SECURITY ISSUES IN CLOUD COMPUTING

[1]Rejoice Paul, [1]Mansi Talreja, [1]Aman Sahu and [2]K. John Singh,

[1]School of Information Technology and Engineering
[2]Assistant Professor (Selection Grade),
School of Information Technology and Engineering
VIT University,
Vellore, Tamil Nadu,
India

***Abstract*-Cloud Computing is a way through which data are stored on networked resources , enabling the data to be accessed from any corner of the world. Cloud Computing is an emerging platform for sharing resources like infrastructure, software and various applications. Cloud computing infrastructure consists of reliable services delivered through data centers and built on servers. Now, Cloud computing can be seen a lot on the internet. Apple and google are one of the top IT companies that use cloud computing. Companies are now realising that by using cloud computing they can gain access to best business applications and boost their business resources at less cost. But As more and more data is being stored on the cloud, concerns are starting to grow about security issues in cloud computing. In this paper, the various security risks of Cloud Computing are analyzed and presented.**

Keywords-Cloud Computing, Security risks , privacy

I. INTRODUCTION

Cloud computing is one of the fastest growing segment of IT industry today . Companies are increasingly using cloud computing for their business. Cloud Computing has become a major part in today's IT sector. It is an Internet based computing where data and information are stored on networked resources, enabling it to be accessed from anywhere in the world. Cloud computing has become the top platform for sharing data and information over the internet. Cloud computing is emerging but along with it the security issues are also emerging. It has many advantages and benefits but it also entails many security risks and issues in it. Google one of the top technology company which has invested a lot of money on Cloud computing recognizes that having a reputation for security is necessary to have success. Users must avoid companies that do not provide information on security. They need to trust the cloud provider that their information will not be misused. With cloud computing users and companies are frequent victims of hacking and data loss. Hence It is necessary to analyze the security issues in cloud computing and make cloud computing more secure and safe.

II. SERVICE MODELS OF CLOUD COMPUTING

1) Cloud computing is divided into 3 different services:

A. Software as a Service (SaaS)

Applications are hosted and delivered online through a web browser offering desktop functionality.

B. Platform as a Service (PaaS)

The cloud provides the software platform for systems.

C) Infrastructure as a Service (IaaS)

A set of virtualized computing resources, such as storage and computing capacity are hosted in the cloud.

2) Cloud Computing is also differentiated by visibility.

A. private clouds

Services are provided to trusted users through a single tenant operating environment. Organization's data centre delivers cloud computing services to clients who may or may not be in the premises .

B. Public clouds

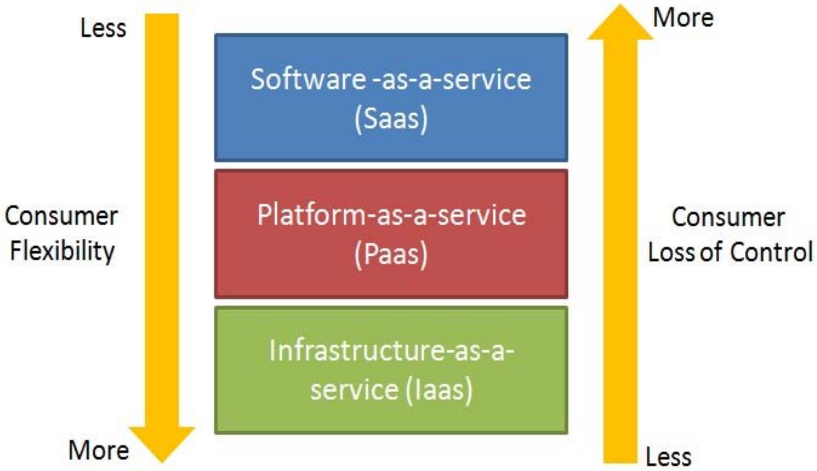
Services are offered to individuals and organizations who want to retain elasticity and accountability without the full costs of infrastructures .

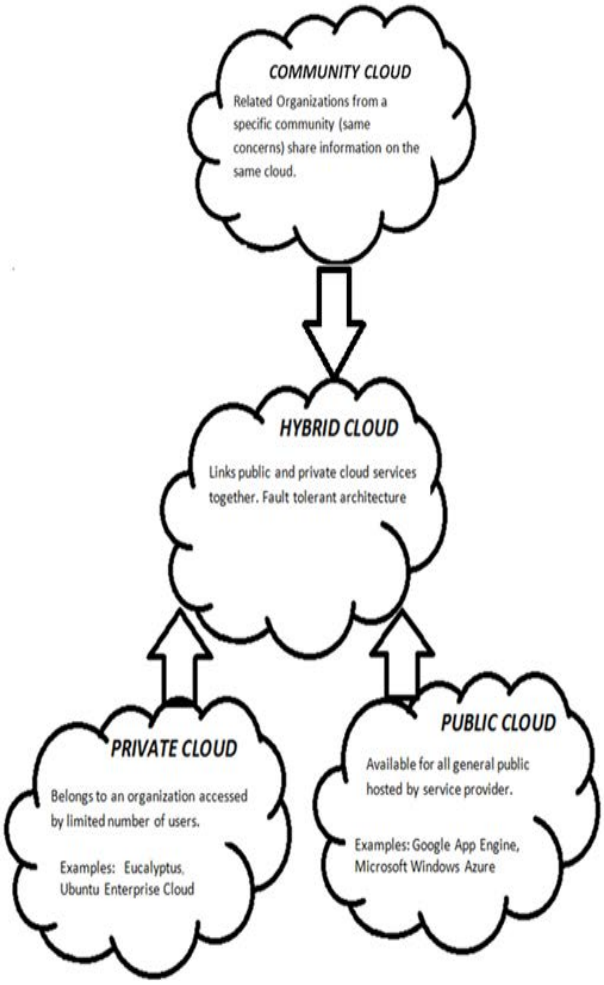
C. hybrid clouds

It is the combination of private and public cloud service offerings.

D. Community cloud

Organizations share information on the cloud managed by themselves or a third party and hosted by service provider.


Less
Consumer Flexibility
More
Software -as-a-service (Saas)
Platform-as-a-service (Paas)
Infrastructure-as-a-service (Iaas)
More
Consumer Loss of Control
Less


COMMUNITY CLOUD
Related Organizations from a specific community (same concerns) share information on the same cloud.
HYBRID CLOUD
Links public and private cloud services together. Fault tolerant architecture
PRIVATE CLOUD
Belongs to an organization accessed by limited number of users.
Examples: Eucalyptus, Ubuntu Enterprise Cloud
PUBLIC CLOUD
Available for all general public hosted by service provider.
Examples: Google App Engine, Microsoft Windows Azure

III. SECURITY RISKS IN CLOUD COMPUTING

There are many security concerns that has to be considered while using cloud computing.

A. Confidentiality

The Cloud providers sometimes hire third party companies to store data and information of their customers. It is possible that they can use the data and expose it. The cloud providers have to make sure that the personal information in not being shared with third party companies.

B.Data Integrity

When data is on the cloud anyone can access them.Cloud does not differentiate between sensitive data and common data thus enabling anyone to access those sensitive data. It leads to lack of data integrity in cloud.

C.Data Theft

Most of the cloud providers try to lease a server from other service providers because it reduces cost and makes operations more flexible. There is a high chance that the data stored in their servers can be stolen by a malicious user.

D.Data loss

If the cloud provider shuts down due to some problems there will be a loss of data for the customers. The customers won’t be able to access those data because it is no more available for the customer as the cloud provider does not exist anymore.

E.Data location

The customer don’t know where his own data is located. The Cloud provider does not reveal where all the data are stored. The Data’s won’t even be in the same country of the Customer, it might be located anywhere in the world.

F.Deletion of Data

There are possibilities that the data which is no longer needed is deleted by the user but is still there somewhere in the cloud. It is a serious problem in the cloud. Customers must be vigilant and make sure that data deleted from the cloud is no longer kept. The cloud providers must make sure that the data which the customer deletes is completely removed from the cloud.

G.Malicious Insiders

A Cloud provider does not give information on how it grants employees access to data and information in the cloud. The customers do not know whether the employees in the Cloud company are granted access data stored. The customers data can be easily exposed by an employee of the cloud company. The cloud providers must follow guidelines and polices for preventing employees from accessing data and information of its customers.[3]

H.Account or Service Hijacking

In Cloud computing a hacker can easily hijack a customer’s or user’s account and can easily manipulate and steal confidential data of the the user. A customer would never want his data or information to be stolen. The cloud providers must put strong protection and prevent hackers and malicious people from gaining access to its customer’s data and information.

I.Data Segregation

Data can be stored in the shared mode or in private mode as per the user wishes. Mostly user’s data and information is kept in the shared environment. Due to this there is high chance that the user’s private data can be seen by other users.

J.Users

While cloud services, users' activities such as clicking links in e-mail messages, Instant Messaging, visiting fake web sites, etc. can download malware to a local workstation. The malware can launch attacks on your internal network.

IV.STEPS TO MAKE ClOUD COMPUTING MORE SECURE

A. Making sure that staff don’t suddenly gain access privileges they are not supposed to.

B. Installing exception monitoring systems.

C. Be carefull to develop good policies around passwords;How they are created, protected and changed.

D. Check whether any third party companies are able to access your data.

E. When a user registers for any cloud computing services, strict validation check should be applied.

F. The Cloud Service Provider and the customer must sign an Agreement stating the responsibilities of both parties and terms and conditions of contract breakup.

G. In case of Data loss, measures of data backup should be there in the cloud.

H. The Cloud Provider must have strict authentication and validation policy for employees.

I. There should be a minimal set of standards for cloud computing.

J. The cloud providers should be accredited, trustworthy and reputed.

CONCLUSION

Cloud computing is emerging as the various organisations that are developing cloud services are evolving. Cloud computing is in evolving stage and hence the security solutions are not yet complete. Even the leading cloud computing providers such as Amazon, Google etc are facing many security issues. With security issues in cloud computing, decision to adopt cloud computing could only be based on the benefits to risk and threat ratio.

REFERENCES

[1] Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee, “A Survey on Cloud Computing Security, Challenges and Threats**”,** International Journal on Computer Science and Engineering (IJCSE)[J]. pp 1227-1231

[2] Krishna Chaitanya.Y, Bhavani Shankar.Y, Kali Rama Krishna.V, V Srinivasa Rao. “Study of security issues in cloud computing”, International Journal of Computer Science and Technology. pp 51-53

[3] Anthony Bisong, Syed (Shawon) M. Rahman, “An overview of the security concerns in enterprise cloud computing “,International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011. pp 30-45

[4] Kevin Hamlen,Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham,” Security Issues for cloud computing” , International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010. Pp 39-51

[5] Rizwana Shaikh, M. Sasikumar,” security Issues in Cloud Computing: A survey “ , International Journal of Computer Applications (0975 – 8887) Volume 44– No19, April 2012”, pp 4-10