ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Cloud Security: PaaS Aspect

Dana Isa AL Themazi
Department of Computer Science,MITCS Student , Ahlia University, Bahrain Internet Exchange, Bahrain
Muheet Ahmed Butt
Scientist, PG Department of Computer Science, Unvierstiy of Kashmir, J&K
Majid Zaman
Scientist, Directorate of IT &SS,University of Kashmir, J&K, India

Abstract:- ***The security demands affiliated to cloud computing are of high priority, importance and of close attention. When it comes to security cloud-based services have to be used & managed at all possible levels of enterprise system. The main issue with commercial enterprise is that they do not want to store their sensitive data on commercial cloud due to lack of faith on third party entities, however things all together change when it comes to retail users because sensitivity and sensitivity of data varies from retail to cooperative user. Cloud users will have no control over the cloud storage servers used, and there is a built-in risk of information vulnerability to third parties in the cloud or to the cloud provider itself. This paper reviews the classical security services and requirement in an open environment and introduces a Trust Based framework for cloud security.***

Index Terms: **Cloud Computing, PAAS, IAAS, Security.**

I. INTRODUCTION

Cloud computing changes the domain of computing, everything now is connected to the cloud world. Now a day the opportunities for improving IT efficiency and performance through centralization of resources have increased dramatically in the last few years with the development of technologies such as virtualization, SOA , management automation and grid computing[1]. A natural outcome of this is what has become progressively referred to as "cloud computing", where consumer and customer of computational capabilities sets up or makes use of cloud computing over the network. But in fact it's initially referring to services provided by third parties over the Web, cloud computing evolving in a public and private cloud. Realization of performance in cloud computing comes of efficiency and agility benefits to reinforcing the developments for cloud service provider [1].

II. CLOUD COMPUTING: A GLOBAL OVERVIEW

Cloud computing has been called the 5th utility in the line of electricity; water, telephony and gas. The reason why cloud has been called with such a name is that the cloud computing has been changing the way computer resources have been used up to now [5][6]. Cloud computing has brought a standard change in how computing resources have been worked. And that's works as the following; Cloud providers host their resources on the internet on virtual computers and make them available to multiple clients [7]. Multiple virtual computers can run on one physical computer sharing the resources such as storage, memory, the CPU and interfaces giving the feeling to the client that each client has his own dedicated hardware to work on. Virtualization thus gives the ability to the providers to sell the same hardware resources among multiple clients. Previously the advent of electrical utilities, in every farm and business produced its own electricity from freestanding generators. But after the electrical grid was created, all the farms and businesses shut down their generators and bought electricity from the utilities, at a much lower price. (and with much greater reliability) than they could produce on their own. Cloud computing came with huge revolution to ensure that cloud computing takes hold [2]. Both centralization and distribution have important merits for enterprise IT. Centralization of control enables consistency, economies of scale, and efficient rollout of innovations that are applicable across the enterprise. Distribution of control enables agility for departments, allowing flexibility to respond quickly to needs and imperatives specific to their roles within the organization [1]. Optimizing the balance between centralization and distribution is an ongoing challenge for IT architecture, organization of the consumer who support that architecture, and organization of the persons who use that architecture. Client server computing was the first big step toward more centralization from the world of distributed PCs and workstations [1]. As the ubiquity and quality of Internet-based networking made client-server more viable and widespread, much of computing shifted to the server in a more centralized model but the concerned is about security [1]. What are the cloud security abstraction and aspects? These we will explain them in the next section.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

III. CLOUD SECURITY ASPECTS

There are many benefits of cloud computing by virtue of abstraction, prevents the consumer from having the same level of influence over the computing resource [3] [4]. Great concern is the ability of consumer to assert quality of service [5]. QoS refers to aspects of a service that are not functional but are important considerations, This is leads to some of the following challenges with public cloud computing. "One of the key challenges in cloud computing is data-level security" [5]. Starting with the most important challenges which are:

- (Availability)
- Then ,(Data Residency),
- And,(Multitenancy),
- With,(Performance),
- (Data Evacuation),
- Ending with Supervisory Access & Privacy).

Even large enterprises with significant resources face considerable challenges at the network level of infrastructure security. Are the risks associated with cloud computing actually higher than the risks enterprises are facing today? Consider existing private and public extranets, and take into account partner connections when making such a comparison. For large enterprises without significant resources, or for small to medium-size businesses (SMBs), is the risk of using public clouds (assuming that such enterprises lack the resources necessary for private clouds) really higher than the risks inherent in their current infrastructures? In many cases, the answer is probably no—there is not a higher level of risk. In other hand, the virtualization technologies enable multitenancy cloud business models by providing a scalable, shared resource platform for all tenants. More importantly, they provide a dedicated resource view for the platform's consumers. From an enterprise perspective, virtualization offers data center consolidation and improved IT operational efficiency. Today, enterprises have deployed virtualization technologies within data centers in various forms, including OS virtualization (VMware, Xen), storage virtualization (NAS, SAN), database virtualization, and application or software virtualization (Apache Tomcat, JBoss, Oracle App Server, Web Sphere). From a public cloud perspective, depending on the cloud services delivery model (SPI) and architecture, virtualization appears as a shared resource at various layers of the virtualized service (e.g., OS, storage, database, application) [6,7].

The simplicity of self-provisioning new virtual servers on an IaaS platform creates a risk that insecure virtual servers will be created. Secure-by-default configuration needs to be ensured by following or exceeding available industry baselines. Securing the virtual server in the cloud requires strong operational security procedures coupled with automation of procedures. Here are some recommendations:-

- Use a secure-by-default configuration. Harden your image and use a standard hardened image for instantiating VMs (the guest OS) in a public cloud. A best practice for cloud based applications is to build custom VM images that have only the capabilities and services necessary to support the application stack. Limiting the capabilities of the underlying application stack not only limits the host's overall attack surface, but also greatly reduces the number of patches needed to keep that application stack secure.
- Track the inventory of VM images and OS versions that are prepared for cloud hosting. The IaaS provider provides some of these VM images. When a virtual image from the IaaS provider is used it should undergo the same level of security verification and hardening for hosts within the enterprise. The best alternative is to provide your own image that conforms to the same security standards as internal trusted hosts.
- Protect the integrity of the hardened image from unauthorized access.
- Safeguard the private keys required to access hosts in the public cloud.
- In general, isolate the decryption keys from the cloud where the data is hosted—unless they are necessary for decryption, and then only for the duration of an actual decryption activity. If your application requires a key to encrypt and decrypt for continuous data processing, it may not be possible to protect the key since it will be collocated with the application.
- Include no authentication credentials in your virtualized images except for a key to decrypt the file system key.
- Do not allow password-based authentication for shell access.

IV. PAAS PLATFORMS

PaaS platforms have functional differences from traditional development platforms and that make it one of the challenges, which include

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

- ***Multitenant development tools:*** Traditional development tools are intended for a single user; a cloud-based studio must support multiple users, each with multiple active projects.
- ***Multitenant deployment architecture:*** Scalability is often not a concern of the initial development effort and is left instead for the system administrators to handle when the project deploys. In PaaS, scalability of the application and data tiers must be built-in (e.g., load balancing and failover should be basic elements of the developing platform).
- ***Integrated management:*** Traditional development solutions (usually) are not associated with runtime monitoring, but in PaaS the monitoring ability should be built into the development platform.
- ***Integrated billing:*** PaaS offerings require mechanisms for billing based on usage that are unique to the SaaS world.

One of the furthermost challenges are Identity Management-As-A-Service (IDaaS) only recently emerged as an example of SaaS, in comparison to email filtering, web content filtering, and vulnerability management, which are more established as SaaS offerings. There are some significant deficiencies in today's Identity and Access Management (IAM) capabilities with regard to uses in cloud computing (e.g., scalability). IDaaS attempts to provide some IAM services in the cloud. To end with benefits of PaaS lie in greatly increasing the number of people who can develop, maintain, and deploy web applications. In short, PaaS offers to democratize the development of web applications in much the same way that Microsoft Access democratized the development of the client/server application. For that we must know the exiting tools which in the cloud computing to understand it more.

V. CONCLUSION

We already know that cloud computing is very huge thing in computing world, and for its success the security level in the cloud computing has to be achieved; it must achieve all the security services features, otherwise what will happen is that cloud will lose its trust and end up being the best thing, with worst fear. Emphasis on the importance of PaaS as the future of cloud services and we are now seeing complete transformation of PaaS space with all the Platforms vendors focusing on multi language and multi cloud trends. In fact the way of developing the PaaS framework is by develop the way of securing the clouds with insuring the infrastructure security, data security and storage, security management, privacy and Security as a service Cloud is all about security and companies have to ensure security to ascertain it success without doubt.

REFERENCES

[1]. Oracle," Platform-as-a-Service Private Cloud with Oracle Fusion Middleware", available: http://www.oracle.com/us/technologies/cloud/036500.pdf, October 2009.

[2]. N. Elkadhi, D. Altehmazi, "Global QoS Framework for Cloud Security: A Paradigm Shift toward a New Trust Concept", in Proc. The 2012 International Conference on Security and Management (SAM'12), Las Vegas, 2012, pp. 295-307.

[3]. Zhiguang, S. and L. Chuang. Modeling and Performance Evaluation of Hierarchical Job Scheduling on the Grids. in Grid and Cooperative Computing, 2007. GCC 2007. Sixth International Conference on. 2007.

[4]. Weidong, H., Y. Yang, and L. Chuang. Qos Performance Analysis for Grid Services Dynamic Scheduling System. in Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on. 2007.

[5]. Afzal, A., A.S. McGough, and J. Darlington, Capacity planning and scheduling in Grid computing environments. Future Generation Computer Systems 2008. 2008(24): p. 404-414.

[6]. Kiran, M., et al. A prediction module to optimize scheduling in a grid computing environment. in Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on. 2008.

[7]. Yuan-Shun, D., X. Min, and P. Kim-Leng, Availability Modeling and Cost Optimization for the Grid Resource Management System. Systems, Man and Cybernetics, Part A, IEEE Transactions on, 2008. 38(1): p. 170-179.