International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Study of Cloud Computing Technologies and security issue

Manoj Kumar Dhruw
Student, Bachelor of Engineering in Computer Science & Engineering Kirodimal Institute of Technology, Raigarh (C.G.), India
dhruwmanoj2010@gmail.com
Amarjit Ram
Student, Bachelor of Engineering in Computer Science & Engineering Kirodimal Institute of Technology, Raigarh (C.G.), India
amarjitram772@gmail.com
Rakesh Patel
Lecturer, Department of Information Technology Kirodimal Institute of Technology, Raigarh (C.G.), India
rakeshpatel.kit@gmail.com

Abstract

The term Cloud Computing works with different computing technologies like Virtualization, Service-Oriented Architecture, Grid Computing, and Utility Computing. It access over a network but also it refer to manipulate, configure. The Cloud Computing has many technologies that working with different Cloud model and related to each other. It also necessary of Security issue for each Cloud Computing technologies.

1. Introduction

The cloud is not simply the latest fashionable term for the Internet. Though the Internet is a necessary foundation for the cloud, the cloud is something more than the Internet. The cloud is where you go to use technology when you need it, for as long as you need it, and not a minute more. You do not install anything on your desktop, and you do not pay for the technology when you are not using it. [1]

The cloud can be both software and infrastructure. It can be an application you access through the Web or a server that you provision exactly when you need it. [1]

2. Cloud Computing Technologies:

There are certain technologies working behind the cloud computing platforms making cloud computing flexible, reliable, and usable. These technologies are listed below:

- Virtualization
- Service-Oriented Architecture (SOA)
- Grid Computing
- Utility Computing

2.1 Virtualization

Virtualization is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants (customers). It does this by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.

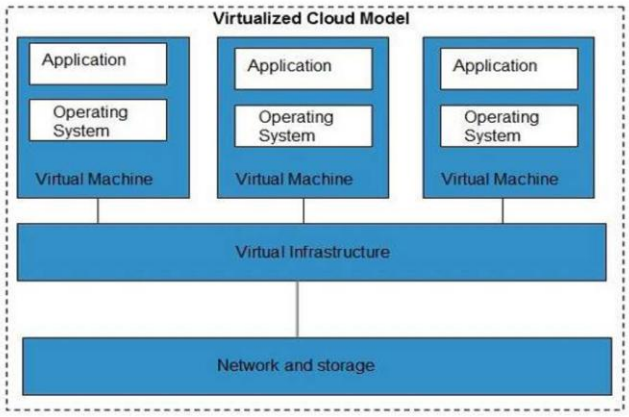


Fig. 1 Virtualization technology

The **Multitenant** architecture offers **virtual isolation** among the multiple tenants. Hence, the organizations can use and customize their application as though they each have their instances running. [2]

2.2 Service-Oriented Architecture (SOA)

Service-Oriented Architecture helps to use applications as a service for other applications regardless the type of vendor, product or technology. Therefore, it is possible to exchange the data between applications of different vendors without additional programming or making changes to services.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

The cloud computing service oriented architecture is shown in the diagram below:

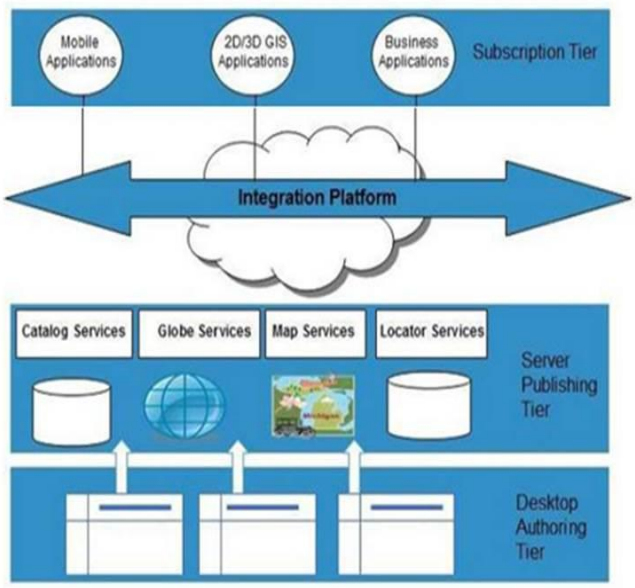


Fig. 2 Service-Oriented Architecture (SOA) technology [2]

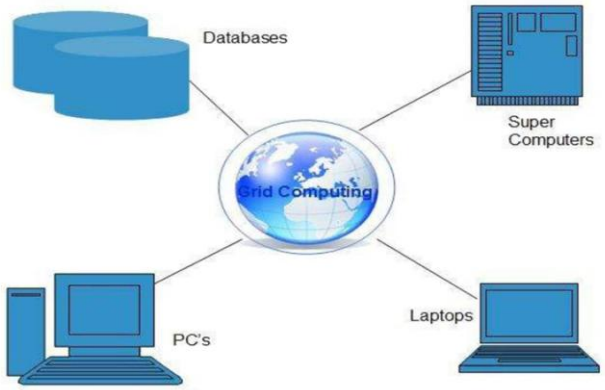
2.3 Grid Computing

Grid Computing refers to distributed computing, in which a group of computers from multiple locations are connected with each other to achieve a common objective. These computer resources are heterogeneous and geographically dispersed.

Grid Computing breaks complex task into smaller pieces, which are distributed to CPUs that reside within the grid. [2]

Fig. 3 Grid Computing technology

2.4 Utility Computing



Utility computing is based on Pay-per-Use model. It offers computational resources on demand as a metered service. Cloud computing, grid computing, and managed IT services are based on the concept of utility computing. [2]

3. Cloud Computing Security

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from accessing the shared data directly, proxy and brokerage services should be employed. [2]

Any individual tenant on a multitenant service is placed in a security sandbox that limits its ability to know anything about the other tenants, even the existence of other tenants. This is handled in different ways on different services. For example, hypervisors manage security on virtual machines, relational databases have robust user management features, and cryptographically secure keys are used as controls for cloud storage. [4]

3.1 Security Planning

Before deploying a particular resource to cloud, one should need to analyze several aspects of the resource such as:

- Select resource that needs to move to the cloud and analyze its sensitivity to risk.
- Consider cloud service models such as IaaS, PaaS, and SaaS. These models require customer to be responsible for security at different levels of service.
- Consider the cloud type to be used such as public, private, community or hybrid.
- Understand the cloud service provider's system about data storage and its transfer into and out of the cloud.

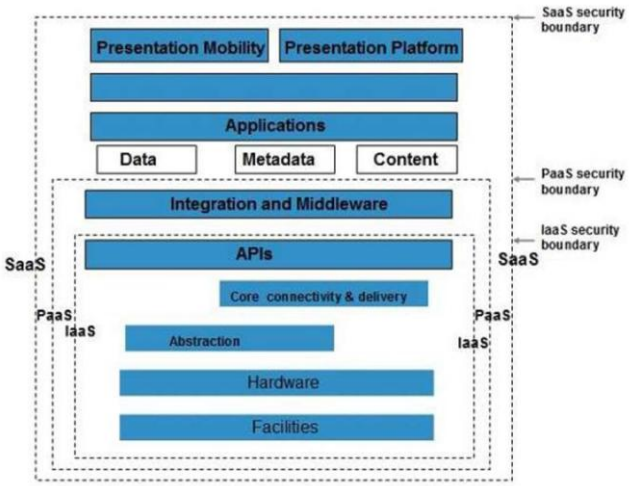
The risk in cloud deployment mainly depends upon the service models and cloud types. [2]

4. Understanding Security of cloud:

4.1 Security Boundaries

A particular service model defines the boundary between the responsibilities of service provider and customer. Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the CSA stack model: [2]

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org



4.2 Key Points to Cloud Security Alliance (CSA) Model:

- IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.
- IaaS is the most basic level of service with PaaS and SaaS next two above levels of services. Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.

Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud. [2]

5. Understanding Data Security

Since all the data is transferred using Internet, data security is of major concern in the cloud. Here are key mechanisms for protecting data.

- Access Control
- Auditing
- Authentication
- Authorization

All of the service models should incorporate security mechanism operating in all above-mentioned areas. [2]

Physical security defines how you control physical access to the servers that support your infrastructure. The cloud still has physical security constraints. After all, there are actual servers running somewhere. When selecting a cloud provider, you should understand their physical security protocols and the things you need to do on your end to secure your systems against physical vulnerabilities. [1]

5.1 Data Control

The big chasm between traditional data centers and the cloud is the location of your data on someone else's servers. Companies who have outsourced their data centers to a managed services provider may have crossed part of that chasm; what cloud services add is the inability to see or touch the servers on which their data is hosted. The meaning of this change is a somewhat emotional matter, but it does present some real business challenges.

The main practical problem is that factors that have nothing to do with your business can compromise your operations and your data. For example, any of the following events could create trouble for your infrastructure:

- The cloud provider declares bankruptcy and its servers are seized or it ceases operations.
- A third party with no relationship to you (or, worse, a competitor) sues your cloud provider and obtains a blanket subpoena granting access to all servers owned by the cloud provider.
- Failure of your cloud provider to properly secure portions of its infrastructure—especially in the maintenance of physical access controls—results in the compromise of your systems.

The solution is to do two things you should be doing anyway, but likely are pretty lax about: encrypt everything and keep off-site backups.

- Encrypt sensitive data in your database and in memory. Decrypt it only in memory for the duration of the need for the data. Encrypt your backups and encrypt all network communications.
- Choose a second provider and use automated, regular backups (for which many open source and commercial solutions exist) to make sure any current and historical data can be recovered even if your cloud provider were to disappear from the face of the earth. [1]

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

6. Isolated Access to Data

Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client's direct access.

Brokered Cloud Storage Access is an approach for isolating storage in the cloud. In this approach, two services are created:

- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker. [2]

7. Cloud Security Reference Model

The cloud security reference model addresses the relationships of these classes and places them in context with their relevant security controls and concerns. For organizations and individuals grappling with cloud computing for the first time, it is important to note the following to avoid potential pitfalls and confusion:

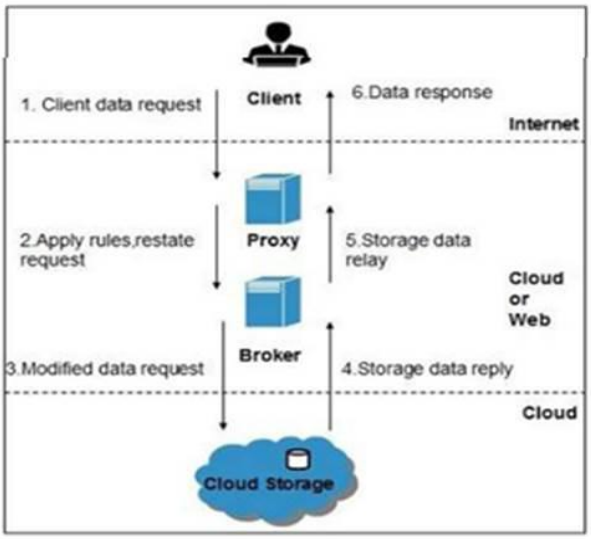
- The notion of how cloud services are deployed is often used interchangeably with where they are provided, which can lead to confusion. For example, public or private clouds may be described as external or internal clouds, which may or may not be accurate in all situations.
- The manner in which cloud services are consumed is often described relative to the location of an organization's management or security perimeter (usually defined by the presence of a firewall). While it is important to understand where security boundaries lie in terms of cloud computing, the notion of a well-demarcated perimeter is an anachronistic concept.
- The manner in which cloud services are consumed is often described relative to the location of an organization's management or security perimeter (usually defined by the presence of a firewall). While it is important to understand where security boundaries lie in terms of cloud computing, the notion of a well-demarcated perimeter is an anachronistic concept.
- The re-parameterization and the erosion of trust boundaries already happening in the enterprise is amplified and accelerated by cloud computing. Ubiquitous connectivity, the amorphous nature of
- information interchange, and the ineffectiveness of traditional static security controls which cannot deal with the dynamic nature of cloud services, all require new thinking with regard to cloud computing. The Jericho Forum has produced a considerable amount of material on the re-parameterizations of enterprise networks, including many case studies. The deployment and consumption modalities of cloud should be thought of not only within the context of 'internal' vs. 'external' as they relate to the physical location of assets, resources, and information; but also by whom they are being consumed by; and who is responsible for their governance, security, and compliance with policies and standards. This is not to suggest that the on-or off-premise location of an asset, a resource, or information does not affect the security and risk posture of an organization because they do —but to underscore that risk also depends upon:

1) The types of assets, resources, and information being managed
2) Who manages them and how
3) Which controls are selected and how they are integrated. [3]

8. Working of Brokered Cloud Storage Access System

When the client issues request to access data:

- The client data request goes to the external service interface of proxy.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally the proxy sends the data to the client.



All of the above steps are shown in the following diagram:[2]

9. Encryption

Encryption helps to protect data from being compromised. It protects data that is being transferred as well as data stored in the cloud. Although encryption helps to protect data from any unauthorized access, it does not prevent data loss. [2]

Conclusion

The study of Cloud Computing technologies are provide us working behind the Cloud Computing platforms and how many technology work together in Cloud computing. Here in this paper we discussed the Cloud Computing technologies and Security issue which is necessary for Cloud Computing services.

References

[1] Cloud Application Architectures by George Reese, April 2009 First Edition, Published by O'Reilly Media, Inc.

[2] http://www.tutorialspoint.com/cloud_computing/cloud_computing_overview.

[3] An Study of Security Issues & Challenges in Cloud Computing by Mili Patel, Rakesh Patel, Department of Information Technology of Kirodimal Institute of Technology Raigarh (C.G.), India.

[4] Cloud Architecture Patterns by Bill Wilder, 2012-09-20 First release, by O'Reilly Media, Inc.