CLOUD COMPUTING APPLICATIONS IN MULTI-TENANCY

Sukhwinder Kaur

Assistant Professor
Computer Science and Application
JB Institute of Technology, Dehradun , India

Abstract: Cloud computing has enabled businesses to infinitely scale services based on demand while reducing the total cost of ownership. It provides a multitenant feature that enables an IT asset to host multiple tenants, improving its utilization rate. The feature provides economic benefits to both users and service providers since it reduces the management cost and thus lowers the subscription price. Security concerns are mainly driven by the Multi-Tenancy situation which refers to resource sharing in Cloud Computing and its associated risks where confidentiality and/or integrity could be violated. As a result, security concerns may harness the advancement of Cloud Computing in the market. So, in order to propose effective security solutions and strategies a good knowledge of the current Cloud implementations and practices, especially the public Clouds, must be understood by professionals. To cope with that, this paper introduces techniques, with which it identifies technical issues on enabling multi-tenancy.

IndexTerms **– Saas,Iaas,Paas,Multi-Tenancy**

I. INTRODUCTION TO CLOUD COMPUTING

Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through cloud services platform via the internet with pay-as-you-go pricing. A cloud is a combination of hardware, networks storage, services, and interfaces that helps in delivering computing as a service.

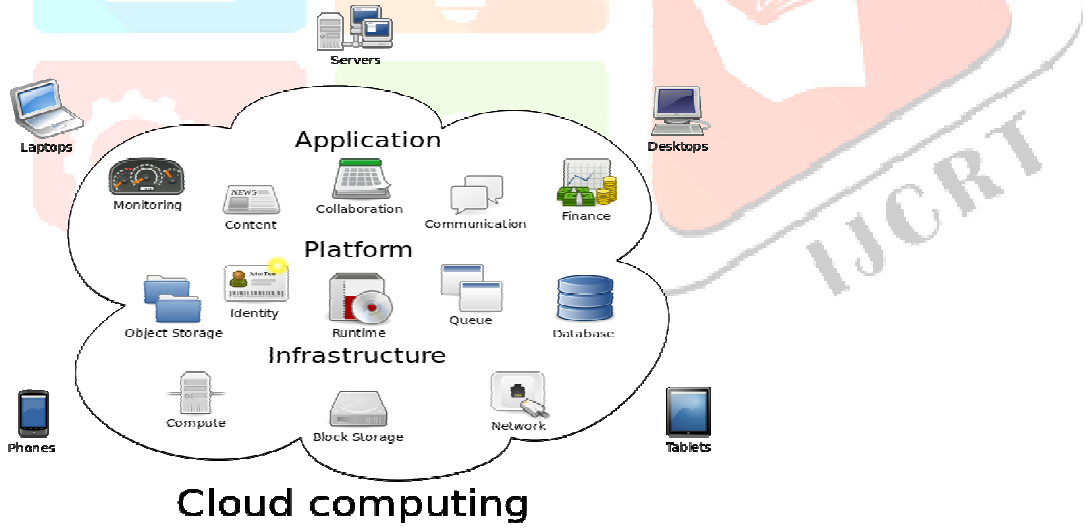

Figure -1
Cloud computing metaphor: the group of networked elements providing services need not be individually addressed or managed by users; instead, the entire provider-managed suite of hardware and software can be thought of as an amorphous cloud.

II. LITERATURE REVIEW

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another. Knowing what they are and how they are different makes it easier to accomplish your business goals.

- **INFRASTRUCTURE-AS-A-SERVICE (IAAS)**

The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

- **PLATFORM AS A SERVICE (PAAS)**

Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

- **SOFTWARE AS A SERVICE (SAAS)**

Software-as-a-service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

Although cloud computing has changed over time, it has been divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

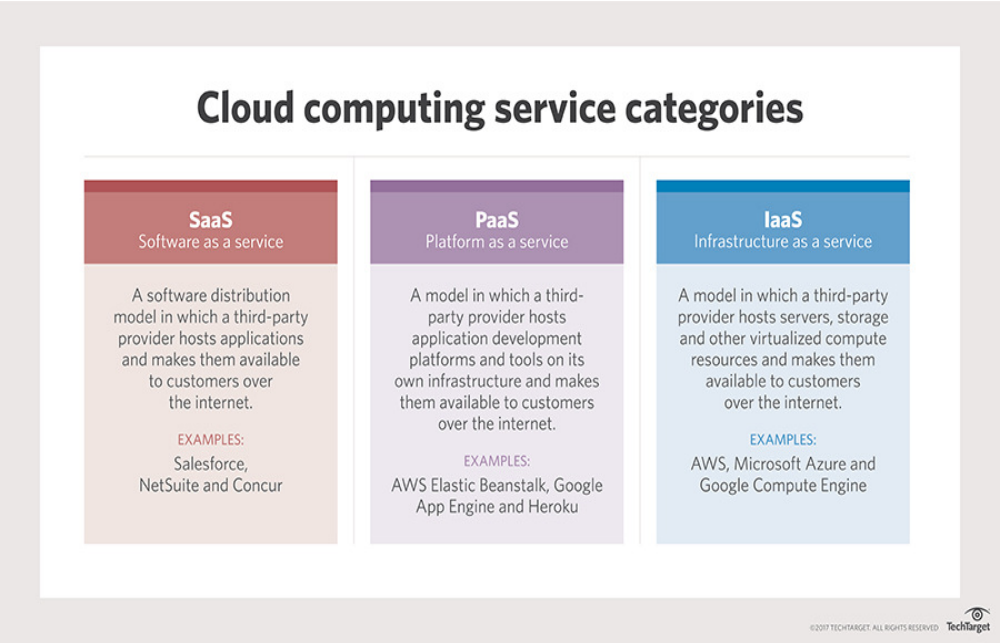

Figure-2

III. MULTITENANT TECHNOLOGY

The multitenant application design was created to enable multiple users (tenants) to access the same application logic simultaneously. Each tenant has its own view of the application that it uses, administers, and customizes as a dedicated instance of the software while remaining unaware of other tenants that are using the same application.

Multitenant applications ensure that tenants do not have access to data and configuration information that is not their own. Tenants can individually customize features of the application, such as:

- *User Interface* - Tenants can define a specialized "look and feel" for their application interface.
- *Business Process* - Tenants can customize the rules, logic, and workflows of the business processes that are implemented in the application.
- *Data Model* - Tenants can extend the data schema of the application to include, exclude, or rename fields in the application data structures.
- *Access Control* - Tenants can independently control the access rights for users and groups.

Multitenant application architecture is often significantly more complex than that of single-tenant applications. Multitenant applications need to support the sharing of various artifacts by multiple users (including portals, data schemas, middleware, and databases), while maintaining security levels that segregate individual tenant operational environments.

Common characteristics of multitenant applications include:

- *Usage Isolation* - The usage behavior of one tenant does not affect the application availability and performance of other tenants.
- *Data Security* - Tenants cannot access data that belongs to other tenants.
- *Recovery* - Backup and restore procedures are separately executed for the data of each tenant.
- *Application Upgrade* - Tenants are not negatively affected by the synchronous upgrading of shared software artifacts.
- *Scalability* - The application can scale to accommodate increases in usage by existing tenants and/or increases in the number of tenants.
- *Metered Usage* - Tenants are charged only for the application processing and features that are actually consumed.
- *Data Tier Isolation* - Tenants can have individual databases, tables, and/or schemas isolated from other tenants. Alternatively, databases, tables, and/or schemas can be designed to be intentionally shared by tenants.

A multitenant application that is being concurrently used by two different tenants is illustrated in Figure 5.11. This type of application is typical with SaaS implementations.

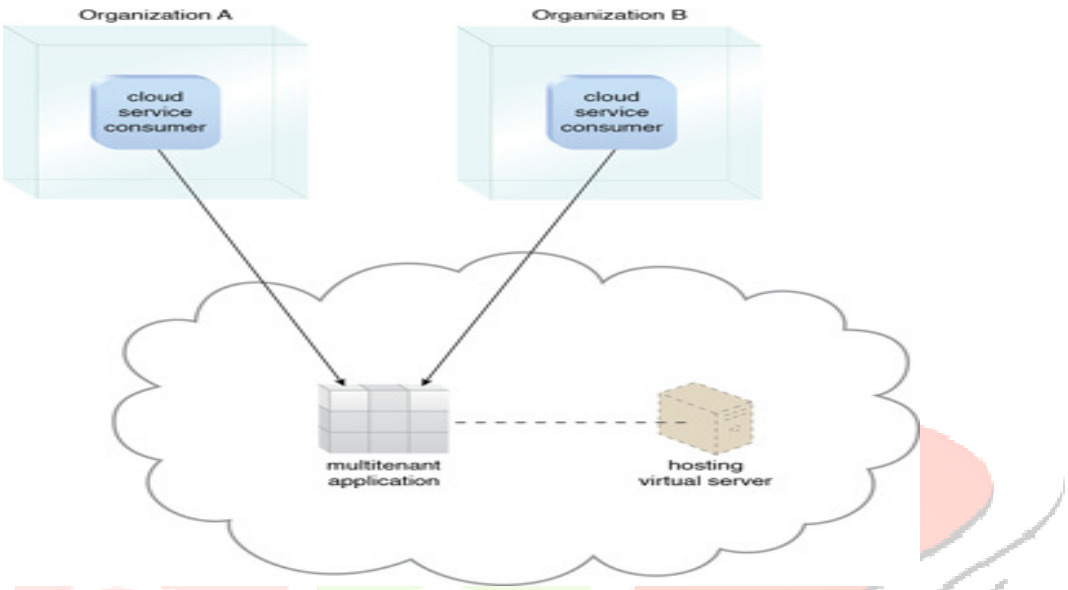

Figure 3 - A multitenant application that is serving multiple cloud service consumers simultaneously

IV. MULTITENANCY VS VIRTUALIZATION

Multitenancy is sometimes mistaken for virtualization because the concept of multiple tenants is similar to the concept of virtualized instances.

The differences lie in what is multiplied within a physical server acting as a host:

- With virtualization: Multiple virtual copies of the server environment can be hosted by a single physical server. Each copy can be provided to different users, can be configured independently, and can contain its own operating systems and applications.
- With multitenancy: A physical or virtual server hosting an application is designed to allow usage by multiple different users. Each user feels as though they have exclusive usage of the application.

V. SECURITY ISSUE: MULTI-TENANCY

Multitenancy is a major concern in cloud computing Multi-tenancy occurs when various consumers using the same cloud to share the information and data or runs on a single server. Multi-Tenancy in Cloud Computing occurs when multiple consumers share the same application, running on the same operating system, on the same hardware, with the same data-storage system and both the attacker and the sufferer are sharing the common server

.**Architecture**: This architecture fully separates your information from other customer's information while allowing us to roll out rapidly the latest functionality to each, all at once. This approach offers the most configurability and allows you to extract deep insight from your information Oracle delivers a latest Multitenant architecture that allows a multitenant container database to grasp numerous pluggable databases. An existing database can simply be adopted with no application changes necessary.

VI. ISSUES IN SERVICES OF CLOUD COMPUTING

- ***SaaS Security Issues***: In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors).Web application security miss-configuration and breaking-web

application security miss-configuration or weaknesses in application-specific security controls is an important issue in. Security miss-configuration is also very critical with multi-tenancy where each tenant has their own security configurations that may conflict with each other leading to security holes. It is mostly recommended to depend on cloud provider security controls to enforce and manage security in a consistent, dynamic and robust way

- ***Paas Security Issues***: SOA related security issues–the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks. Mutual authentication, authorization and WS-Security standards are important secure the cloud provided services. This security issues shared responsibility among cloud providers, service providers and consumers.
- ***IaaS Security Issues***: VM security–securing the VM operating systems and workloads common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud-oriented security solutions. Virtual network security-sharing of network infrastructure among different tenants within thesame server (using vSwitch) or in the physical networks will increase the possibility to exploit vulnerabilities in DNS servers, DHCP, IP protocol vulnerabilities, or even the vSwitch software which result in network-based VM attacks. Securing VM boundaries-VMs have virtual boundaries compared with to physical server ones. VMs that co-exist on the same physical server share the same CPU, Memory, I/O, NIC, and others (i.e. there is no physical isolation among VM resources). Securing VM boundaries is the responsibility of the cloud provider.

VII. CONCLUSION

This paper discussed the architecture of cloud computing. It also addressed challenges and issues of cloud computing in detail. In spite of the several limitations and the need for better methodologies processes, cloud computing is becoming a hugely attractive paradigm, especially for large enterprises. Cloud Computing initiatives could affect the enterprises within two to three years as it has the potential to significantly change IT.

VIII. REFERENCES

1. Venkata Sravan Kumar Maddineni & Shivashanker Ragi (2011), Security Techniques for Protecting Data in Cloud Computing.
2. Garima Gupta,P.R Laxmi & Shubhanjali Sharma, A Survey of Cloud Security Issues and Techniques.
3. Santosh Kumar and R.H Gaudar, Cloud Computing-Research Issues, Challenges, Architecture, Platform, and Applications: A Survey.
4. Varsha, A Study of Security Issues in Cloud Computing