ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Cloud Computing Concepts, Securities issues, and its techniques

Dimpi Rani[1], Rajiv Kumar Ranjan[2]

M.Tech (CSE) Student, Arni University, Indora, Kangra , India[1]

Assistant Professor, Dept. Of CSE, Arni University, Indora, Kangra, India[2]

Abstract: "Cloud" computing – a relatively recent term, provides virtualization, distributed computing, utility computing, and more recently networking, web and software services. It defines the paths ahead in computer science world. Cloud facilitates its users by providing virtual resources via internet and helps to increases its capacity or add capabilities to create new infrastructure .It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing becomes the fast growing segments of the IT industry. But many organization and individuals companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Security is one of the major issues which reduces the growth of cloud computing Users of cloud save their data in the cloud hence the lack of security in cloud can lose the user's trust .This paper discusses the concept of "cloud" computing, its securities issues its technology it tries to address, challenges and possible applications. This paper is not only a clear picture of what the cloud does extremely well and a brief overview of them, but also describes their benefits. criteria and challenges ahead of them. Cloud computing is another name for Internet computing

Keywords: Cloud Computing , Internet, cloud technology, cloud security, security threats.

I. INTRODUCTION

Cloud computing popularity becomes a major trend in IT. While industry has been pushing the Cloud research agenda at high pace, academia has only recently joined, as can be seen through the sharp rise in workshops.Cloud computing is the next generation in computation. Maybe Clouds can save the world; possibly people can have everything they need on the cloud. Cloud computer provides services such as Platform as a Service (PaaS) and Software as a Service (SaaS) and Infrastructure as a Service (IaaS) for consumers. Cloud computing is a computing technology that has very specific. National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is popular in organization and academic today because it provides its users scalability, flexibility and availability of data. Also cloud computing reduces the cost by enabling the sharing of data to the organization. Google apps is an example of cloud computing. However Cloud provides various facility and benefits

II. CLOUD COMPUTING-CONCEPTS

CLOUD: The term cloud represents as internet or large network environment and based on how the internet is depicted in computer network diagrams and is an abstraction for the complex infrastructure it conceals.

COMPUTING: The broader term of "computing" encompasses: computation coordination logic storage. So Cloud computing is the use of a computing resources (hardware and software) that are delivered as a service over a network. There are basically three most common services models of cloud computing:

2.1 SOFTWARE AS A SERVICE (SAAS):

In SaaS users can simply use of a web-browser and other services. In this level, users do not have control or access to the underlying infrastructure being used to host the software. Examples of SaaS service is Salesforce's Customer Relationship Management software3and Google Docs4 All the applications that run on the Cloud and provide a direct service to the customer are located in the SaaS layer.

2.2 Platform as a Service (PaaS):

In PaaS where applications are developed using a set of programming languages and tools that are supported by the PaaS provider. PaaS provides users with a high level of abstraction Just like the SaaS model, users do not have control or access to the underlying infrastructure being used to host their applications at the PaaS level. Google App Engine and Microsoft Azure6 are popular PaaS examples.

2.3 Infrastructure as a Service (IaaS):

In IaaS service user require computing resources such as processing power, memory and storage. This model is a low level of abstraction that allows users to access the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

underlying infrastructure through the use of virtual machines. IaaS gives users more flexibility than PaaS as it allows the user to deploy any software stack on top of the operating system. Amazon Web Services' EC2 and S37are popular IaaS examples. Many industry, such as Microsoft, Google, and IBM, have provided their initiatives in promoting cloud computing.. Big IT companies are also uses Cloud for data security.

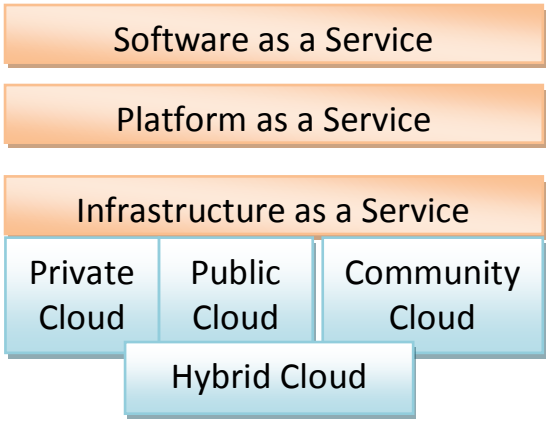


Figure1: An overview of the common deployment and service models in cloud computing .

Deployment model of cloud computing:-

1. Private Cloud:- It is also known as Internal Cloud or on-premises Cloud. It is managed and operated by single organization or a group. It is also known as internal cloud or on-premise.

2. Public cloud: This cloud that can be used (for a fee) by the general public. Public clouds require significant investment and are usually owned by large corporations such as Microsoft, Google or Amazon.

3. Community cloud: This cloud is shared by several organisations and is usually setup for their specific requirements. The Open Cirrus cloud testbed could be regarded as a community cloud that aims to support research in cloud computing.

4. Hybrid cloud: This cloud using a mixture of the above three deployment models. Each cloud in a hybrid cloud could be independently managed but applications and data would be allowed to move across the hybrid cloud.

Drivers of Cloud Computing:-

Cloud Computing is rapidly growing area in the IT because of its popularity. The major driving thought Cloud providers present in the current market segment are Amazon, Microsoft, Google, IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Salesforce, Rackspace and there are many different vendors offering different Cloud services.

1. Amazon: Amazon Web Services including the Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), etc. Provides a highly scalable computing platform to the customer with high flexibility and availability to build a wide range of applications.

2. Google: Google App Engine- It supports application programming interfaces for the data store, image manipulation, Google accounts and e-mail services.

3. Microsoft: Windows Azure Platform Windows Azure platform is a group of Cloud technologies which provides a specific set of services to application developers.

Essential Characteristics of Cloud Computing:-

1. On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2. Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

3. Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

4. Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

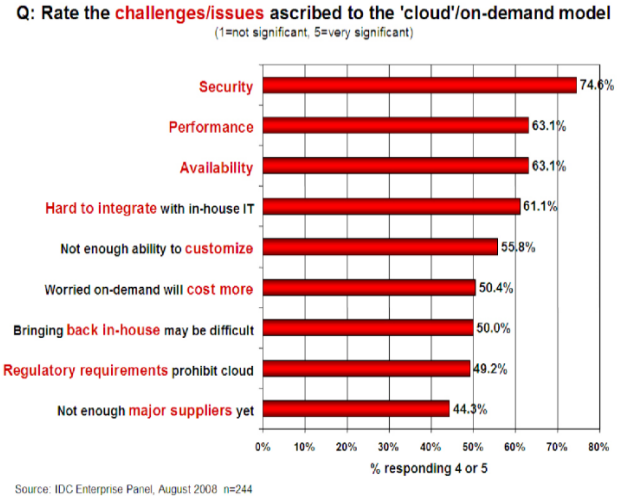
5. Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability (pay-per-use basis) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

III. CLOUD COMPUTING SECURITY ISSUES

Organization uses various cloud services such as IaaS, PaaS, SaaS and the models like public, private, hybrid. Each models and services has various cloud security issues. Each service model is associated with some issues. In security Each user wants to their secure data So security of Cloud is very big issue for every organization. For every user cloud is like financial institutions where a customer deposits his cash bills into an account with a bank. The statistical graph represents the results of the survey which was conducted by the IDC (International Data Corporation) in August, 2008 regarding the challenges/issues which mainly affect the performance of Cloud Computing. And the results show security at the top of the list which declares its importance compared to other parameters of Cloud Computing.



Their are certain rules which helps for security:-

1. For privacy and security of user storage data cannot be managed or viewed by anyother (including operator).

2. At runtime user's data cannot be viewed or handled by any other (loaded to system memory).

3. During transferring of user data through internet must be in secure way.

4. Authentication and authorization needed for users to access their data. Users can access their data through the right way and can authorize other users to access.

IV. CLOUD COMPUTING SECURITY THREAT

The threats is information which is residing in the cloud. There are many threats to which effect the user data. We briefly discuss some of the threat, highlighting what is genuinely different and new in a world of cloud hosting, what threats are similar to the dominant model of local applications Their are different types of cloud security threats which effects the cloud.

1. Insider user threats: The threat of insiders accessing customer data held within the cloud is greater as each of the delivery models can introduce the need for multiple internal Users such as SaaS – cloud customer and provider administrators. PaaS- application developers and test environment managers and IaaS- third party platform consultants.

2. External attacker threats: The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data. This includes the threat of hardware attack, social engineering and supply chain attacks by dedicated attackers.

Types of Attackers in Cloud Computing :-

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involvedin traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers that can be divided into two groups.

1. Internal attackers:- An internal attacker has the following characteristics:

- Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service

- May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role

- Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.

2. External attackers: An external attacker has the following characteristics:

- Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service.

- Has no authorized access to cloud services, customer data or supporting infrastructure and applications

•Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service

V. TECHNIQUES TO SECURE DATA IN CLOUD

1. User Authentication and Identity: Authentication of users and its identity plays an important role in securing of data . User can authenticate by using its passwords that is known individually, or in the form a measurable quantity like finger print.Authentication of users takes place in various ways like in the form of passwords that is known individually, in the form of a security token, or in the form a measurable quantity like finger print.

2. Cryptography: If user wants to store their confidential information by using cryptography techniques. Passwords and Firewalls is good techniques but it is not too much secure. With Cryptography techniques User can encrypt and decrypt data by using cryptographic algorthims. If any one wants to read the encrypted data they should have the secret key or password.

3. Information integrity and Privacy:A conveninent way to privacy the data information integrity which provide mutual trust between provider and user. Some secured access mechanisms should be provided like RSA certificates, SSH based tunnels.

4. Availability of Information(SLA): Non availability of information or data is a major issue regarding cloud computing services. It is a trust bond between consumer and provider. An way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability.

CONCLUSION

Cloud computing is an emerging computing paradigm that is increasingly popular. These applications have a large numbers of advantages like platform independency, cost of service, number of users and etc. The socio-technical aspects of cloud computing that were reviewed included the costs of using and building clouds, the security, legal and privacy implications that cloud computing raises as well as the effects of cloud computing on the work of IT departments. The technological aspects that were reviewed included standards, cloud interoperability, lessons from related technologies, building clouds, and use-cases that presented new technological possibilities enabled by the cloud.This paper describes some of the cloud concepts and securities issues releated with cloud demonstrates the technology used in cloud.. Although there are various security challenges in cloud computing but in this paper, we have discussed some of them and also the techniques to prevent them, they can be used to maintain the secure communication and remove the security problems.

REFERENCES

1. Balachandra Reddy Kandukuri ,RamakrishnaPaturi, Dr. Atanu Rakshit,"Cloud Security Issues ", pp.517-520, 2009 IEEE International Conference on Services Computing,
2. John Harauz ,Lori M. Kaufman,Bruce Potter," Data Security in the World of Cloud Computing " IEEE Security and Privacy July 2009.pp. 61-64
3. Satyendra singh rawat & Mr. Alpesh Soni (2012) ,A Survey of Various Techniques to Secure Cloud Storage
4. VOUK, M. A. 2008. Cloud computing Issues, research and implementations. In Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on, 31-40.
5. R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing
6. Satyendra singh rawat & Mr. Alpesh Soni (2012) ,A Survey of Various Techniques to Secure Cloud Storage
7. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Ensuring Data StorageSecurity in Cloud Computing", 2009 , Page(s): 1 –9
8. Kreimir Popovi, eljko Hocenski, "Cloud computing security issues and challenges", May 24-28, MIPRO, 2010 Proceedings of the 33rd International Convention , Page(s):344-349