, S. Sajida, Lokesh, "Security Techniques for multi tenancy applications in cloud", IJCSMC, August 2013.
- [6]. Website <https://searchcloudcomputing.techtarget.com/definition/cloud-automation>
- [7]. Website <https://cloud.netapp.com/blog/cloud-automation-why-where-and-how-cvo-blg>
- [8]. Website <https://dzone.com/articles/multi-tenancy-after-10-years-of-cloud-computing>
- [9]. Website <https://cloudcheckr.com/cloud-automation/automating-cloud-security-frees-your-it-team-to-focus-on-what-they-do-best/>