iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44694

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Research on Cloud Data Storage Security

Shweta Sukhram Prasad[1], Aarti Kanahiyalal Yadava[2]
[1, 2]*Student, MCA, ASM IMCOST College Thane*

Abstract: ***Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centers there still exist significant issues that need to be considered before shifting into cloud. Security stands as major obstacle in cloud computing. This paper gives an overview of the security issues on data storage along with its possible solutions many companies are not ready to implement cloud computing technology due to lack of proper security control policy and weakness in protection which lead to many challenge in cloud computing. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper, we will discuss the different techniques that are used for secure data storage on cloud. This paper also provides a process to avoid Collusion attacks of server modification by unauthorized users.***
Keywords: Introduction, Cloud Computing And Cloud Storage, Cloud Storage Security, issues, solution, conclusion.

I. INTRODUCTION

Cloud computing is the combination of many pre-existing technologies that have matured at different rates and in different contexts. The goal of cloud computing is to allow users to take benefit from all these technologies.

Many organizations are moving into cloud because it allows the users to store their data on clouds and can access at anytime from anywhere. From small to large enterprises poignant towards cloud computing to increase their business and tie-ups with other enterprises Security and privacy stands as major obstacle on cloud computing i.e. preserving confidentiality, integrity and availability of data. Cloud computing has given a new dimension to the complete outsourcing arena (SaaS, PaaS and IaaS) and they provide ever cheaper powerful processor with these computing architecture The major thing that a computer does is to store in the available space and retrieve information whenever requested by the authenticated user

As simple solution encrypt the data before uploading it onto the cloud. This approach ensures that the data are not visible to external users and cloud administrators but has the limitation that plain text based searching algorithm are not applicable.

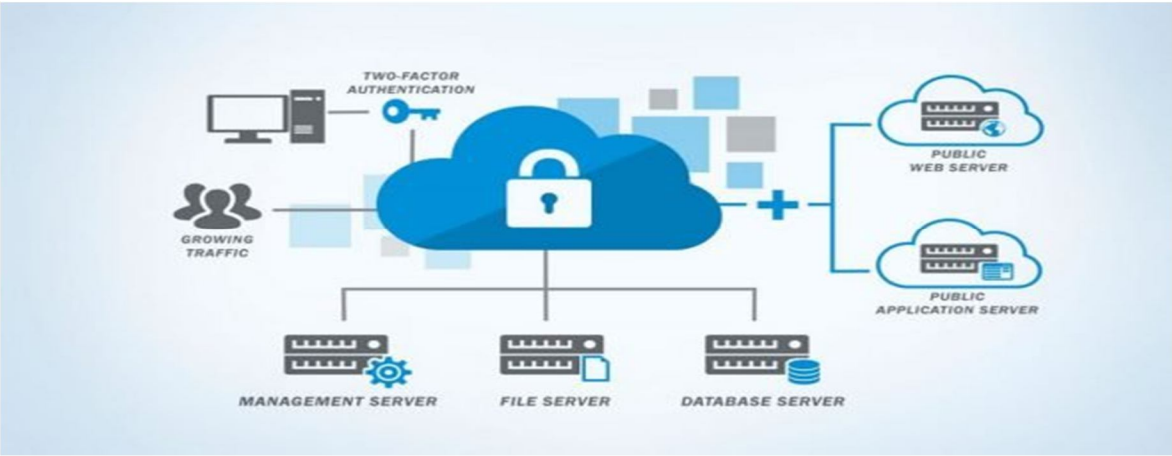


Fig1.cloud storage security

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

II. CLOUD COMPUTING AND CLOUD STORAGE

Cloud computing arises from the combination of the traditional computer technology and network technology, such as grid computing, distributed computing, parallel computing, utility computing, virtualization.

Cloud storage is a system that provides functions such as data storage and business access. It assembles a large number of different types of storage devices through the application software which are based on the functions of the cluster applications, grid techniques, distributed file systems, etc.

Users can use the powerful computing and processing function on clouds and they can order their service from the cloud according to their own needs.

Cloud storage is essentially one of the simplest applications of cloud technology available. Google Drive, Microsoft OneDrive, Dropbox; all of these services are cloud storage services. They do one thing and one thing only: they allow you to store data on the cloud.

Meanwhile, a company like Google, Microsoft, Amazon, Dropbox, or one of the many other cloud service providers has much, much more money and resources at their disposal. They can provide petabytes of storage for near-trivial amounts of money, with redundancy and backups in case of hardware failure. All you need to do is pay to access it.

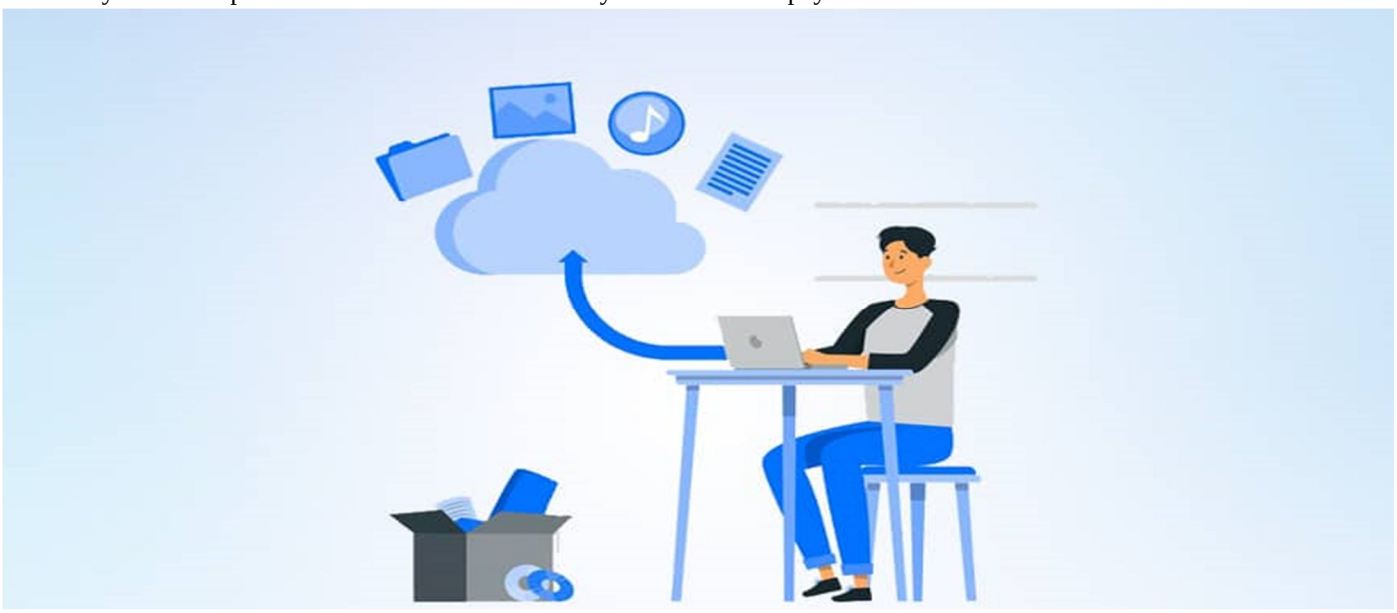


Fig2.cloud computing and cloud storage

A. Personal Cloud Storage

It is also known as mobile cloud storage. In this typestorage, individual's data is stored in the cloud, andhe/she may access the data from anywhere.

B. Public Cloud Storage

In Public cloud storage the enterprise and storageservice provider are separate and there aren't anycloud resources stored in the enterprise's data centre.The cloud storage provider fully manages theenterprise's public cloud storage

C. Private Cloud Storage

In Private Cloud Storage the enterprise and cloudstorage provider are integrated in the enterprise'sdata centre. In private cloud storage, the storageprovider has infrastructure in the enterprise's datacentre that is typically managed by the storageprovider.

D. Hybrid Cloud Storage

It is a combination of public and private cloudstorage where some critical data resides in theenterprise's private cloud while other data is storedand accessible from a public cloud storage provider.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

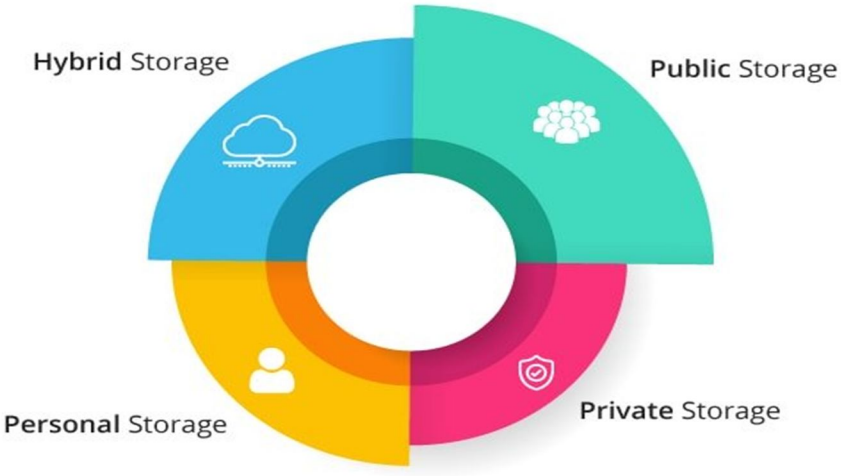


Fig3.type of storage

III. CLOUD STORAGE SECURITY

In cloud storage system, companies stores their data in the remotely located data server. Accordingly, correctness of the data is assured. Cloud data security typically involves a number of tools, technologies and approaches. A major advantage to the cloud is that many security elements are already built into systems. This typically includes strong encryption at rest and in motion.

1) *Geo-Fencing:* The use of IP addresses and other geolocation data to create a geographic boundary and identify suspicious activity.
2) *Policy-based Lifecycle Retention:* Systems use data classification polices to manage and automate how data is stored, retained, archived and deleted.
3) *Data-aware Filtering:* This function allows organizations to watch for specific conditions and events – and who has accessed information and when they accessed it. It can be tied to role-based authorizations and privileges.
4) *Detailed logs and full user/workload audit trail Reporting:* The ability to peer into logs and audit workloads can provide insight into security concerns and vulnerability risks.
5) *Backup and Recovery Functions:* These essential capabilities allow an organization to navigate an outage but also deal with security risks such as ransomware attacks and maliciously deleted data. Robust cloud-based disaster recovery solutions leads to availability across all conditions.

Fig4.security

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

IV. ISSUES

A. Data Privacy and Integrity

Even though cloud computing provide less cost and less resource management, it has some security threats. As we discussed earlier cloud computing has to ensure integrity, confidentiality, privacy and availability of data in generic cloud computing model but the cloud computing model is more vulnerable to security threats in terms of above conditions.

B. Misconfiguration

Misconfigurations of cloud security settings are a leading cause of cloud data breaches. Many organizations' cloud security posture management strategies are inadequate for protecting their cloud-based infrastructure.

C. Data Backup

The data backup is an important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored to ensure the data availability.

D. Rogue Devices

Not every security risk comes from the storage provider itself. The devices that access your data are also a potential source of danger. Many companies are embracing BYOD culture, which certainly has its benefits.

E. Unauthorized Access

Unlike an organization's on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet.

V. SOLUTIONS

The SecCloud is presented by Wei et al. it provides a storage security protocol for cloud customer's data and it not only secures the stored data but also provides security on computational data.

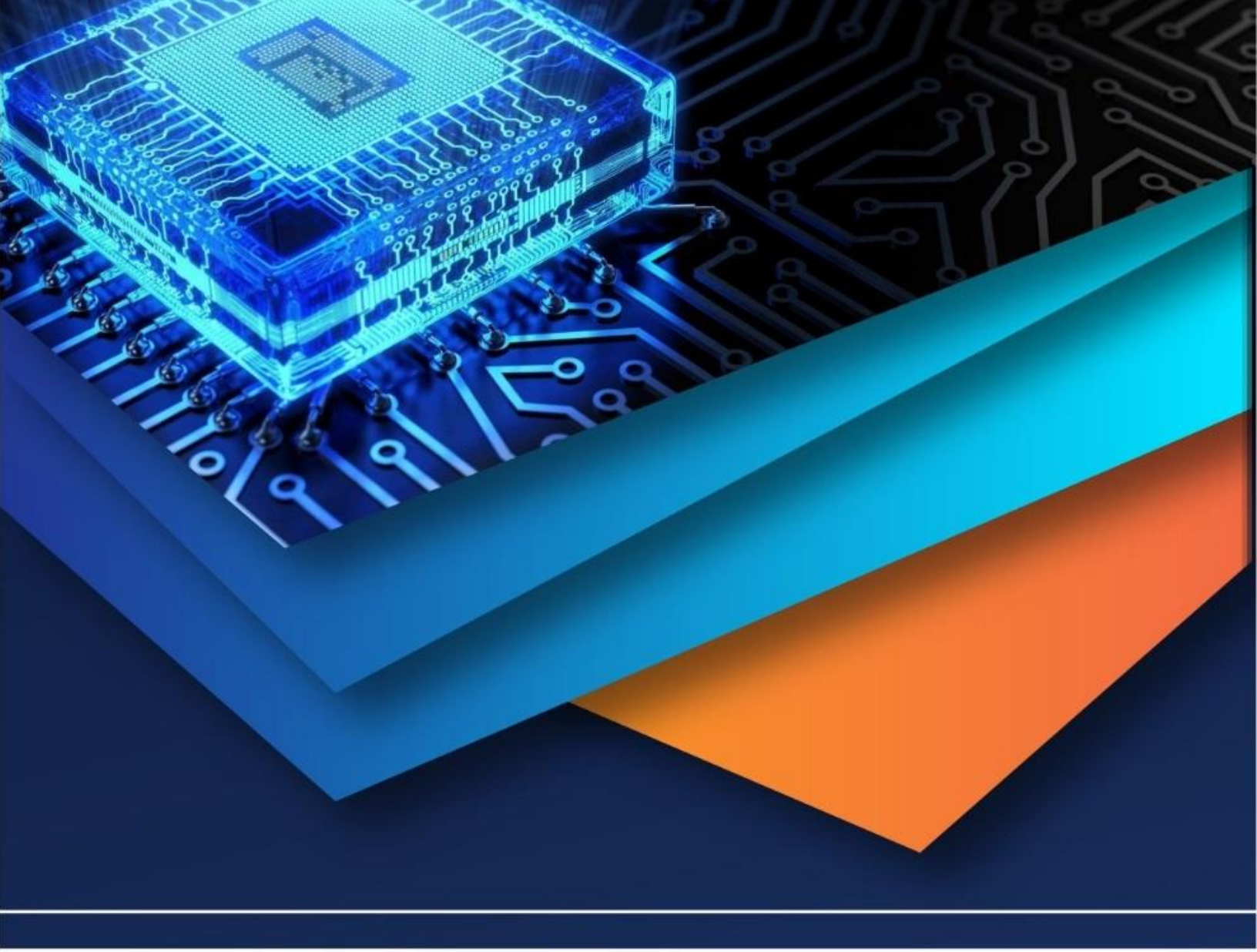
The SecCloud protocol uses encryption for storing data in secure mode. The multiplicative groups and cyclic additive pairing is used for key generation for cloud customers, CSP, and other business partners or trusted third party.

1) *Data Discovery and Classification:* Scan data repositories for important data and sort it into categories with clear labels, tags, or digital signatures.
2) *Change Auditing:* Monitor changes made to configurations across the cloud environment.
3) *Event Logging and Management:* Create detailed logs with full user and workload audit trail reporting.
4) *Data Access Monitoring and Control:* Promptly spot unauthorized access to your sensitive data.
5) *Authentication:* Use multi-factor authentication (MFA) to reduce the risk of unauthorized access to your applications, systems and data.
6) *Data Encryption:* Guard your data by adding this critical additional barrier to unauthorized data access.

The encrypted data along with the verifiable signature is sent to cloud data center along with session key. The Diffie-Hellman algorithm is used for generation of session key for both bilinear groups.Effective auditing mechanisms also can be used for providing data integrity.

VI. CONCLUSION

In large scale, massive data, virtualization, and high scalability cloud computing environment, how to optimize the performance of the distributed storage system and ensure its high reliability is a key research problem. The cloud computing architecture stores data and application software with minimal management effort and provides on demand services to customers through internet. But with cloud management customer don't have trust worthy commitments or policies



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY