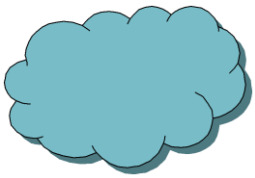
Problems Faced by Cloud Computing

Security in any Distributed system is always a challenge; it does not end with User Authentication or Digital Certificates

Author:L0rd CrusAd3r
Email : lord.v5111@gmail.com



INTRODUCTION

Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be deployed by the vendor, and used by the client. It also shares necessary software's and on-demand tools for various IT Industries. Amazon is the first company to look into the growing importance of Cloud computing very seriously followed by Google and IBM. Some of the other companies which make use of Cloud are Salesforce.com, Zoho, Rackspace, Microsoft.

Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises.

The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to Cloud it's more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud.

IBM had differentiated Cloud into three types according to the usage. They are Private Cloud, Public Cloud and Hybrid Cloud. The Private Cloud is owned by a single organization and Public clouds are shared on a larger scale. Private cloud provides better control and more flexibility. Hybrid cloud is a combination of Private cloud and Public Cloud which is used by most of the industries.

The advantages of cloud computing may be very appealing but nothing is perfect. Cloud got many issues when it comes to security especially on Data theft, Data loss and Privacy.

Security Issues faced by Cloud computing

When it comes to Security, cloud really suffers a lot. The vendor for Cloud must make sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud. Some of the problem which is faced by the Cloud computing,

1. Data Integrity
2. Data Theft
3. Privacy issues
4. Infected Application
5. Data loss
6. Data Location
7. Security on Vendor level
8. Security on user level

Data Integrity

When a data is on a cloud anyone from any location can access those data's from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data's. Thus there is a lack of data integrity in cloud computing

Data Theft

Most of the cloud Vendors instead of acquiring a server tries to lease a server from other service providers because they are cost affective and flexible for operation. The customer doesn't know about those things, there is a high possibility that the data can be stolen from the external server by a malicious user.

Privacy Issues

The Vendor must make sure that the Customer Personal information is well secured from other operators. As most of the servers are external, the vendor should make sure who is accessing the data and who is maintaining the server thus enabling the vendor to protect the customer's personal information.

Infected Application

Vendor should have the complete access to the server for monitoring and maintenance, thus preventing any malicious user from uploading any infected application onto the Cloud which will severely affect the customer.

Data Loss

Data loss is a very serious problem in Cloud computing. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers won't be able to access those data's because data is no more available for the customer as the vendor shut down.

Data Location

When it comes to location of the data nothing is transparent even the customer don't know where his own data's are located. The Vendor does not reveal where all the data's are stored. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world.

Security on Vendor level

Vendor should make sure that the server is well secured from all the external threats it may come across. A Cloud is good only when there is a good security provided by the vendor to the customers.

Security on User level

Even though the vendor has provided a good security layer for the customer, the customer should make sure that because of its own action, there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud.

PROTECTING THE CLOUD

A Secure cloud is always a reliable source of information thus protecting the cloud is a very important task for security professionals who are in charge of the cloud.

Some of the ways by which a cloud can be protected are Protection of data, making sure data is available for the customers, delivering high performance for the Customers, using Intrusion Detection System on Cloud to monitor any malicious activities, to make sure the application used by the customer is safe to use, Vendors must provide a support system for the customer, customer should be able to recover any loss of data in the cloud.

Most important of them all is that, there should be a good degree of encryption provided by the vendor to the customer that only the customer should be able to access the data and not the malicious User.

Conclusion

Both the Vendor and the customer should make sure that the cloud is safe from all the external threats, thus there will be a mutual understanding between the customer and the vendor when it comes to the security on Cloud.