A Report on

**Cloud Computing: Storage Techniques and their Optimization**

**Dr. Syed Iqbal Omar B.SC., M.E, Ph.D.**

CSEN 5303 SECTION 004

CLOUD COMPUTING

**BY**

**SHWETA NOTIYAL K00430349**



Department of Computer Science Engineering

TEXAS A&M UNIVERSITY KINGSVILLE

955 University Blvd, Kingsville, TX 78363

**CONTENTS**

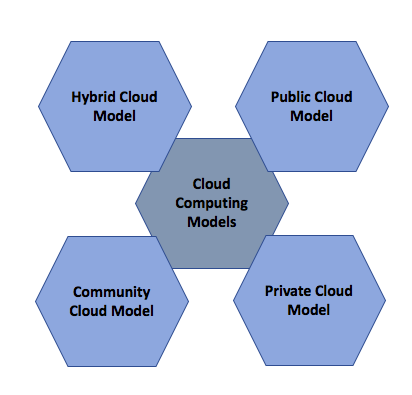
1. Introduction 3
2. Overview of Cloud Computing and Cloud Service Models in terms of Storage as a Service 3
   1. Cloud Computing Models 3
      1. Public Cloud Computing Model 4
      2. Private Cloud Computing Model 4
      3. Community Cloud Computing Model 5
      4. Hybrid Cloud Computing Model 5
   2. Cloud Service Model 5
      1. Infrastructure as a Service
      2. Software as a Service
      3. Platform as a Service
3. Different Cloud Computing Storage Techniques – Advantages and Disadvantages
   1. Secure distributed cloud storage scheme
      1. Storage technique for Static Data
      2. Storage technique for Append-only Data
   2. Optimized multitenant cloud storage
   3. Hierarchic Storage Technique
      1. Security Measures
4. Fog Computing
5. Hierarchic Storage Architecture
6. **INTRODUCTION**

Cloud computing has been evolved in last few decades and it is still not half way through yet of its evolution process. Companies of all forms and magnitudes are remodeling as per this technology. As business is increasing, user demand and data also increases which is directly proportional to storage, i.e. requirement of storage skyrocket. If storage increases than computing parameters like: execution speed, processing power, efficiency, response-time, etc. increases. Managing storage in cloud environment increases the performance, which is usually done by maintaining performance equilibrium of data centers by optimizing the resources of cloud storage. Many data storage optimizing technologies, tools has been proposed till now. This paper summarizes and compared these cloud storage techniques briefly. Analysis of cloud storage is done on the basis of parameters, that is speed, accuracy, efficiency, etc. This paper is concluded with the list of technologies discussed and its advantages and disadvantages.

Data storage is an idea for archiving data in binary or other forms which are used by computer device. In cloud computing term it is called as remote data storage. Remote data storage revolutionized business era and made much easier for users to compute complex application data, which require more storage and efficiency. Cloud computing is the term where services are provided over the internet, i.e. remotely and one of the service are storage. And these services can be private, public, community or hybrid, i.e. services depends on the type of cloud community deployment model.

1. **Overview of Cloud Computing and Cloud Service Models in terms of Storage as a Service.**
   1. **Cloud Computing Models**

The cloud servers various functionality over internet, one of the main service is storage from virtual servers (single or cluster depend on type of model), applications (mobile applications), authorizations of desktop, etc. Below define different types of model [3] :



**Figure 1. Cloud Computing Deployment Models**

* + 1. **Public cloud model**

Mediator service provider provides services over the internet. These services are on-demand, which can be by the minute or by the hour. Customers do not have control over where the infrastructure is situated. As earlier mentioned services are on-demand, which can also defined as pay-as-you-go (terms mostly used by AWS). Cost is usually shared by users or can be free or can be in the form of license policy. Public cloud have major advantage for the organizations that manages the host applications and various other user applications.

* + 1. **Private cloud model**

Private cloud provide assurance of security and privacy to the user. These cloud model are usually accessed by a single user or a group of users or a company. It gives control to organizations over security and data is secured by firewall and managed internally. Private clouds are good for company’s which are more focused on security, authentication, require peak time demands, etc.

* + 1. **Community cloud model**

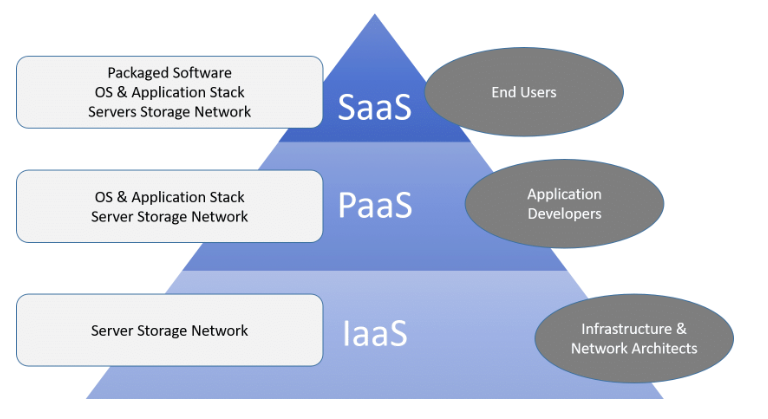
Community cloud shares infrastructures and services between various organization or companies. As the name says, shared within a community. These services are usually provided by a specific group (service provider) that divide computing concerns such as security, authorization access, jurisdiction consideration, etc. A community cloud can be managed and hosted internally or by a third party provider. These cloud is good for companies that need centralized cloud computing for managing their projects.

* + 1. **Hybrid cloud model**

This model is a mix of both private cloud and public cloud, because of which it has more advantage for the user (single or a group or an organization). It provides the user more elasticity as data workload flow rotates between both models and as per which cost is decided which is on-demand. Hybrid cloud model is great for scalability, resilience and security. An example of hybrid cloud model is an organization can use public cloud to interact with customers, while keeping their data secured through a private cloud.

* 1. **Cloud Service Models**

Cloud service model is more focused on providing services at different level of their complexity to the users. These services distributed among end users, application developers and infrastructure and network architects level. Different types of service models are given below:



**Figure 2: Cloud Service Models [3]**

* + 1. **Cloud Software as a Service “SaaS”**

Software as a service, is type of cloud service which provide applications to the clients via web browser. Data for the applications executes on a server i.e. on the network, not through an application on client system. It can also be said as software is provided as a service at application layer. Software is usually vend via subscription. Some main examples of SaaS is Salesforce, Google Docs, Office 365, Basecamp etc.

* + 1. **Cloud Infrastructure as a Service “IaaS”**

Cloud Infrastructure as a service provides hardware as a service and provide virtual O.S to the customer called as “Hypervisor”. These services are charged only for the computational power which is used by the customer. Major service provider examples are Amazon EC2 (Elastic Cloud Computing), Rackspace, Google Compute Engine etc.

* + 1. **Cloud Platform as a Service “PaaS”**

Platform as a service or platform based service provides platform, that allows customer to maintain, execute and build applications without the any issues. It can be delivered in three ways:

* As a public cloud service provider where consumer have control over software deployment with ease and provider provide on-demand network, server and **storage**.
* As a private service, where user does not have control which is done all behind the firewall.
* As software deployed on a public infrastructure as a service.

1. **DIFFERENT CLOUD COMPUTING STORAGE TECHNIQUES – ADVANTAGES AND DISADVANTAGES**

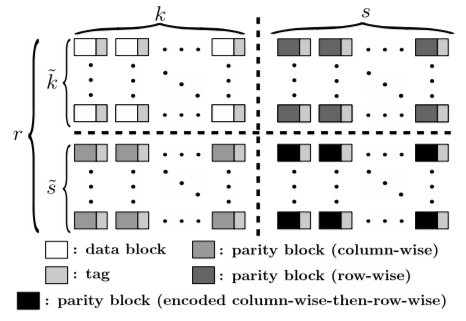
In this report different cloud storage technique related survey is done on the basis of many parameter, which mainly includes accuracy, request-response speed, complex computation, authentic data (error-less data), etc. and their advantages and disadvantages

* 1. **Secure distributed cloud storage scheme**

B. Sengupta and S. Narayanamurthy [1], proposed a technique which is totally based on security of client data, which is now a days a critical reason why users demands to use more trustworthy service provider or to say known service provider like Amazon, Google, Microsoft, etc. Technique is called as “**Secure distributed cloud storage scheme**”, it ensures client (users) by storing data more reliable and unaffected way on multiple servers. This idea uses two most famous concepts in cloud storage environment which is:

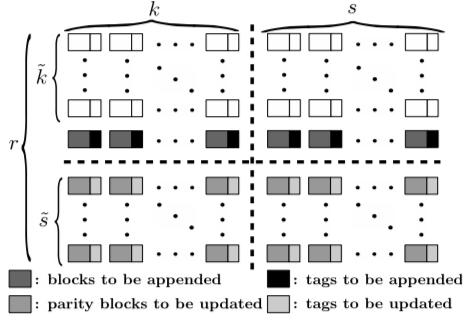
* “Provable data possessions” (PDP) and
* “Proof of retrievability” (POR).

Also researchers not only focused on static data but also for append-only data as well, which require more security comparatively. Encoding of the data blocks of a file is done in two steps: across multiple servers (dispersal code) and within each server (server code). Secure cloud storage schemes address this problem where the client (or a third party auditor) checks the availability of the file uploaded on the remote server.



**Figure 3. Distributed storage structure for static data [1]**

* + 1. As per above diagram, an idea is constructed for **static data** by encoding data blocks (using error correcting functionality i.e. codes/functions) and then putting tags which is used as a authentication information for these encoded blocks for specification purpose. Author proposed a secure distributed cloud storage scheme for static data that borrows the basic storage structure from HAIL (high-availability layer for cloud storage). This scheme offers POR guarantees. It defines a security model for distributed cloud storage schemes. Unlike HAIL, an adversary in this scheme cannot modify a dispersal codeword without being detected by the client.

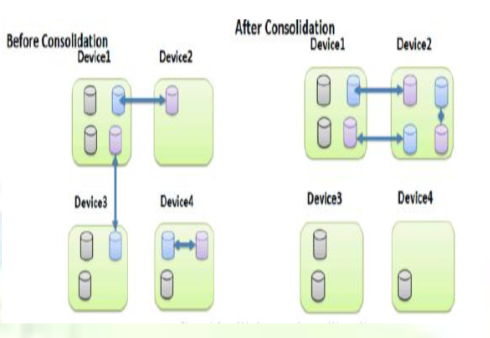


**Figure 4. Distributed storage structure for append-only data [1]**

* + 1. **Append-only data** is more difficult to handle, therefore, “Distributed cloud storages scheme” is suggested and faced the challenges efficiently. It overcome many disadvantages and made it into advantage like, it provides the server which all the rights to update its data block on its own. Also client does not have to download any parity (or data) block to update the tags of modified data blocks which is located on the servers.
  1. **Optimized multitenant cloud storage**

P Jyothi introduces an “Optimized multitenant cloud storage framework that incorporates the storage data analytics that suggest the service recommendation for the storage administrator”. In addition, secured cloud storage architecture is presented to assure the security of the data stored in the multitenant cloud storage system.

Storage Resilience Optimization Technique, this paper presents optimization technique which recommend a storage volume consolidation plan to improve the efficiency of storage resiliency usage. This technique are designed for data protection usually in the process of replication pair relationship. To enable the replication relationship the device hosting the primary and secondary volume must have the specific resilience. Performance analysis is done on the by analyzing storage and computation overhead



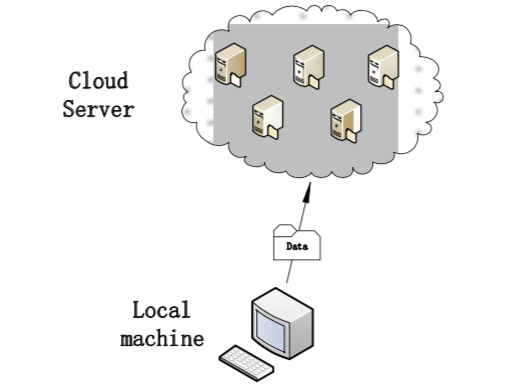
**Figure 5. Consolidation can reduce the Resilience [2]**

Advantage:

* It benefit the storage administrator and service provider for future budgeting planning and cost-aware optimization , while the exact saving depends on the license pricing model and charging facility.
  1. **Hierarchic Secure Storage**

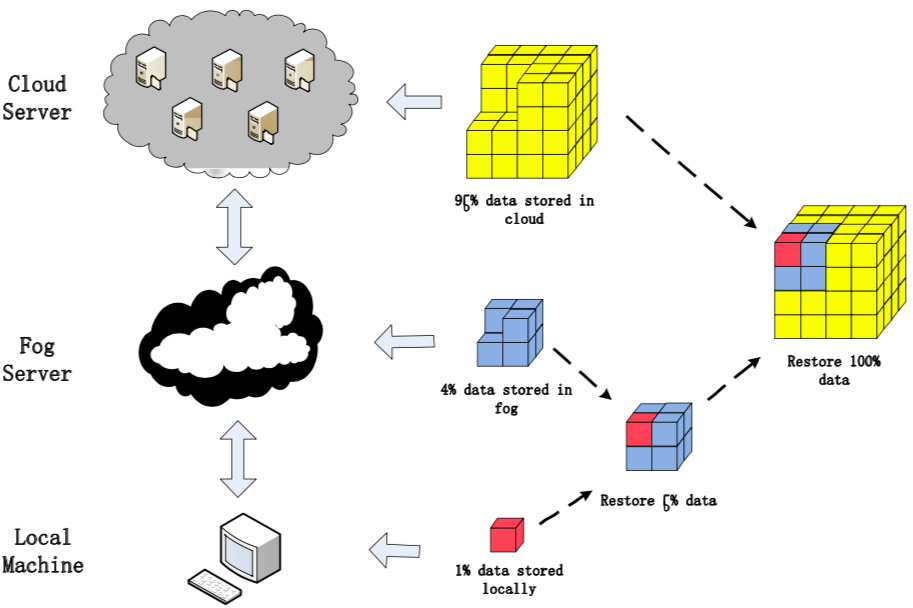
As with the growth of cloud computing environment, users depend on more powerful storage capacity of cloud storage. However, in these storage user data is stored in the cloud servers which is at risk of data leakage.

**“Classic design of cloud storage technique”** is mostly based on encryption and decryption [4] methods to store and retrieve data, as per user demand. But this is still not as secure as it seems, if users password is somehow gets compromised than all the users data is exposed to the public.



**Figure 6. Classic cloud storage structure[4]**

To overcome these issues Jiyuan Zhou, Tiang Wang, Md Zakirul Alam Bhuiyan and Anfeng Liu proposed a hierarchic model “**Hierarchic Secure Cloud Storage Architecture Based on Fog Computing Model**” [4]



**Figure 6. Three-level Storage scheme based on Fog Computing[4]**

* + 1. **Security measures**

Security degree is an important parameter to measure the quality od cloud storage system. Cloud data security is most critical part of cloud computing system and it three aspects – data privacy, data integrity and data availability.

1. **Fog Computing:** is the concept of a network fabric that stretches from the outer edges of where data is created to where it will eventually be stored, whether that's in the cloud or in a customer’s data center. Fog computing is usually a three-level architecture [5], the upmost is cloud computing layer which has powerful storage capacity and compute capability.
2. **Hierarchic Secure storage Architecture:** user’s data is divide into three different-size parts with encoding technology. Every part of the data will lack a part of key information for confidentiality. Combine with the fog computing model, the three parts of data will be stored in the cloud server, the fog server and user’s local machine according to the order from large to small. By this method, the attacker cannot recover the user's original data even if he gets all the data from a certain server. As shown in Figure. 6, the three-level storage scheme makes full use of fog server’s storage and data processing capability. The architecture includes three layers, the cloud server, the fog server and the local machine. Each server saves a certain part of data. As for how to allocate the ratio. Firstly, user’s data will be encoded on user’s local machine and let 1% encoded data be stored in the machine. Then upload the remainder 99% data to the fog server. Secondly, on the fog server, we do similar operation to the data which comes from user’s machine. There will be about 4% data stored in the fog server and then upload the remainder data to the cloud server.

**REFERENCES**

[1] B. Sengupta and S. Narayanamurthy “A Efficient Secure Distributed Cloud Storage for Append-only Data” 2018 IEEE 11th International Conference on Cloud Computing, May 2018, pp. 146-153

[2] P. Jyothi “Efficient Technique to optimize cloud multi-Tenant Environment” IJCERT ISSN(O): 2349-7084, January-2016,pp. 23-29

[3] Arron Fu “7 Different types of Cloud Computing Structures - <https://www.uniprint.net/en/7-types-cloud-computing-structures/> ” CTO UniPrint.net March 3, 2017.

[4] Jiyuan Zhou, Tian Wang, Md Zakirul Alam Bhuiyan and Anfeng Liu “A Hierarchic Secure Cloud Storage Scheme based on Fog Computing ” 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress pp. 471- 477.

[5] I. Stojmenovic and S. Wen, “The fog computing paradigm: Scenarios and security issues,” Computer Science and Information Systems (FedCSIS), IEEE, 2014, pp. 1-8