DATA INTEGRITY, COMPRESSION & SECURITY IN CLOUD : A SURVEY

A. Jeevarathinam[1]

ABSTRACT

Cloud is an internet-based computing technology. With the presence of Cloud computing huge amount of data can be stored and accessed from anyplace. It uses internet and preserves the servers for data storage and other applications with the help of data providers to decrease the preservation process of the information using upload and delete method. Software, Infrastructure and platform are the variety of services provided by the users with the help of Cloud storage. It is cost effective, easy to manage and a powerful resource accessible over the Internet [1].

Data integrity and data compression are the two most significant aspects of Cloud storage. With the help of the integrity control protocol, users can avoid Unauthorized and malicious downloading of outsourced data. With the progress of Cloud services, data security becomes more and more significant in Cloud.

This paper analyses the fundamental difficulty of Cloud data security, integrity and compression [2].

Keywords:

Data integrity, Data Compression, Main Cloud, Remote Cloud.

[1]Assistant Professor, Department of CS, CA & IT, KAHE.

I. INTRODUCTION

Data cache is one of the models of Cloud storage. There are two kinds of formats available to stores data in Cloud computing. Logical pool is one kind of format of digital data, and multiple server the other. Logical and physical storage can be managed with the help of Host Company.

Data availability, accessibility, physical environment protection and running are managed by the Cloud storage provider. Co-located Cloud computer service, a web service Application Program Interface (API) is accessed by Cloud storage [4].

Distributed resources and services belong to different organizations provided with the help of Cloud. Authentication, encryption, decryption and compression are the methods of security services in Cloud environment. Figure 1.1. Shows an architectural view of Cloud.
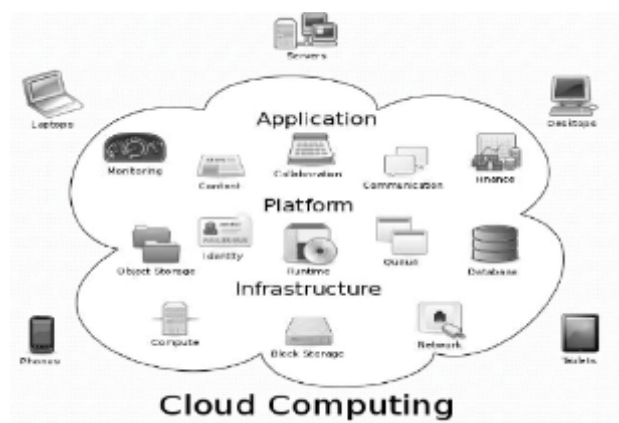

Figure 1.1- Architectural view of Cloud

2 SERVICE MODELS IN CLOUD

The Cloud has three essential features, which are presented below [2].

SaaS

SaaS is the expansion of "Software as a Service". It is a software allocation model in which a third-party provider hosts applications and makes them available to customers over the Internet. With the help of web browser, SaaS applications are run directly. It does not permit the users to download or install the applications. Storage, network and computing resources are managed with the help of Cloud provider .It can distribute the underlying infrastructure. Examples of SAAS: -Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting[1].

PaaS

PaaS is the expansion of "Platform as a Service".It provides Cloud components to certain software while being used mainly for applications. Customers can develop their applications with the help of Paas, because provides the framework for creating applications. A third-party provider can provide all servers, storage space, and network access because of the maintenance of the applications by the customer. Examples of PAAS :- AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift

IaaS

IaaS is the expansion of "infrastructure as a Service". It is made of highly scalable and automated compute resources. Computing, networking, storage, and other services are accessed and monitored by IaaS, since it is

offers self-service and allows businesses to purchase resources on-demand as needed, instead of having to buy hardware outright. Examples of IAAS:- DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE). Figure 2.1. shows service model of Cloud.
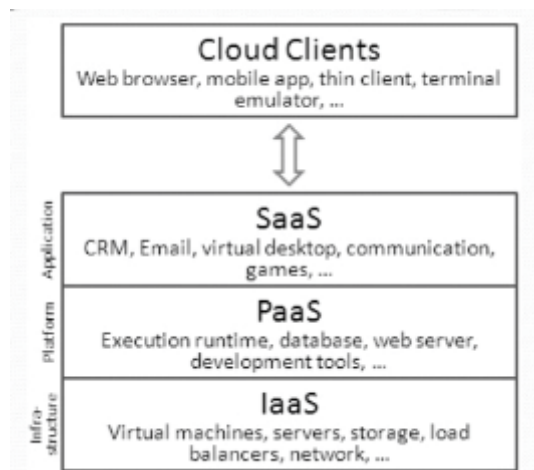

Figure 2.1.shows service model of Cloud.

Five important characteristics of Cloud are described under this section [1].

3 CHARACTERISTICS OF CLOUD

1. On-demand Self-service

On-demand computing is a delivery model in which computing resources are made available to the user as needed. It refers to the service provided by computing vendors that enables the provision of Cloud resources on demand, whenever they are required. Cloud service provider may be maintaining the resources of the user project. With the help of online control panel, the user can access the Cloud services.

2. Broad network access

It makes available access resources in the Cloud over

multiple type of devices .This not only includes the most common devices but also mobile phones, thin clients and so on.

3. Resource Pooling

It is a fundamental premise of scalability in the Cloud. Without pooled computing, networks, and storage a service provider must provision across multiple silos, independent resources with a few or no interconnections. Multi-tenant environments, where multiple customers share adjacent resources in the Cloud with their peers, are the basis of public Cloud infrastructure.

4. Rapid elasticity

It is Cloud terminology for extensible facilities. While clients can ask for and get resources at any time and in any quantity, the Cloud must be able to scale up and down according load demands.

5. Measured service

Cloud system automatically controls and optimizes resources, which are measured by an appropriate type of Cloud service. This is crucial for billing, access control, resource optimization, capacity planning and other tasks.

4. METHOD OF CLOUD

Three significant forms of Cloud storage are described under this section.

1. Data integrity

One of the key challenges in Cloud is maintaining data integrity. In the presence of security mechanisms, the data can be protected because the customer has no power over the security. Securing data is a kind of significant essential mechanisms for storing data in Cloud. In case corruption due to hardware and software failure occur data integrity can protect data. State, process and function are referred by data integrity and it ensures data quality. Cloud service provider can provide a guarantee to the consumer that the record is not converted or damaged.

Auditing is one kind of mechanism for checking the integrity of the data stored in the Cloud. The data performance can be measured by Error Detection rate. Data integrity mechanism is also used for correcting data, apart from error detection rate. In the field of data security, data integrity is an important part of Cloud. At the moment security is a key concern in Cloud. Thus, data integrity mechanism needs to be enhanced. Data integrity is required because of the increasing demand of Cloud in latest technologies. Parameters for measuring the efficiency of data integrity in Cloud are time for processing the data, maintenance cost and memory for storage.

2. Data compression

Data compression is a method of removing redundancies in order to save storage space and cost of Cloud storage. It implies transfer and storage of lesser quantity of bits. It can reduce the size of data using manipulation and modification of bits' structure. Data Compression is required for WSN applications, which have a huge amount of data to be sent across the network, and depending on the importance of data type, one may be better than the other. Data compression techniques include reducing the size of information before transmission. Decompression of data occurs at the base station. In compression it is important that no

information is lost and independent readings are retained [3].

Compression

Compression is the formation of coding. It will completely reduce the total number of bits which will be essential to perform secured data. It makes optimal use of finite storage volume to save time and helps to optimize the resources [7]. In general,

Data + Compression = information - redundancy

Compression ratio :

The term compression ratio means the ratio of the number of bits compressed before to the number of bits compressed after. So, after compression the size of the sensed data will be less. This helps to transmit the information easily.

3. Security

Cloud security is a fast-developing service that provides many of the same functionalities as traditional IT security. This includes protecting critical information from theft, data leakage and deletion. Security and privacy of personal data are the leading concerns in Cloud. Users can log in from any geographical locality to access data, files and applications on Cloud systems. Thus, there is a possibility of an intruder to make a security breach in any manner. So there arise problems of Confidentiality, Integrity and Authenticity (CIA) of the data. Novel and effective method of user authentication are a must to overcome these security issues [5].

5. PROBLEM DEFINITION

Transferring data from main Cloud to remote Cloud using a number of issues is described below:

1. Data integrity can be present even while moving data from remote Cloud to main Cloud.

2. It the presence of malicious attacks, authentication between remote Cloud and main Cloud security can be compromised [8].

3. Data compression can be present for storing data from remote to main Cloud, with the aim of consuming storage space in the remote Cloud

6. PROPOSED SOLUTION STRATEGY

There are three significant approaches to deal with the problems of Cloud as described below-:

1) Using MAC, user can verify uncorrupted transmission by means of data integrity.

2) MAC can provide the Authentication among remote Cloud and main Cloud using HMAC [8].

3) Using LZW compression algorithm, efficient utilization of remote Cloud storage can be implemented [7].

7. A COMPARATIVE STUDY

Comparison between integrity, compression and security is described in the following table.

S.No	Method	Issues	Proposed techniques
1	Data integrity	• Data Loss or Manipulation • Untrusted Remote Server Performing Computation on Behave of User	• Third Party Auditor • Provable Data Possession • Proof of Retrievability • Proof of Ownership

2	Data compression	• high demand for data processing • redundancy	• Compression algorithms(LZW) reduce the redundancy • Increasing effective data density
3	Security	• Virtualization • IP address • Elasticity • Network Insecurity • Insecure APIs • Provider Security • Malfunction Reliability and Availability	• Proof of Retrievability (POR) • Provable Data Possession (PDP) • Using Strong Algorithms [2] Integrity Verification for Static Data

Table : Comparison between integrity, compression & security

8. CONCLUSION

This paper has taken up a combined approach to observe the performance analysis of integrity, compression and security of Cloud storage. In future, improvements on LZW for compression, RSA Secured Hash algorithm for security and MAC algorithm for integrity have to be made for better management of Cloud storage.

REFERENCES

1. Abhijit Choudhury, Santanu Kumar Misra ,Bijoyeta Roy "A brief Survey on Data Integrity and Compression in Cloud Computing", International Journal of Computer Applications (0975 - 8887) Volume 156 - No 13, December 2016

2. K. Muthulakshmi, K.Lalitha,and S.Uma "An Efficient Data Compression And Storage Technique With Key Management Authentication In Cloud Computing", International Journal of Scientific & Engineering Research Volume 9, Issue 1, January-2018 979 ISSN 2229-5518

3. A.Jeevarathinam, Dr.S.Manju Priya," "Data Compression Techniques In Wireless Sensor Networks : A Survey" "Karpagam JCS Vol.12 Issue 2 Jan - Feb 2018

4. A.Jeevarathinam, Dr.S.Manju Priya, "Comparison On Hierarchical Routing Protocols In Wsn" Karpagam JCS Vol.10 Issue 5 July - August 2016

5. Ashwin Dhivakar M R , Prof. D Ravichandran , Dr. Vijay Dakha "Security and Data Compression in Cloud Computing Using blobseer Technique", Special Conference Issue: National Conference on Cloud Computing & Big Data

6. Monika Soni1, Dr Neeraj Shukla2, "Data Compression Techniques in Cloud Computing" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Special Issue 3, November 2016

7. A.Jeevarathinam, Dr.S.Manju Priya, "Comparative Study on Data Compression Algorithm For Wireless Sensor Network, Karpagam JCS Vol.11 Issue 4 May - June 2017

8. V.Kalpana and V. Meena, Study on Data Storage Correctness Methods in Mobile Cloud Computing, Indian Jour