**What is Multi-Tenancy in Cloud Computing?**

Multi-tenancy in cloud computing means that many tenants or users can use the same resources. The users can independently use resources provided by the cloud computing company without affecting other users. Multi-tenancy is a crucial attribute of cloud computing. It applies to all the three layers of cloud, namely infrastructure as a service (IaaS), Platform as a Service (PaaS), and software as a Service (SaaS).

The resources are familiar to all the users. Here is a banking example to help make it clear what multi-tenancy is in cloud computing. A bank has many account holders, and these account holders have many bank accounts in the same bank. Each account holder has their credentials, like bank account number, pin, etc., which differ from others.

All the account holders have their assets in the same bank, yet no account holder knows the details of the other account holders. All the account holders use the same bank to make transactions.

**Multi-Tenancy Issues in Cloud Computing**

Multi-tenancy issues in cloud computing are a growing concern, especially as the industry expands. And big business enterprises have shifted their workload to the cloud. Cloud computing provides different services on the internet. Including giving users access to resources via the internet, such as servers and databases.Cloud computing lets you work remotely with networking and software.

There is no need to be at a specific place to store data. Information or data can be available on the internet. One can work from wherever he wants. Cloud computing brings many benefits for its users or tenants, like flexibility and scalability. Tenants can expand and shrink their resources according to the needs of their workload. Tenants or users do not need to worry about the maintenance of the cloud.

Tenants need to pay for only the services they use. Still, there are some multi-tenancy issues in cloud computing that you must look out for:

**Security**

This is one of the most challenging and risky issues in multi-tenancy cloud computing. There is always a risk of data loss, data theft, and hacking. The database administrator can grant access to an unauthorized person accidentally. Despite software and cloud computing companies saying that [client data is safer](https://rivalime.com/web-application-security-testing-checklist/) than ever on their servers, there are still security risks.

There is a potential for security threats when information is stored using remote servers and accessed via the internet. There is always a risk of hacking with cloud computing. No matter how secure encryption is, someone can always decrypt it with the proper knowledge. A hacker getting access to a multitenant cloud system can gather data from many businesses and use it to his advantage. Businesses need high-level trust when putting data on remote servers and using resources provided by the cloud company to run the software.

The multi-tenancy model has many new security challenges and vulnerabilities. These new security challenges and vulnerabilities require new techniques and solutions. For example, a tenant gaining access to someone else’s data and it’s returned to the wrong tenant, or a tenant affecting another in terms of resource sharing.

**Performance**

SaaS applications are at different places, and it affects the response time. SaaS applications usually take longer to respond and are much slower than server applications. This slowness affects the overall performance of the systems and makes them less efficient. In the competitive and growing world of cloud computing, lack of performance pushes the cloud service providers down. It is significant for multi-tenancy cloud service providers to enhance their performance.

**Less Powerful**

Many cloud services run on web 2.0, with new user interfaces and the latest templates, but they lack many essential features. Without the necessary and adequate features, multi-tenancy cloud computing services can be a nuisance for clients.

**Noisy Neighbor Effect**

If a tenant uses a lot of the computing resources, other tenants may suffer because of their low computing power. However, this is a rare case and only happens if the cloud architecture and infrastructure are inappropriate.

**Interoperability**

Users remain restricted by their cloud service providers. Users can not go beyond the limitations set by the cloud service providers to optimize their systems. For example, users can not interact with other vendors and service providers and can’t even communicate with the local applications.

This prohibits the users from optimizing their system by integrating with other service providers and local applications. Organizations can not even integrate with their existing systems like the on-premise data centers.

**Monitoring**

Constant monitoring is vital for cloud service providers to check if there is an issue in the multi-tenancy cloud system. Multi-tenancy cloud systems require continuous monitoring, as computing resources get shared with many users simultaneously. If any problem arises, it must get solved immediately not to disturb the system’s efficiency.

However, monitoring a multi-tenancy cloud system is very difficult as it is tough to find flaws in the system and adjust accordingly.

**Capacity Optimization**

Before giving users access, database administrators must know which tenant to place on what network. The tools applied should be modern and latest that offer the correct allocation of tenants. Capacity must get generated, or else the multi-tenancy cloud system will have increased costs. As the demands keep on changing, multi-tenancy cloud systems must keep on upgrading and providing sufficient capacity in the cloud system.

Multi-tenancy cloud computing is growing and growing at a rapid pace. It is a requirement for the future and has significant potential to grow. Multi-tenancy cloud computing will keep on improving and becoming better as large organizations are looking.