Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 5, April-2019, ISSN 2230-7540

A Study on Muti-Tenancy Approaches with Its Application for the Issues in Cloud Computing Models

Dipti Prava Sahu[1]* Dr. B. L. Raina[2]

[1] Research Scholar, Computer Science & Engineering, Glocal University, Uttar Pradesh

[2] Professor, Computer Science & Engineering, Glocal University, Uttar Pradesh

Abstract – Cloud Computing is becoming a standard in the IT computational model, cloud protection is becoming a major issue in the implementation of the Cloud, where security is perceived to solitary of the most significant issues for Cloud's large customers (i.e. governments and businesses). The Multi-Tenancy case, which relates to the sharing of resources in cloud computing and its related risks wherever confidentiality and/or reputation could be infringed, is driving such a legitimate problem. This paper provides a inclusive review of existing literature using reliable methods on relevant issues and developments linked to cloud multi-tenancy. Multi-tenance is a key feature in cloud computing. which enables the use of a single resources by multiple user from different places. Multi–tenancy has unique architecture based on the data or multi – tenant application. Cloud service suppliers could provide security for all elements of their services (i.e. IaaS and SaaS) with multi-tenance. Before all this, Multi-Tenancy will have a clear understanding, its roots and its benefits. A creative way to handle Multi-Tenancy will also be demonstrated.

Keywords – Cloud computing; Security Issues; Multi-Tenancy; Multi-Tenant Characteristics

----------X----------

INTRODUCTION

Cloud computing (CC) including the National Institute of Science and Technology (NIST) is described as a model that allows easy and pervasive access to a collective group of extensible computing resources which can be quickly set up or torn down on consumer demand with little interference from the service provider[1]. CC resources might be at hardware level: Infrastructure-As-A-Service (IAAS), at the software level: Software-As-A-Service (SAAS) or at a developer level: Platform-As-A-Service (PAAS) and deployed either as a private, public, community or hybrid model. In the IAAS model, hardware resources can be instantly allocated or released to customers through the use of Virtual Machines [2]. Automated resource allocation techniques such as Amazon's Elastic Cloud Compute are used by Cloud providers to achieve this [2]. Furthermore, easy management and better resource utilization are achieved by hosting multiple customers on the same Physical Machine (PM) using VMs. This is known as Multi-tenancy. CC and related technologies are advancing at such a drastic rate and will continue to impact the Information Technology world for many more years. Cloud Service Providers (CSPs) are improving their services while Cloud users continue to understand and enjoy the benefits offered. CSPs use the SAAS to provide applications for the Cloud users over the Internet. Consequently, Cloud users access and use such software using any computer, anywhere, wherever, without any concern about the installation and program specifications. The only drawback, though, is the cost per use nature of such programs. CSP utilizes the PAAS to provide a forum for Cloud customers to build and install their own software. With the benefits of the cloud computing environment along the platform's downsides, steadiness is one of those viewpoints that is most measured. Information Security refers to the security of systems of data and information from unauthorized access, use, release, disruption, alteration, investigation, recording, or destruction. In the light of the Cloud Security Alliance (CSA) survey, there are seven major threats to cloud computing that affiliations will look for[6]. These include Cloud Computing Violence and Nefarious Usage, Insecure Application Programming Interfaces (APIs), Malicious Insiders, Vulnerabilities in Remote Systems, Data Loss / Leakage, Server, Network and Traffic Hijacking, and Known Risk Profile. In reality, Gartner has identified seven Cloud Computing Safety Hazards including

Outsourcing Goods, Regulatory Compliance, Knowledge Location, Sharing Infrastructure, Business Continuity and Disaster Recovery, Tough Environment for Criminal Crime Investigation and Long Term Viability[7]. Such issues are motivated by the cloud existence of the shared assets and the multi-tenancy. The risk of data trading rises in the cloud is due to the increase in the amount of meetings leading to an increase in the number of access purposes[2]. Likewise, the appointment of data control to the Cloud leads to an increase in the risk of data bargaining where the re-appropriated administrations are sidelined by the individual, consistent and physical security controls of the shopper. Numerous questions exist with regard to the problems of multi-tenancy and data protection. Multi-Tenancy refers to Cloud Computing assets where any asset object is reusable in the Cloud Foundation. Reusable papers must be carefully monitored and regulated because they trigger real impotence and violation of privacy by potential data leakage. For now, data leakage is triggered by the fact that Cloud Computing hardware is not isolated; nevertheless, there is a reasonable degree of separation of Cloud Computing in the implementation and the software system in the infrastructure field. In fact, owing to the reusability of asset demonstrations, classification could be disrupted by rethinking data, where a client might order extra room from a cloud provider to run a search to check for confidential data from different clients[3-5].

SECURITY ISSUE: MULTI-TENANCY

Multi-Tenancy is a major concern for cloud computing. Multi-tenancy happens as multiple users use the same platform to exchange information and data or run on a single server. Multi-tenancy in cloud computing occurs in which many applications use the same code, running within the same operating system, in the same infrastructure, with the same data storage network, and sharing a common server with both the victim and the sufferer.

Architecture: This design totally distinguishes your details from other customer information, thus helping us to easily carry out the latest features to each, all at once. This solution provides the most configurability and helps you to gain deep insight from your details. Oracle introduces the new multi-tenant design that enables a multi-tenant cloud database to access a wide range of pluggable databases. An current database will easily be implemented without the need for any improvements to the program.

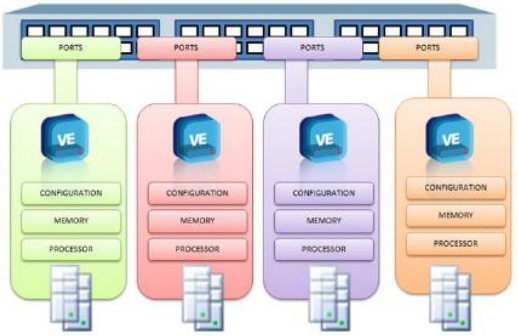

Fig1.Multi-tenancy architecture

MULTI-TENANCY SECURITY THREATS

As Armbrust and Fox (2010) and Feng et al (2011) also pointed out, the key security issues with multitenancy are customers using cloud computing that use single and similar PC equipment to share and process information. It demonstrates various challenges in terms of consistency, security and protection (Bernardo and Hoang, 2010). In addition, the lack of client detachment renders Cloud Computing defenseless against hazards, as does the lack of effective transmission capacity and traffic disconnection, as malignant occupants may dispatch assaults to different residents in a similar cloud data focus. Existing forms to work with cloud management do not scale well to multi-tenancy needs, because they rely only on specific client IDs. The sharing of programming and data by multiple customers poses risks, such as infringements of intellectual property, infringements of data and specialized and industrial sabotage (Bernardo, 2012).

In this sense, Cloud Computing providers are effective across ensuring the users can not traverse and reach each other's supported structures. Another simple risk within the Cloud scenario is the "vixen" assault (Feng, et al, 2011), which indicates that the incredibly low amount of packages setting up the intrusion payload and the surprisingly short length of the assault make it hard to detect the attack on the fingerprint. In fact, counter measures rely on truly educated program chairmen for use at the center for the sharing and guiding purposes of the CSP framework. In a multi-rented environment, the device will get to the specifications of the Cloud-based program chairs and clients from outside the CSP framework address space. Typically, each inhabitant needs a thorough arrangement of IP addresses, which are routable and accessible from the open Internet, in order to get to their applications and operational ease. The CSP is responsible for dealing with a limited pool of IPv4 addresses and must insure that each occupant has its own allocated place.

MULTI-TENANT CHARACTERISTICS

Multi-tenancy has the subsequent uniqueness which are [8]:

- Hardware Resources Sharing:- In traditional single tenant software architecture, tenants have their own VMs, which they customize to their requirements. Unfortunately, using VMs, there is a limit to the number of tenants that can be hosted on a PMs due to high requirements for every VMs [9]. However, With use of multi-tenancy, multiple tenants will share that same software case, thus implicitly increasing resource utilization, that eventually results in lower total implementation costs.

- High Degree of Configurability:- Every tenant has its own personalized application instance in a single tenant environment; while all tenants share the same application instance in a multi-tenant setting, which appears to the tenants as a single, dedicated one. Because of this, a key requirement for multi-tenant systems is the possibility of configuring and customizing software to meet the needs of the widely diverse tenants. In multitenancy, configuration options must be integrated into the product design. In perspective of the large degree of specification of the multi-tenant software system, it could be sufficient to run different versions of the evaluation next to every other.

- Shared Application and Database Instance :- A single tenant program can have many running occurrences, and they may all be different from one another due to configuration. Multi-tenancy inequalities no longer exist, as the program can be changed to runtime. It means that the total number of instances will typically be much less than one in the case of multi-tenancy, but the function may be replicated for purposes of scalability. As a result, deployment is much easier and cheaper, particularly in the area of delivering upgrades, as the number of instances impacted by the deployment operation is much smaller. In fact, new data collection tools are opened because all resident data is in the same area. The signs of user behavior can therefore be quickly identified, which can help to improve user experience. On the basis of the above features, multi-tenancy allows greater use of infrastructure services. It enables easier and cheaper application maintenance. In addition, services are provided at a lower cost, with new data aggregation opportunities.

INDUSTRY TREND IN PREVENTING MULTI-TENANT ATTACKS

Multi-Tenancy in Private Clouds- Organizations is escalating their use of private clouds. Creating a private cloud involves delivering a whole new service management platform from a data center focused on virtualization, orchestration, multi-tenancy and provisioning. IT planners concentrate on private IAAS or the provision of dynamic computing, storage and networking to the design teams. To benefit private Cloud IAAS, it needs to offer elastic, self-supplied, multi-tenant on-demand shared computing, storage, and networking pools[1]. The problem in today's data center is that some elements of networking are not consistent with private cloud computing principles. Actually, most network designs presume a defined partnership between system identity and physical address. Previously, it was unusual for virtualization servers and storage to move around the data center. Virtual machines are currently moving for a number of reasons, such as load handling, power management, repair and disaster recovery. Multi-tenancy is the key feature of the cloud. In a private data center this means creating virtual networks across a physical network because the same computer, storage and network resources are used, for example, for human resources and finance. It is critical that controls are in position to separate one occupant from another. This is important for purposes of revenue, defense and enforcement.

In fact, the bulk of IT companies depend on VLAN's virtual local area network as their central mechanism to provide meaning and multi-awareness in the private cloud. VLANs (802.1q) are efficient for multi-tenancy by isolating the computer machine of one entity from another. There are difficulties with VLAN since, theoretically, the maximum number is 4,096. This may not be a small data center problem, but a large data center with thousands of servers will have issues of limitation. Hypervisors also have limits on how many hosts can be assisted in certain systems, which greatly increases the number of VLANs. VLAN control can be complicated for handling network and virtualization in a cloud environment. The method of connecting a simulated VLAN to a real VLAN is a manual process and handling more than 100 VLANs is a major challenge.

Multi – Tenancy Security- Security in a multi-tenant setting must be discussed at both the SAAS and IAAS layers due to the current services provided. Steps to ensure security in a multi-location environment involve segmentation of VMs, segmentation of databases and introspection of VMs

- VM Segmentation:- Virtualization is the architecture underpinning IaaS services. A

customized and streamlined operating system called a hypervisor is essential to the virtualization process. The hypervisor helps, in turn, to link traffic from virtual machines to the underlying VM host hardware so that traffic will pass through the data center and the Internet, and vice versa. The bulk of security concerns in the virtualized network contribute to the co-residencyof computers operated by different customers. Different clients on the same infrastructure with sensitive data and potentially different access policies are put together. This can contribute to unwanted link tracking, unmonitored program access attempt, dissemination of malware and other types of attacks. Today, in the context of physical computers, network segmentation is used to insure that critical back-end systems are well shielded from potentially vulnerable front-end resources available to the public. This has led to the development of the DMZ and staggered solutions to the architecture of the network core. Segmentation is equally important in a virtual environment, since back-end databases or application servers are worthwhile. VM isolation and segmentation is the key requirement for VMs that contain data relating to compliance, such as personal identifiable information (PII).

- Data Segmentation-: Data segmentation is needed in SaaS wherever tenants share a network of databases while tenants have the same use. Data from different tenants can be held in the same servers and can even be shared in the same tables. Usually, the process for authenticating and approving an access request is implemented so that only certain fields or checks can be modified according to security policies. Encryption is also the main protection mechanism to encrypt data at rest so that if the database becomes hacked or the data is robbed, it would be impossible to decode the underlying data.

- VM Introspection-: VM Introspection (VMI) allows the collection of knowledge regarding virtual machines, computer networks, protection and general world without the use of agents. The potential of malware to conceal or kill security agents is a security issue that has troubled the defense industry for decades. VMI offers an interesting way to use the hypervisor for uncommitted testing of VMs. VMI is basically a service based on hypervisors that explore the internal state of a running machine. New innovations that exploit VMI have been commercialized to provide guest VMs or cloud service tenants with high levels of segmentation and insulation. VMI offers rich descriptions of the program and services built on the virtual machine and the configuration thereof.

LITERATURE REVIEW

The user is considered a tenant in the software-as -a-service distribution model. In a high-volume system in which a single instance of a software application and service network acts as a stand-alone program for one user. Multi tenancy in IaaS is accomplished by exchanging storage, database and servers the principle is called virtualization. Virtualization uses virtual machine technologies that offers a layer of device emulation over real hardware. It allows a single instance of program to serve multiple customers in multiple organizations. SaaS involves the sharing of application servers between rising tenants at a low running cost[11]. Customizations are required to meet the needs of each occupant in addition to sharing application resources. Saas application architecture provides various features for customizing SaaS applications, including organizational structure (role sets and access control), user interface, data model, workflow, and business logic. To meet the multitenancy of the SaaS framework, the metadata-driven model introduced by Force.com[10] has been implemented. This involves control, the supervision of tenants, the setup of tenants and large data management services. In this multi-tenancy framework, the Memcached model used is adopted by almost all databases to boost performance. In addition, a code pooling on a web server is considered to control priority among tenants[10]. The SaaS system named SaaSpia[12] proposed to track and handle multi-tenant environmental issues in real time. A advantage of this process is the complex implementation of user interface codes and business principles. Business logic technology allows runtime configuration without restarting program servers. It is important to use industry-specific customizations and department-specific customizations for inheritance[2].

For Secure data in the framework, use the protection principles in each layer of the cloud system[7] shown in Table1.Hypervisor layer methodology isolates tenants by having independent virtual machines (VMs) for each device. The OS-layer strategy isolates users by isolating their systems, so the customizability of the insulation for each device is related to that of the applications, and the insulation is safely allowed if the power is isolated and the kernel is working properly. Application layer strategies isolate logical resources for each user separated by a database and need to be authenticated and allowed to allow safe isolation. Cloud layer technologies identify customers and acknowledge their exposure to multi-tenant cloud computing resources over networks. Every accident that occurs in this layer can trigger other

layers to malfunction. To stop that, the server-side code needs to be secured and the client-side framework needs to be checked.

Table I. Technical Layers and Categories

Layers	Categories
Web	Server side security
	Client side validation
Application	Secure Data storing
	User data isolation
	Authentication and Authorization
Operating System	Privilege Separation
	Kernel Integrity
Hypervisor	VMM Security
	VMM Security
H/W &S/W Primitive	Programming code
	Hardware processing

The writers in[13] define the multi-tenant design of the WSO2 business process application, which focuses mainly on the multi-tenant workflow engine framework. This method allows several tenants to operate their workflows on the same instance without any updates to workflows.

In[14], the authors defined multi-tenancy at different cloud levels. The highest degree renders the database schema used by several tenants using the SaaS framework. The middle and lower degrees include IaaS and PaaS layers with a multi-tenant history.

The writers in[15] addressed the design of enterprise resource planning[ERP] web applications in the SaaS multi-tenancy setting. A secure multi-tenancy configuration application in the cloud environment suggests security and privacy issues.

In[16], the writers introduced an assault model tailored for multi-tenant scenarios. The program concept and resource allocation strategy was explored with a view to achieving high protection and gaining from a multi-tenancy method.

In[17], the authors introduced a cost-effective and reliable approach to detect suspicious incidents in a large, virtualized cloud computing system. They also provided a comprehensive task estimate of virtual host events in the cloud environment and also introduced a monitoring model for identifying compromised hosts with low malicious events contained within their relevant workload and theoretically spread through several tenants.

In[18], see D. Gonzales et al. introduced a cloud computing architecture that incorporates a wide range of security mechanisms and procedures, and a software security assessment methodology using a system confidence model. Data confidence analysis measured high-level security indicators that determine the level of integrity and secrecy provided by cloud service providers. We also found that the security level of four multi-tenant IaaS software systems has a high probability of cloud computing device leakage (high-value data compromise) if minimal security measures are enforced.

In[19], an SLA-aware, fine-grained QoS supply and bandwidth allocation layout. Their analysis maximized revenue by forecasting success of the SLA using the K-nearest neighbor algorithm.

[20] The writers have shown that tenants must be segregated from one another on the basis of security policies and cloud infrastructure. Their research introduced a multi-level permission (rules) separation concept through learning from cloud trustworthiness.

Two-stage defense provisioning policy was addressed in[21]. Second, a trustworthy partnership with guest Virtual Machines is developed by hypervisor by considering each subjective and object sources of confidence and by using Bayesian inference to combine them. They also proposed Maximin game among hypervisor maximising this minimization within finite resource restriction and DDoS attacker attempting to minimize detection of cloud computing systems.

In[22] F. Banaie and S, guy. A. H. Seno, identified the tool for detecting a wide range of attacks in trusting virtual environments, malicious intruder attacks, attacks against computer staff in different domains, and attacks against specific services such as DNS, database, and domain-based web servers. They introduced fine granular identification of harmful actors and processes and helped to improve interactions between computer staff in different domains.

[23] The authors stated that as communication channels and other computing tools are exchanged in multi-tenant architecture, the state-of - the-art paradigm is vulnerable to a number of security and privacy concerns. Since the renters are confidential in design, the customer may not consider asuitable co-tenant. The tenants rely on the cloud service provider to appointstable co-tenants. Nevertheless, the cloud service company requires full co-tenancy, regardless of the actions of the tenants, to optimize resource utilization. For the presentation, they introduced a comprehensive reputation management system that lets cloud service providers distinguish successful and bad tenants and allocate resources in such a manner that they do not share resources.

CONCLUSION

Cloud computing is hastily expanding and offering valuable services to Cloud users. There as various Cloud services such as SaaS, PaaS, and IaaS. Services such as application, compute resources and storage are provided by the CSP at price to Cloud users. Cloud deployment types such as private, public, community and hybrid Clouds are

available in Cloud computing. Multitenance is a key feature of cloud computing, which allows multiple users from different locations to use a single resource. Multi-tenancy has a unique data-based or multi-renter architecture. Cloud service providers will provide protection for all facets of their services (i.e. IaaS and SaaS) by multi-tenance. Cloud service providers owe their customers the latest and best technologies, such as Hypervisor, Server segmentations, etc., to improve cloud protection as many tenants share the infrastructure. For future work, we could develop a system that would address the multi-tenancy security issues.

REFERENCES

[1]. Mell, P. and Grance, T. (2011) "The NIST Definition of Cloud Computing", NIST Special Publication 800-145 White Paper. Retrieved from acm.org/citation.cfm?id=2206223

[2]. I AWS LLC, "Amazon Elastic Compute Cloud (EC2)" Retrieved from http://aws. amazon.com/ec2

[3]. S. Subashini, and V. Kavitha (2011). "A Survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications.

[4]. Dimitrios Zissis, and Dimitrios Lekkas (2011). "Addressing cloud computing security issues," Future Generation Computer Systems.

[5]. Cloud Security Alliance (2009). "Security guidance for critical areas of focus in cloud computing V2.1" (Dec. 2009).

[6]. Cloud Security Alliance (2010). "Top threats to cloud computing V1.0" (March 2010).

[7]. Jon Brodkin (2008). "Gartner: seven cloud-computing security risks" (July 02, 2008).

[8]. Bezemer, C., Zaidman, A. (2010). "Multi-Tenant SaaS Applications: Maintenance Dream or Nightmare?" Accessed on 24 May 17

[9]. Ngo, C., Demchenko, Y., and Laat, C. (2016), "Multi-tenant attribute-basedaccess control for Cloud infrastructure services", Journal of Information Security and Applications 27-28, pp. 65–84.

[10]. Piyush Aghera et. al. (2012). An Approach to Build Multi-Tenant SaaS Application With Monitoring and SLA, International Conference on Communication Systems and Network Technologies.

[11]. Wonjae Lee et. al. (2012). A Multi-tenant Web Application Framework for SaaS, IEEE Fifth International Conference on Cloud Computing.

[12]. J. Lee and S.J. Hur (2011). "Level 2 saas platform and platform management framework", in advance communication technology (ICACT), 2011 13th International conference on June 2011, pp. 384-387

[13]. Milinda Pathirage, Srinath Perera, Indika Kumara, and Sanjiva Weerawarana (2011). "A Multi-tenant Architecture for Business Process Executions," In proceedings of the 2011 IEEE International Conference on Web Services ICWS'11, IEEE Computer Society, 2011.

[14]. KaushalJani, Bimal Kumar, and Harshal Shah: "Degree of Multi-tenancy and its Database for Cloud Computing," International Journal of Engineering Development and Research (IJEDR) pp. 168-171.

[15]. Ziani, Djamal (2014). "Configuration in ERP SaaS Multi-Tenancy." arXiv preprint arXiv:1405.0650.

[16]. Hussain Al-Jahdali, Abdulaziz Albatli, Peter Garraghan, Paul Townend, Lydia Lau, and JieXu (2014). "Multi-tenancy in cloud computing," In proceedings of the 8th IEEE International symposium on service-oriented system engineering.

[17]. R. Cogranne, G. Doyen, N. Ghadban and B. Hammi (2018). "Detecting Botclouds at Large Scale: A Decentralized and Robust Detection Method for Multi-Tenant Virtualized Environments," in IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 68-82, March 2018.

[18]. D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods (2017). "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 523-536, 1 July-Sept. 2017.

[19]. G. Li, J. Wu, J. Li, Z. Zhou and L. Guo (2018). "SLA-Aware Fine-Grained QoS Provisioning for Multi-Tenant Software-Defined Networks," in IEEE Access, vol. 6, pp. 159-170.

[20]. W. Ma, Z. Han, X. Li and J. Liu (2016). "A multi-level authorization based tenant separation mechanism in cloud

computing environment," in China Communications, vol. 13, no. 5, pp. 162-171.

[21]. O. Abdel Wahab, J. Bentahar, H. Otrok and A. Mourad (2017). Optimal Load Distribution for the Detection of VM-based DDoS Attacks in the Cloud," in IEEE Transactions on Services Computing. doi: 10.1109/TSC.2017.2694426

[22]. F. Banaie and S. A. H. Seno (2014). “A cloud-based architecture for secure and reliable service provisioning in wireless sensor network," 2014 4th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, pp. 96-101.

[23]. S. Thakur and J. G. Breslin (2017). "A Robust Reputation Management Mechanism in Federated Cloud," in IEEE Transactions on Cloud Computing. doi: 10.1109/TCC.2017.2689020.

Corresponding Author

Dipti Prava Sahu*

Research Scholar, Computer Science & Engineering, Glocal University, Uttar Pradesh

diptiprava29@gmail.com