Security Related Issues in Cloud Computing: A Survey

Palkesh Soni
Department of Computer Science & Engineering
Acropolis Technical Campus Indore, India

Ankit Upadhyay
Department of Computer Science & Engineering
Acropolis Technical Campus Indore, India

Arvind Maheshwari
Department of Computer Science & Engineering
Acropolis Technical Campus Indore, India

Prashant Lakkadwala
Department of Computer Science & Engineering
Acropolis Technical Campus Indore, India

Abstract

Cloud computing is a type of computing model in which services are delivering through which resources are accessed from a centralized pool of resource. The cloud management software has to manage the resources at large scale. Cloud computing has become an alternative means of internet for this computing world. Cloud represents ubiquitous computing means that it found everywhere. Cloud user and the cloud service provider are the two main units involved in cloud computing. Also, a cloud broker can be exists. Since a cloud is the set of many nodes, which can support a variety of application which is used by the clients on the basis of pay per use. By its pay per use characteristics cloud computing is very popular now a days.However, there are issues and problems in regarding of cloud computing security which is becoming a competitive boundary among various cloud service providers. In this survey paper, we introduces in depth analysis of security issues in the cloud computing environment and challenges which are focusing on the types of cloud computing. We shown cloud trust protocol which is a solution approach to limit these challenges and issues.

Keywords: Cloud Computing; Cloud Trust Protocol; Cloud Security

I. INTRODUCTION

Cloud computing is a paradigm, in which computing services are delivered over the internet. Cloud computing provide access to individuals and businesses to use software and hardware as a service that are managed by third party over the internet. Cloud computing allow access to resources and information from any geographic location where network connection is available.

A. Service models of Cloud Computing:

Services that are offered by cloud providers can be classified into three categories.

1) Software as a Service (SaaS) :

In the SaaS model an application is offered to the customer by the cloud service provider. In which application is hosted by the provider at their infrastructure and distributed over the network as a service on demand.

2) Platform as a Service (PaaS) :

Here, in the PaaS model a development environment is offered to the customer which is managed by the provider. On which customer can develop and run their applications without building and managing complex infrastructure.

3) Infrastructure as a Service (IaaS) :

In IaaS model computer resources such as storage, computing capabilities are made available to the customer on demand. It's cost saving model. In this model customer only pay to use IT infrastructure as needed.

B. Deployment models of Cloud Computing:

There are four deployment models of Cloud Computing.

1) Public Cloud:

Public cloud is publicly accessible cloud which is managed by third parties. All customers share a common infrastructure pool with limited configuration. The cloud provider is responsible for creation and ongoing maintenance of the public cloud.

2) Private Cloud:

Private cloud is accessible only by an organization and also managed by the organization. Private cloud enables an organization to use cloud computing by means centralizing access to IT resources from different geographical location.

3) Hybrid Cloud:

Hybrid cloud combine both public and private cloud models. With Hybrid cloud organization can utilize third party cloud provider service in a full or partial manner. Thus, Hybrid cloud increases flexibility of computing.

4) Community Cloud:

Community cloud is a multi-tenant infrastructure which is shared among several organizations. And it is managed, governed and secured by all the participating organization. These organizations have similar cloud requirements and their ultimate goal is to achieve business objective. It is beneficial in order to cost saving

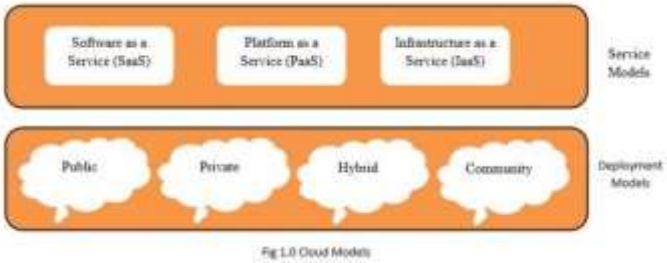

Fig. 1: Cloud Computing Models

II. VARIOUS CLOUD PROVIDER

In this section we clearly explain the cloud storage providing companies with comparison of their existing features like Storage Space, Platform Supported, File Size Limit, Supported File Format, Security Type, Developer Tools, Online Document Editor

S.No	*Features*	*Cloud Storage Providing Companies*		
		Google drive	*One Drive*	*Drop box*
1.	*Storage Space*	*15 GB free and we can Purchase storage plan as per requirement [8].*	*7 GB free and addition plan can be purchased [9].*	*2 GB free and get up to 16 GB referrals [10].*
2.	*Platform Supported*	*ios, Android, Mac, Windows[11].*	*ios, Android, Windows , Mac, Windows Phone [11].*	*ios, Android, Blackberry, Windows, Mac, Linux [11].*
3.	*File Size Limit*	*It support file size up to 10 GB [12].*	*It gives file size limit up to 2 GB [12].*	*It provides file size unlimited [12].*
4.	*Supported File Format*	*It supports Word, Excel, PowerPoint, PDF, Apple Pages, Photoshop, AutoCAD, Xps, Zip, Rar etc[13].*	*It supports Microsoft word, Excel, PowerPoint, OneNote's, photos, and video [13].*	*It supports photos and videos [13].*
5.	*Security Type*	*It has SSL/TLS type security only [14].*	*It provides SSL security only [14].*	*It has SSL and AES 256 bit encryption [14].*
6.	*Developers Tools/API*	*Yes*	*Yes*	*Yes*
7.	*Best For*	*It is best for its web apps [15].*	*It is best for windows/office integration free space [15].*	*It is best for seamless syncing [15].*
8.	*Online Document Editor*	*Google Docs [16]*	*MS office Web Apps [16]*	*Not Available [16]*

III. SECURITY CHALLENGES

Today, cloud computing facing many security challenges including data segregation, authentication, and data recovery, data management. Public cloud increases the highest data explosion and it should be managed properly. Security is main issue because the device used to serve the service doesn't belong to the user themselves. This is great concern when user have valuable and personal information stored in cloud computing services.

A. Data Security:

Data security is a significant task with a lot of complexity. Data protection method such as redaction, truncations, obfuscation, and others, should be taken with great concern. Homomorphism encryption can be used for data security. But with this key management is a problem [1].

B. Data Segregation:

Encrypted data from multiple companies or user may be stored on same hard disk so a mechanism should be there to protect data.

C. Data Recover:

Every service provider should have the data recovery mechanism to recover user data from any disaster [2].

D. Data integration:

Data integrity comprises the following cases, when some human errors occurs when data is entered**.** Errors may occur when data is transmitted from one computer to another; otherwise error can occur from some hardware malfunctions, such as disk crashes. Software bugs or viruses can also make viruses. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing [3].

E. Authentication:

As user keep their valuable information on cloud service across the internet. It can be accessible by unauthorized people. Hence authenticating user cloud should have identity management system [4].

IV. PROBLEM STATEMENT

Any client, organization or enterprise that keeps their data in the cloud is subject to inherent level of risk because outsourced service bypasses the physical, logical and personnel controls of the user [5]. When client is storing data on the cloud he/she might want to make sure if data is stored correctly or retrieved later. The data of client stored in cloud may be enormous and it may be impractical to retrieve all the data. One's purpose is just to make sure that their data is stored correctly. Hence there is need to provide guarantee to a client.

It is very important for both client as well as cloud provider to have mutual trust so that cloud provider make sure their client is not any malicious hacker or attacker. And user can assured of data consistency, data security.

The necessity for developing trust protocols/models is demanding. There is need to assure the client about infrastructure that if any server crashes or user's data grows continuously at very high rate their data will never lost.

In some cases, the user may need to perform block level operations on his data. The most general forms of these operations that we are considering are block update, delete, insert and append.

As users no longer possess their data locally, it is of critical importance to assure users that their data are being correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies.

With multi-tenancy resources are shared by multiple users. For example, two or more tenants could have their OSs running on the same server or two or running an instance of the same application with different data. Depending on the cloud deployment model the level of importance and sharing of multi-tenancy would be different [6]. But without any doubt Infrastructure-as-a-Service (IaaS) in public clouds creates the most risks off all.

It is necessary to adopt virtualization technologies to allow the use of multi-tenant environments. Both give place to a new set of challenges when put together. Virtualization adds a new layer that can be targeted, and multi-tenancy facilitates the process to reach the layer. Virtualization security issues need to be reviewed from a new point of view not seen before, coexisting with possible malicious tenants.

V. SOLUTION APPROACHES

First approach should be that cloud user and cloud provider must make sure whatever request/response they have got is from trusted source by estimating the correctness of data that they have received. This can be done by implementing trust based protocol between user and cloud provider. That will ensure cloud provider as well as user about data consistency and data security of user data.

A. Cloud Trust Protocol (CTP):

The Cloud Trust Protocol is a mechanism that help cloud user to request and retrieve standardized inquiries about cloud provider transparency. CTP is a procedure for establishing digital trust between cloud user and cloud service provider. With the CTP cloud user are provided a way to find important information about security, privacy that is being performed in the cloud. The CTP empower the cloud consumer with right information to make right choices about data what to put in the cloud or leave the cloud and to decide which cloud is best suited for his data.

VI. CONCLUSIONS

Cloud computing is the innovative rising technology which is available on leased basis to its clients and if it issued suitably then it can increase the effectiveness of institutes, reducing management responsibilities, and costing factor. Cloud computing has the potential to turn into a frontrunner in promoting a secure, virtual and economically viable it solution in the future. In this paper key security considerations and challenges which are currently faced in the cloud computing environment are explained clearly. We also concentrate on the security issues which are related to availability or back up, storage location and access of the data. We explained cloud trust protocol which is a protocol which can provide solution to present issues, but we are also working on the solution part in consideration of developing a safe framework in java programming language.

REFERENCES

[1] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009.
[2] L.Arockiam,S.Monikandan & G.Parthasarathy "Cloud Computing: A Survey" http://interscience.in/IJIC_Vol1Iss2/paper5.pdf
[3] Anitha Y "Security Issues in Cloud Computing - A Review" in International Journal of Thesis Projects and Dissertations (IJTPD) Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013.
[4] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam "Research Challenges and Security Issues in Cloud Computing" in International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 342 http://www.academia.edu/2179974/Research_Challenges_and_Security_Issues_in_Cloud_Computing.
[5] Available on http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.
[6] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009, https://cloudsecurityalliance.org/wpcontent/uploads/2011/07/csaguide.v2.1.pdf
[7] Digital Trust in the cloud available on https://cloudsecurityalliance.org/wpcontent/uploads/2011/05/cloudtrustprotocolprecis_073010.pdf.
[8] Available on http://www.google.com/drive/using-drive/
[9] Available on https://onedrive.live.com/about/en-us/compare/
[10] Available on https://www.dropbox.com/features
[11] Available on http://www.bestcloudstorage.net/dropbox-vs-skydrive-vs-google-drive-vs-icloud/
[12] Available on http://www.techradar.com/news/internet/best-cloud-storage-dropbox-vs-skydrive-vs-google-drive-vs-icloud-1120024
[13] Available on http://www.mytechguide.org/11891/cloud-storage-comparison/
[14] Availableon http://www.yummywakame.com/archives/2013/03/31/ cloud-storage-comparison-drop-box-vs-google-drive-vs-skydrive-vs-icloud-vs-box
[15] Available on http://geekotech.com/google-drive-vs-dropbox-vs-icloud-vs-skydrive/
[16] Available on http://www.buzzle.com/articles/dropbox-vs-google-drive-vs-skydrive-which-cloud-storage-is-the-best.html