Cloud Computing - Is Your Information Secure

Beaulah AloysiusNavamani

CS5910 – Project work

University of Colorado, Colorado Springs

**bnavaman@uccs.edu**

**ABSTRACT*-*** Cloud Computing is unquestionably the backbone for almost all the networks that we use today. There are many cloud service provider (CSP) who offers cloud service to the customers to host their information. Cloud Service Providers like Amazon, Google, Microsoft Azure, IBM and Sun provide services to the users to instantiate virtual machines (Virtual machine-VM in EC2 and Virtual Image - VI in IBM cloud) on demand and hence purchase and pay for the capacity and resources they require and when they require. However in this paper I have also explained about the possible threats in the cloud infrastructure and also quoted the recent incidents, research and the proposed solution for those security issues.

**General Terms**

Security, Proposal, Experiment

**Keywords**

Cloud computing, Virtual images, Instances

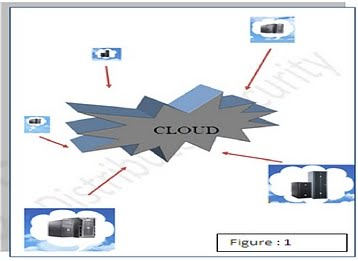
1. **INTRODUCTION**

With cloud computing infrastructure it is ok for a truck to crush your laptop or storage. Well then, what is cloud computing? It can be defined as the use of the computer technology that ties together the processing power of many computers inter-connected in the network by concealing the structure that is behind it. The most important benefit of cloud computing is, an average user does not need a powerful computer to handle complex resources. Instead, the user can be connected to cloud, which we can say as the point of contact in the network. From the figure: 1 you can see that the clouds (which will be the resources) are shared between many users. The resources and the database can be shared across the world using the cloud technology. The cloud computing system showed a comfortable and profitable way to deal with the users. The cloud system allows the vendor to concentrate more on the software than its core framework by providing an incorporated interface between the vendor and the user. Cloud system prioritize the customers’ resources requests and dynamically allocates the recourses to the customers (users) based on their needed quality of service (QoS).

Permission to make digital or hard copies of all or part of this work for

Personal or classroom use is granted.

CS5910-UCCS, December 12, 2010, Colorado Springs, Colorado



There are massive benefits from using cloud computing. They provide Flexibility, Scalability and Portability at high end. Everyone agrees that every new technology has its own risks, so as this cloud computing, it lacks in strong security. But, even with this drawback no one can deny that it has become a widely accepted terminology in the tech world. So without a doubt the cloud computing is ruling the Tech World! And there are few important criteria for why someone want to lean towards the cloud computing, 1. In this paper I addressed about the security issues and some proposal to solve these issues in the following sections:

Section1: Why Cloud? - Cloud model, available services, cloud providers and their launches

Section 2: Related work

Section 3: What should be secured in the cloud?

Section 4: What are the possible categories of threats for cloud computing?

Section 5: Security breach and incidents that happened in cloud computing

Section 6: Proposed work and future work

Section 7: Conclusion

Section 8: References

1. **Why Cloud**

The most important reasons or attributes that makes the cloud computing so attractive is the multi-tenancy- the cloud is totally a business model in which all of the resources are shared at all the three levels (network, host and application), the enormous scalability- the cloud has high level of ability to scale bandwidth and storage, elasticity- the customers and users can quickly increase or decrease the resources they want, pay as you go facility- pay only for your resources and the self-provisioning- users can provision the additional resources as they need. The cloud is totally a business model in which all of the resources are shared at all the three levels (network, host and application).

Cloud Models:

*SPI Frame work*

The common cloud computing frame work model goes by the name SPI. This acronym SPI represents the great three services software-as-service (Saas), Platform-as-services (Paas) and infrastructure-as-service (Iaas) offered by the cloud providers. The complete relation between these services (which can also be called as delivery models), the deployment models and the available application domains are shown in the below picture figure: 2 [2]

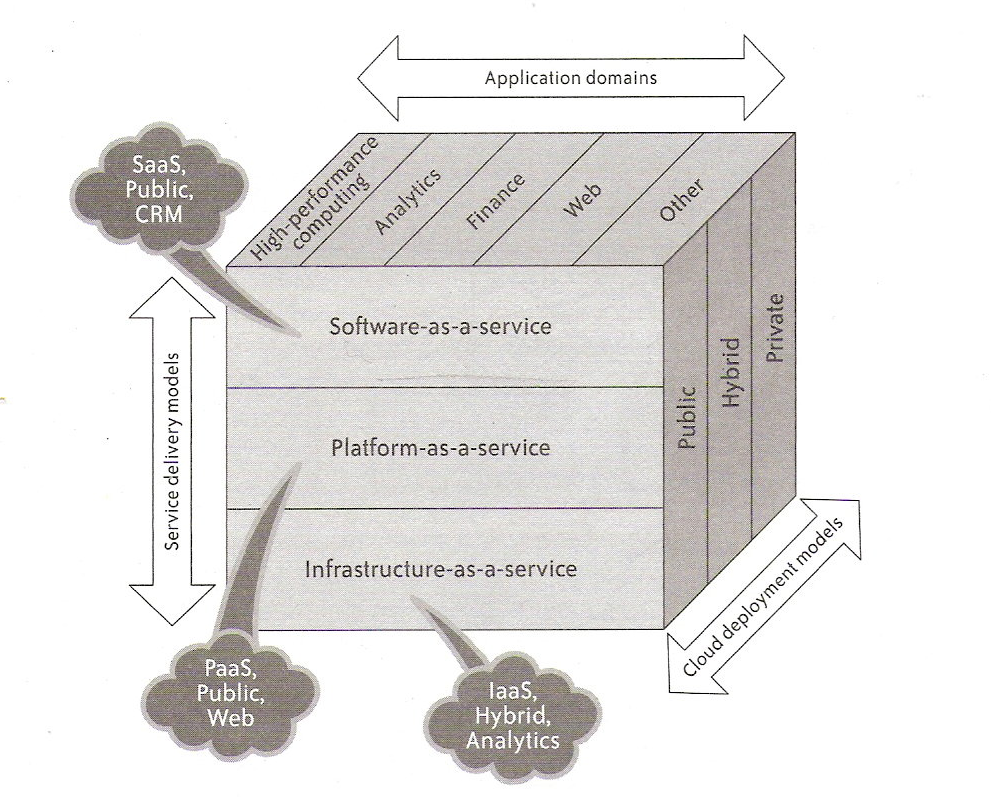


Figure: 2

|  |
| --- |
|  |

[Software as a Service](http://searchCloudComputing.techtarget.com/sDefinition/0,,sid201_gci1170781,00.html) (SaaS) is a software distribution model in which application are hosted by a vendor (sales person) or service provider and made available and accessible to customers (users) over a network, typically the Internet. [Platform as a Service (PaaS)](http://searchCloudComputing.techtarget.com/sDefinition/0,,sid201_gci1332892,00.html) is a model for delivering operating systems and related services over the Internet without downloads or installation. [Infrastructure as a Service (IaaS)](http://searchCloudComputing.techtarget.com/sDefinition/0,,sid201_gci1358983,00.html) involves outsourcing the whole infrastructure used to support operations, including storage, hardware, servers and networking components. The complete definition of the cloud services model and the available examples are shown in the below picture figure: 3 [2]. There are three important cloud deployment models they are private clouds, public clouds and hybrid clouds.

*Delivery Model:*

Public Cloud -

It is also known as external cloud or multi-tenant cloud, this model basically stand for a cloud environment that is openly

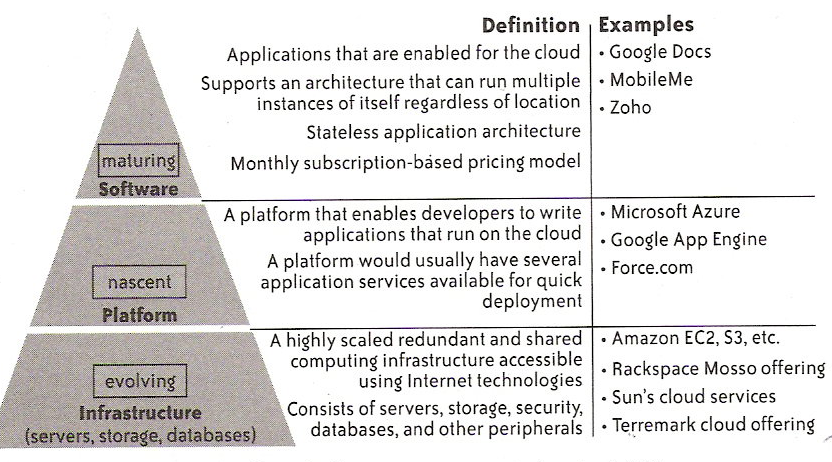


Figure: 3

available. In general it provides an IT infrastructure in a third-party physical data center that can be used to deliver services without having to be concerned with the underlying technical complexities. Vital characteristics of a public cloud include [7]:

* homogeneous infrastructure
* common policies
* shared resources and multi-tenant
* leased or rented infrastructure; operational expenditure cost model
* economies of scale

The public clouds can host both individual services and collections of services.   
1PIXELPrivate Cloud -  
We can say as internal cloud or on-premise cloud, a private cloud purposely restricts access to its resources to serve the consumers that belongs to the same organization who owns the cloud. This type of cloud is managed and operated by the particular organization to maintain security and privacy to some consistent. Important characteristics of a private cloud include [7]:

* Heterogeneous infrastructure
* Customized and tailored policies
* Dedicated resources
* In-house infrastructure
* End-to-end control

Hybrid Cloud-

Most industry-specific regulations (e.g., in health care industries), and national privacy laws may restrict the data an enterprise may migrate to the cloud. As a answer to these issues, there has been major concentration in the industry towards the hybrid architectures where enterprise applications

are partly hosted on-premise, and partly in the cloud. In the enterprise applications there are multiple of components, and hybrid architectures agree to migrate the individual components or kept local if they are confidential [8]. Hybrid architectures propose enterprises flexibility and elasticity in decision making that can facilitate them to find the accurate balance between privacy considerations, performance and cost. For instance, sensitive databases (e.g., related to credit card processing, patients medical records) may be placed local to the enterprise, while comparatively less sensitive components could be migrated to the cloud. Users outside to the enterprise could be controlled through servers deployed in the cloud, while internal users could be controlled through servers placed on premise.

*Cloud Architecture*

The below picture figure: 4 [13] explain the typical cloud architecture. The user or the customers are connected to the cloud via the portal server through the cloud manager or they can bypass the portal server and connected through the cloud manager. They have the image repository where we could store the virtual images (VI), the virtual images can have number of applications and software for executions and the running virtual images are called as the instances. Then they have the computation servers for execution, each cloud can have as many computational servers depend on the cloud providers, ex: Amazon EC2 cloud provide two regions of cloud one in Europe and the other in North America, each region has three zones and they provide five different type of instances. The EC2 could hold eight small instances to the maximum in their computational server (physical server).And the other major component is the storage servers where we could store our computed data but as a user it is our choice either to store the data in cloud or back to our private network.



Figure: 4

*Cloud Service Providers*

There are over 30 cloud service providers for different services and service applications. Below are the few top service providers [9].

## Amazon web services

**

1. Microsoft windows Azure



1. Google app Engine



1. VMware Cloud



1. IBM blue cloud

**

The below picture Figure: 5 [2] explain the recent notable cloud launches

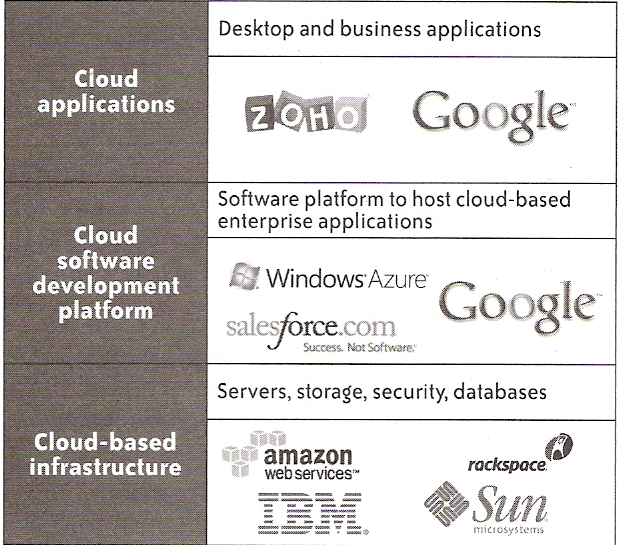
**

Figure: 5

1. **related Work**

“Above the clouds – The Berkeley view of cloud computing” [10] in this paper they have explained about the evolution and economics of cloud and also more details about utility computing. They have given brief examples of cloud computing vendors and how each vendors provision their resources. Another paper [11], “Ensuring the data security in cloud computing” explains about the cloud data storage security, by isolating the storage device in cloud.”Towards analyzing Data Security Risks in Cloud Computing Environments” [12] a conference paper explains about the Security advantages, Security issues and challenges especially for the data in the cloud. There are so many works that explains both the advantages and the disadvantages of cloud based on its security. This paper explains more about the threats and risks that are in the cloud. And also explained a conference paper to show how easily the cloud could be vulnerable to the information residing inside that.

1. **Cloud Security**

Though there are so many benefits in the cloud computing architecture and services, there are so many significant barriers to adapt the cloud architecture. The most vital barriers are the security and the privacy. As the cloud computing is the new type of computing model also it is an extension of already existing computing, there is a great uncertainty about providing security at all levels – network level, host level and data level. Securing the It infrastructure as core at all the three levels mention is bundle up as the infrastructure security. The infrastructure security at the network level includes ensuring data confidentiality and integrity, ensuring proper access control, ensuring the availability of internet-facing resources and network level mitigation.

The infrastructure security at host level includes both software as service and platform as the service host security, virtualization software security (includes threats to the hypervisor), virtual server security (securing the virtual servers). The infrastructure security at application level includes the application level security threats, application level DoS and DDos attack, and end user security. The cloud should ensure the data security for the data in transit, data in store and processing of data. As the special case the cloud security has a lot of limitation to force the security features. The security requirements such as an application firewall, SSL accelerator, cryptography are not supported in the public cloud.

**4. Thread categories**

As per the Cloud Security alliance report in March 2010 [14] the top security threats are:

* *Abuse and despicable Use of Cloud Computing:*

The cloud service provider has a very generic registration process and allow anyone with a valid credit card. Spammers, intruders and malicious code authors take this as an advantage to abuse the cloud environment. For example, IaaS offerings lead to hosting of infoStealer Trojan horses and zeus botnet.

* *Insecure interfaces and APIs*

Cloud service providers expose their cloud for the customers to load their software interfaces and APIs. They perform provisioning, management and monitoring using these interfaces. So basically the security and availability of the cloud depend upon these interfaces and APIs.

* *Malicious insiders*

The customers who were genuine users to the cloud service providers could be a threat to the cloud and the users who shares the cloud. They could extract the other user’s information as all the resources are shared in the cloud

* *Shared resources*

This is the main reason for the security breach in the cloud. The components like CPU caches, GPUS etc are not strongly isolated for user by user as they are muti-tenant in nature. So, one could easily steal other user’s information in the cloud.

* *Data Loss or leakage*

In cloud there are so many ways to compromise the data. For example loss of the encoding key could result in massive destruction. The threat of data compromise increases in the cloud architecture due to its architectural or operational characteristics. Ex: insufficient audit control, authentication and authorization.

**5. Security Incidents**

The cloutage is the available website which reports the security, incidents and breaches happened in the cloud environment. The below picture Figure: 6 [15] list all the cloud security incidents happened in 2010.

****

**6. Proposed work and future work**.

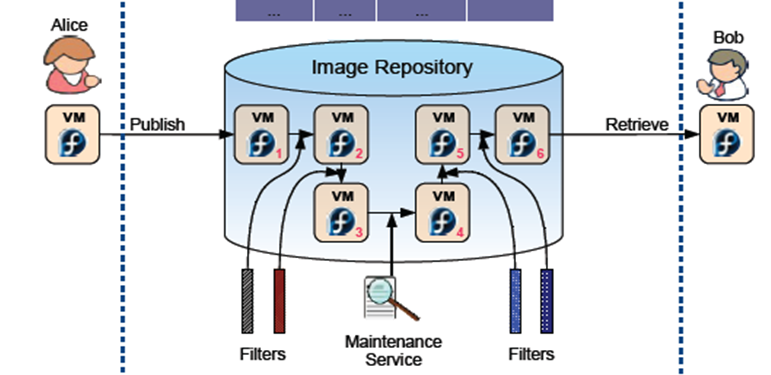
*Proposed work:*

“Exploring Information Leakage in Third-Party Compute Clouds” [1] is the proposed work to expose the vulnerable nature of the cloud. In their work they did this research on the Amazon EC2 as their test bed. By doing this research they achieved the following four steps:

* Determine where in the cloud infrastructure an instance is located
* Easily determine if two instances are co-resident on the same physical machine
* Attacker launch instances that will be co-resident with other user’s instances
* Attacker exploit cross-VM information leakage once co-resident

So they conclude as, in a public cloud one can trace anyone’s virtual machine and steal the sensitive information.

Another proposed work [3] is to show how we could secure the insecure cloud environment. They proposed in adding filters on the virtual machine publisher’s side and the user’s side. In their architecture they are shielding their sensitive information from the malicious intruders residing inside the cloud environment. The below picture Figure: 7 [3] explain their proposed architecture



*The future work:*

This paper is focusing on to improve the security in cloud computing by developing filters for the binary files and developing dynamic filters for the sensitive information based on the users and the publishers virtual machine applications.

**7. Conclusion**

In this paper I argued that even though the cloud computing is a big hit in resource sharing and cost saving the two barriers which make the cloud users to think twice to migrate their information to cloud is the security and privacy. I have exposed how the cloud environment could be insecure for your sensitive information. As there are few proposed solutions to force security to the cloud my next step is to keep moving forward to find a better security solution for the cloud environment.

**8. References**

1. Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage*. Hey, you, get off of my cloud: exploring Information leakage in third-party compute clouds*. In CCS ’09: *Proceedings of the 16th ACM conference on Computer and communications security.*
2. Cloud Security and Privacy, an Enterprise Perspective on Risks and Compliance. [Tim Mather](http://www.oreillynet.com/pub/au/3784), [Subra Kumaraswamy](http://www.oreillynet.com/pub/au/3786), [Shahed Latif](http://www.oreillynet.com/pub/au/3785). *O'Reilly Media2009*
3. Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning, “Managing Security of Virtual Machine Images in a Cloud Environment”. *In CCSW, 09 November 2009.*
4. IBM. IBM Cloud Computing: <http://www.ibm.com/ibm/cloud>
5. Cloud Computing - Implementation, Management and Security. John W. Rittinghouse, James F. Ransome
6. SPI model. Cloud Computing. 01 Feb 2010

<http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1380318,00.html>

1. Cloud deployment models. Private cloud and public cloud. <http://www.whatissoa.com/whatiscloud/p1.php>
2. M. Hajjat, X. Sun, Y.-W. E. Sung, D. Maltz, S. Rao,K. Sripanidkulchai, and M. Tawarmalani. Cloudward bound:Planning for beneficial migration of enterprise applications to thecloud. *In Proc. of SIGCOMM, Delhi, India, Aug. 2010.*
3. Nitin. Top Cloud computing services providers. September 2010. [*http://nitinjaiswal.com/2010/09/top-cloud-computing-service-providers/*](http://nitinjaiswal.com/2010/09/top-cloud-computing-service-providers/)
4. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica,M. Zaharia. *Above the Clouds: A Berkeley View of Cloudcomputing*. Technical Report No. UCB/EECS-2009-28, University of California at Berkley, USA, Feb. 10, 2009.
5. C. Wang, Q. Wang, K. Ren, and W. Lou*, “Ensuring data storage security in cloud computing,”* in Proc. of IWQoS’09, Charleston, South Carolina, USA, 2009.
6. Sangroya, Kumar, Dhok, Varma *“ Towards Analyzing Data Security Risks in Cloud Computing Environments”* in ICISTM, Bangkok, Thailand 2009*.*
7. Wei, Zhang, Ammons, Bala, Ning *“Managing Security of Virtual Machine images in a cloud environment”* in CCSW, Chicago, Illinois, USA 2009.
8. Cloud Security Alliance*.”Top threats to cloud computing V1.0”* in CSA report. March 2010
9. Latest cloud security incidents

[*http://cloutage.org/*](http://cloutage.org/)*. 2010*