

A Survey on Cloud Computing Security, Challenges and Threats

Rajnish Choubey¹, Rajshree Dubey², Joy Bhattacharjee³

1 Assistant Professor, Dept. of CSE, TCT, Bhopal, India

2. Assistant Professor, Dept. of CSE, SIRTE, Bhopal, India

3 Assistant Professor, Dept. of CSE, TCT, Bhopal, India

ABSTRACT

Cloud computing is an internet based model that enable convenient, on demand and pay per use access to a pool of shared resources. It is a new technology that satisfies a user's requirement for computing resources like networks, storage, servers, services and applications, without physically acquiring them. It reduces the overhead of the organization of maintaining the large system but it has associated risks and threats also which include – security, data leakage, insecure interface and sharing of resources and inside attacks.

Keywords : Cloud Computing, on demand, pay per use, threats, data leakage

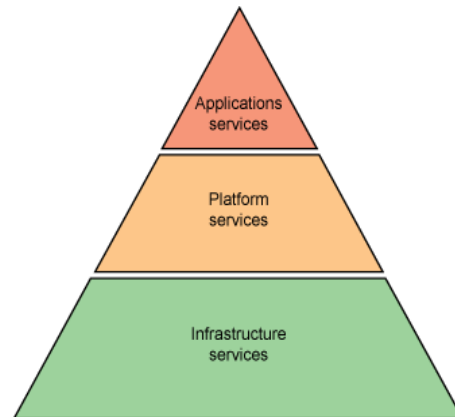
1. INTRODUCTION

Cloud Computing is not new for computer users, the concept behind cloud computing have been in use for decades. Cloud computing can be thought as ability to share computing resource among many different users [1]. In early days of computing there was a single computer, located at a remote data centre and shared by many users (companies). The computer was used to allocate and manage resources to many users and users can request for more or less computing time. Another analogy to cloud computing is that we can generate electricity by using a generator or we can have a connection with electricity board and pay for the electricity used. The later is similar to cloud computing.

Definition of cloud computing:

- Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, services etc, that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].
- Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Examples of such nodes include end user computers, data centers, and Cloud Services. We term such a network of nodes as a Cloud [2].
- A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and **virtualized** computers that are **dynamically provisioned** and presented as one or more unified computing resources based on **service-level agreements** established through **negotiation** between the service provider and consumers.”- Rajkumar Buyya, University of Melbourne[3].

2. CLOUD ARCHITECTURE



Architecture1 [3],

Fig. 1

- Application Services (services on demand)
 - Gmail, GoogleCalender
- Platform Services (resources on demand)
 - Google Appengine
- Infrastructure as services (physical assets as services)
 - IBM Blue house, VMWare, Amazon EC2, Microsoft Azure Platform, Sun Parascale etc.

Architecture 2

As you can see in Fig. 2, at first, user select a Cloud service under the Interface, then the System Management choose the appropriate service, next this service is started and at last launches appropriate data and web application [2].

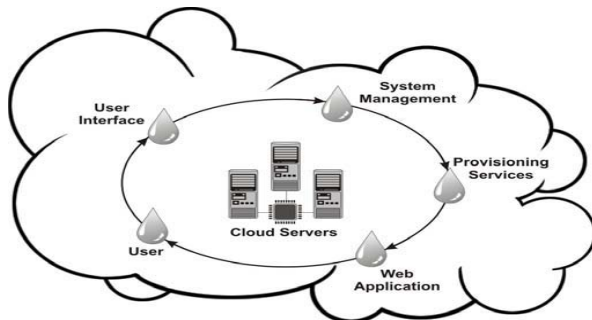


Fig. 2

I. Cloud computing deployment models

Private Cloud – The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.

Community Cloud- Several organizations that have similar policies, objectives, aims and concerns share the cloud infrastructure.

Public Cloud-A large organization owns the cloud infrastructure and sells cloud services to industries or public.

Hybrid Cloud-It is combination of two or more clouds. It enables data and application portability [1].

Each deployment model is either internal or external. Internal clouds are covered under organizations security policy but external clouds are not

II. Advantage of Cloud Computing.

Cloud computing offers lots of advantages:

- *Cost- As in the clouds the user need not own the resources, it just need to pay as per the usage in terms of time, storage and services. This feature educes the cost of owning the infrastructure [1], [2].*
- *Performance-the performance is improved because the cloud is not a single computer but a large network of powerful computers resulting in high processing power [1], [3], [5].*
- *Freedom from up gradation and maintenance- the cloud infrastructure is maintained and upgraded by the cloud service provider [2], [3].*
- *Scalability- The user is can request to increase the resources if the area of application grows or new functionality is added. On the other hand if requirement shrinks the user can request to reduce the resources as well [3], [4].*
- *Speedy Implementation- Time of Implementation of cloud for an application may be in days or sometimes in hours. You just need a valid credit card and need to fulfill some online registration formalities [2], [3], [5].*
- *Its Green- The cloud computing is a green technology since it enable resource sharing among users thus not requiring large data centers that consumes a lot of power [4], [5].*
- *Mobility- We don't need to carry our personal computer, because we can access our documents anytime anywhere [2][3].*
- *Increase Storage Capacity- In Cloud computing we have extreme resources for storing data because our storage consists of many bases in the Cloud. Another thing about storing data in the Cloud is that, because of our data in the Cloud can automatically duplicated, they will be more safety [1], [3].*

III. Disadvantage of Cloud Computing

There are certain security threats and issues of implementing Cloud computing:

- *Data Loss-Customers are responsible for the security of their data, thus in any case if data is lost the customer is in deep trouble [1], [3], [4],[7].*
- *Account Hijacking-Since No native APIs are used for login and anyone can easily register himself as cloud service user chances of hijacking ones account are very high.[1], [3].*
- *Control over the process – in cloud computing the user have very less or no control over the services [3], [4].*
- *Insider attacks by Cloud Service Provider-It may possible that a fraudulent employee may do the fishing and steal the data [1], [4], [7].*
- *Legal aspects-In case of Data loss the user may suffer if there is no Service Level Agreement (SLA), the loss will be of user, because he is not able to put claims against the cloud service provider [1], [4], [7].*
- *Jurisdiction-If the service provider and the user are from different countries then in case of any dispute which country's laws were enforced? This is a big drawback from user's point of view, since the user has opted for the cloud computing for saving costs and the cost of getting legal services is very high [1], [4], [7].*

- Portability/Migration from one service provider to other-Different Service providers have different architecture hence it is difficult for a user to migrate from one cloud service provider to another[3], [4], [7].
- Reliability of cloud service provider-There is lack of standards for cloud computing, hence the reliability of a cloud service provider is largely dependent on its past functioning in similar or other fields [4], [7].
- Auditability - The cloud service provider is not under any kind of audit net. It is possible that the service provider has outsourced some services to a third party and the functioning is not transparent and the user can not inspect the process [3], [4], [7], [8].
- Quality of Service (QoS) in clouds-At present the focus of cloud service providers is on cost effectiveness and fast services therefore QoS in Cloud Computing is an unattended area[4], [7], [8].

IV. The tradeoff between cost and security

Following approaches may be adopted to make cloud computing more secure and convenient while keeping the cost of implementing cloud low [4], [5], [7], [8]:

- When a user registers for any cloud computing services, strict validation check should be applied about the user's background.
- The Cloud Service Provider and the user must sign a Service Level Agreement (SLA), clearly defining the role and responsibilities of both parties and terms and conditions of contract breakup.
- Accountability for data loss (if any), because of the cloud service provider need to defined and measures of data backup should be there.
- The Cloud Service Provider must ensure strict authentication and validation policy for employees.
- There should be an audit process for the cloud service providers.
- Frame a minimal set of standards for cloud computing.
- The cloud service providers should be accredited.

3.CONCLUSION

Where Cloud computing is Applicable-Cloud computing is useful [1], [3], [4], [6], [8]:

- When the applications, processes and data are loosely coupled or they are largely independent This makes it easier to switch to cloud.
- When the data, process and behavior can be shared within an application on well defined points.
- When security of data and information is not at top priority in other words lower level of security is ok with the application and it does not affect the credibility of the company.
- When the core internal architecture of the organization is strong and healthy, because it can easily mapped to cloud architecture.
- When the Web browser can be used as a platform to access the cloud services or no native APIs are required.
- When you are looking for a low cost and effective application.
- When the application is new and to be launched and accessed using the cloud.

Cloud computing is not Useful/Applicable [1], [3], [4], [6], [8]:

- When the applications, processes and data are tightly coupled or interdependent.

- When there are not well defined points to share the data, process and behavior within an application.
- When the application require a very high level of security.
- When you want total control on your processes and data and thus can not outsource your application or its critical components.
- When the core internal architecture of the organization is not functioning well, then first make it strong so that it can be easily mapped to cloud architecture.
- When you need native APIs, since the cloud does not provide native APIs.
- When you are already using a legacy system, since older systems posses number of difficulties to move to cloud architecture.

4.REFERENCES

- [1] David S. Linthicum, Cloud Computing and SOA Convergence in your Enterprise, Pearson, 2010.
- [2] Mehrdad Mahdavi Boroujerdi, Soheil Nazem, Cloud Computing: Changing Cogitation about Computing, World Academy of Science, Engineering and Technology 58 2009.
- [3] R. Buyya, C. S. Yeo, and S. Venugopa, "Marketoriented Cloud Computing: Vision, hype, and reality for delivering it services as computing utilities", in Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, IEEE CS Press, Los Alamitos,CA, USA) 2008.
- [4] Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March 2010.
- [5] Amazon web service, [Online]. Available: <http://aws.amazon.com/>
- [6] Armbrust, M., Fox, A., Griffith, R. et al. Above the Clouds: A Berkeley View of Cloud Computing. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.
- [7] Brodtkin, Jon. (2008, 07):Seven Cloud-Computing security risks, available online, <http://www.infoworld.com/d/securitycentral/gartner-seven-cloud-computing-security-risks-853>
- [8] Controlling Data in the Cloud: Outsourcing computation without Outsourcing Control, Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina Elaine Shi, Jessica Staddon Parc, CCSW'09, November 13, 2009, Chicago, Illinois, USA.