BioGecko

Vol 12 Issue 02 2023

ISSN NO: 2230-5807

# CLOUD STORAGE-CHALLENGES AND OPPORTUNITIES

**Mrs.Vividha Bahety**
**Department of BCA, Indira College of Commerce and Science Pune.**
**Email: vividha.bahety@iccs.ac.in**

**ABSTRACT**
With the emergence of new technologies like Artificial Intelligence, Cloud Computing, IoT, and Fog Computing Information and Communication Technology is changing our home appliances to industry and resulting in bulk data generation. With the increased network speed of 5G technology users can share more data in very less time and future massive data will be shared by the user. Devices are becoming smart with artificial intelligence, and machine learning will also generate big data this data will be heterogeneous and it is very challenging to store and manage such a huge amount of data. Cloud storage is the ultimate solution to these. So, the future of cloud storage is very bright. This paper represents the issues and challenges that the cloud storage industry will face in the future and the opportunities for cloud storage.

**KEYWORDS:** Cloud Storage,Data security, IaaS, Data Management, 5G network

## INTRODUCTION

Smart technology is advancing very fast resulting in a rapid increase in the number of smart devices and as the number of devices increases a massive amount of data is also generated. With the use of artificial intelligence and machine learning the data is generated in unstructured form so managing and storing this bulk is the biggest challenge. Every day more and more embedded devices from our homes to different industries are added to the internet resulting in more data being generated on the internet. Analyzing and managing this data with our existing methods is very challenging we need special infrastructure for storage and modern techniques for processing, managing, and maintaining this large amount of data. Researchers are designing new database solutions with NoSQL for handling these heterogeneous data. Some of the most popular cloud storage providers are Apple (iCloud), AWS (Amazon Web Services), Dropbox, and Google. With the advance in technology, the computing and storage requirements of organizations are rapidly increasing. Also, with the current trend of social media individuals generate more data in the form of photos and videos in real-time. Setting up systems at this large scale requires large investments and efforts, as a result, organizations need to outsource storage and other computing resources This has increased the need for “on-demand storage” or cloud storage. But this gives limited control over the resources as operations are carried out with the cloud over the internet. Some other issues are also like cost, and performance of cloud storage. So, cloud storage is a hot research topic currently. Cloud solutions need different hardware like servers, networking solutions, and storage devices. Cloud solutions must be scalable and cheaper. Cloud storage issues include confidentiality, integrity, security, backup problem, data segregation, data access, data dynamics, authentication, data breaches, authorizations, and many more. In the next section, we discuss the cloud storage architecture challenges and possible solutions and the cloud storage future and opportunities.

## CHALLENGES IN CLOUD STORAGE

Storing the data in the cloud is a crucial part of Infrastructure as a Service (IaaS). Proper data management is required in the cloud environment to avoid data security and data management-related issues. So, cloud storage issues mainly divided into two broad categories -

1. Issues related with data security
2. Issues related with data management

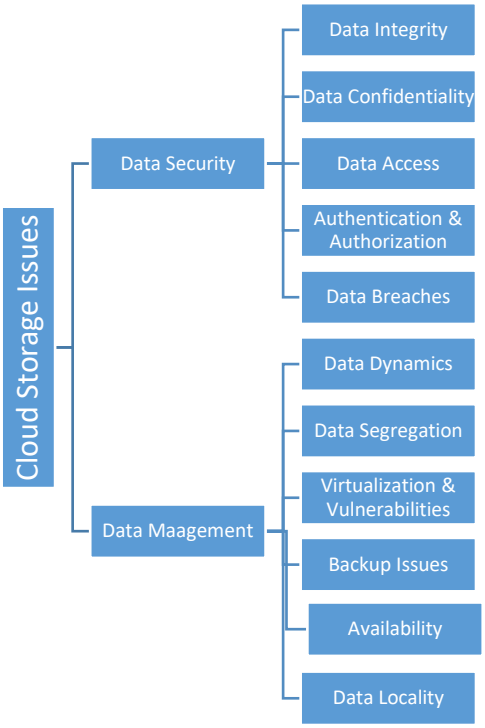


Figure 1: Challenges in cloud storage

**A. Data Security Issues**

Any client as tenant using cloud storage wants data security. Secure services attract more users to store their data in their cloud storage service. So, the companies providing cloud storage are designing and developing new techniques that can provide controlled access to cloud data and improve security of data. Moreover, as a tenant client has right to know "My data is permanently deleted or not or still it is with service provider? Or "Where exactly my data is located?" and many such questions. Many solutions to data security in cloud found with availability, authentication, confidentiality and integrity. If confidentiality is achieved, it automatically ensures integrity.

**1. Data Integrity**

Data integrity implies that the data should be honestly stored on cloud servers and if any violations (Data lose or altered) are to be detected. As data is stored on remote servers it may not be fully trustworthy because client does not have copy of all stored data. Thus cloud service provider must provide data integrity before and after the data update in cloud. For maintaining data integrity over cloud Digital Signatures can be used. Other issue is cloud servers are distrusted which means that data may be lost or modified maliciously or accidentally. Administration errors may cause data loss (e.g., backup and restore, data migration). adversaries may initiate attacks by taking advantage of data owners' loss of control over their own data. With outsourced computation, it is difficult for user to find that the computation is executed with high integrity or not. Another issue is location of data is not known to user so in case of any disaster data can be lost. In single database system data integrity achieved using transactions and constraints. This can be easily achieved by transactions using ACID properties (Atomicity, Consistency, isolation and durability). But in distributed system multiple

applications, multiple databases are accessing data stored at multiple sites must be handled properly to avoid transaction failure and allow various distributed applications through a resource manager to be a part of the global transaction.

**2. Data Confidentiality**

Security in cloud can achieved through confidentiality. In cloud environment cloud service providers know all the details for understanding the user data they become the privileged admins and they can monitor data stored on cloud so ensuring confidentiality in cloud is more essential. Confidentiality is achieved through RSA algorithm that uses encryption and decryption techniques. Encryption is the process of converting the readable text into unreadable form using an algorithm and a key.Obfuscation is another process and it is same encryption. Encryption can be applied to alphabets and alphanumeric type of data and obfuscation can be applied to a numeric type of data. Most important is level ofconfidentiality and privacy of user depends upon the privacy policies and other services provided by a cloud service provider.

**3. Data Access**

Data security is closely linked to access controls because properly assigning permissions to users in a system ensures that resources, data, and other variables aren't compromised. Issues related with accessing data in cloud environment are majorly due to security policies. The Software as a Service (SaaS) model must allow the organizations to integrate their security policies like Implementing a data-centric security plan, Employing Multi-Factor Authentication (MFA) and keep organization data secure when multiple organizations share the same cloud. In literature three categories of secure access control can be found Role Based Access Control (RBAC), User Based Access Control (UBAC) and Attribute Based Access Control (ABAC).

**4. Authentication and Authorization**

Authentication is used to determine and validate user identity. To identify the user through a user name and password is a traditional approach to identify a user. one-time passwords (OTP), and device fingerprinting are more secure methods for user authentication and when used in combination provides stronger combination for authentication. The process of authentication needs to be more efficient and robust thus, ensuring access to authenticated uses only. Authorization determines what the user is allowed to do. Authorization provides users the access to resources that they are allowed to have and prevents users from accessing resources that they are not allowed to access. Typical implementations are account-based, where rights to perform operations are associated with individual user accounts, or role-based, where users are linked to a specific role for which rights are granted.

**5. Data Breaches**

Data of many users is stored in cloud environment. So therefore, any compromise in authentication and authorization lead to data breachesit is a potential threat to the data of all users making cloud a lucrative for attackers. Cloud providers can also access user data because they need the associated encryption keys to see and process data so if any dissatisfied employee use these information and data owners are not aware what is happening with their data. With routine cybersecurity penetration tests, mandatory end-to-end compliance and efficacy are necessary for any enterprise-driven sensitive data.

**B. Data Management Issues**

There are many data management issues related to cloud environment like data availability, data backup, data locality, data dynamics, virtualisation and vulnerability, data segregation.

**1. Data Dynamics**

As cloud storage shifts databases and application software to large centralized data centres data management and performing various operations like insertion, updation and deletion operation in cloud is untrustworthy. This may lead to various security issues. Data may be deleted by cloud service provider without the permission of owner of the data so protection of data becomes very important. Data dynamics support through operations in the cloud for example insertion, block modification, and deletion is a huge step in the direction of practicality as cloud services are not restricted only to

backup and archiving. To support data dynamics number of techniques like data auditing are designed to provide efficiency, unlimited use of queries and information retrieval.

**2. Data Segregation**

The popularity of cloud computing is due to its multi tenancy nature. Multi-tenancy in cloud through SaaS applications allow storage of data from multiple users simultaneously. This may create an opportunity for a user's data to intrude into another user's data since data of different users reside at single location. This intrusion may exploit application's loopholes or by injecting SaaS system with malicious client code. If an application injected with a masked code executes it without verification shows that there are high possibilities of intrusion into others data. Therefore, cloud providers must ensure that the data of each user is bounded both at physical and application levels. Various assessments test must be performed to ensure that data from different users in multi-tenant environment is fully segregated from each other. These tests include; i) Data validation, ii) SQL injection flaws and iii) Storage insecurity.

**3. Virtualisation and Vulnerabilities**

Virtualization meaning different instances of same applications running on the same machine and it is one of the biggest security challenges in cloud environment Another issue is the administrative control of the operating systems, operating as guest and host systems and their imperfect provisioning of isolation and scalability issues. Many of the current Virtual Machine Monitors (VMMs) suffer from bugs allowing escape from VM. Therefore, "root security" is mandatory to prevent the host operating systems from being interfered with by any virtualized guest systems.

**4. Backup Issues**

Sensitive data must be backed up periodically by cloud service providers as part of disaster recovery. Strong encryption techniques must be used while taking backup to avoid accidental leakage of data and any security threats. Various tests like Storage insecurity and Configuration insecurity can be performed to check the security of back up data.

**5. Availability**

In today's time everyone wants highly available data in order to make data to be fully available, your data needs to be reachable in the sense that the infrastructure and software hosting it runs constantly. There are many reasons for data availability such as host server failure, storage failure, network crash, poor data quality, data combability issues. To handle these issues, it requires architecture level changes. Multitier cloud architecture needs to be adopted that support load balancing. Cloud storage must to flexible to handle hardware and software failures and also it must be protected from denial of service (DOS) attack and distributed denial of service attacks (DDOS) For any unforeseen disaster, appropriate disaster recovery that includes proper backup of data and to avoid single point of failure and operational sustainability action plans should be considered.

**6. Data Locality**

Client uses application provided by SaaS provider in SaaS model and its own data. In such scenarios client is not aware of the location of data in client environment which leads to data locality issues. Datastorage servers may exist in different countries and different countries may have different rule to govern data. A secure SaaS model may provide reliability to its clients at the consumer data locality.

## CLOUD STORAGE FUTURE AND OPPORTUNITIES

Due to the emergence of AI, IoT devices, 5G connectivity and the amount of data being produced by devices is changing the future of cloud. In this section we will discuss the future opportunities for the cloud storage:

**A. Cost Effectiveness**

cloud storage services offer a scalable, security-rich and cost-effective home for our data. Cloud storage is the cheapest and most scalable solution for the bulk of data. User can hire resources on cheaper rates which can save investments of consumers.

**B. Internet of Things**

With the introduction of IoT the number of devices has increased and their numbers are going to increase future at a very fast pace and the need of smart devices are also dramatically increasing. These devices are small in size and have not enough space to store or process big data therefore, they will depend on cloud environment to store and process their data.

**C. Remote accessibility**

Remote accessibility (i.e., access from everywhere and anytime) is the core of cloud storage. Many cloud providers providing remote access of data to their clients in a faster and reliable ways. The coming 5G internet service and AI is making it smarter and faster.

**D. Maximum Usability**

Cloud environment allows users to move files back and forth between the cloud and the local system using drag and drop facilities. The integration of smarts technologies (i.e, IoT, AI, fog and 5G), making the cloud storage usability very easy.

**E. 5G Connectivity**

With this high-speed 5G technology, humans will be able to virtually operate any machine at a distance of thousands of KMs. User can process and store data on cloud storage without facing any delay.

**F. Artificial Intelligence**

AI is progressing very fast AI is making smart decisions in complex situations The AI is making the cloud storage further smarter and attractive.

**G. Disaster recovery**

Data is the most valuable asset in today modern world. In cloud storage, data is stored in three different locations and in case of any disaster, data may easily be recovered. 5G technology made the recovery process very easy and fast. Cloud storage recovery is very easy, cheaper and fast.

**H. Privacy and Security**

Security of cloud storage for sensitive and confidential information is usually higher than that for the locally stored data. Privacy and security is an important aspect of the cloud storage and it is maintained by firewalls, intrusion detection systems deployed in cloud, advanced encryption techniques, logging of various events.

## CONCLUSION AND FUTURE DIRECTIONS

As IT industry is changing rapidly with the emergence of the latest technologies like cloud computing, artificial intelligence, and IOT.5G is a new era for cloud storage. This paper mainly focuses on challenges and possible solutions in cloud storage issues related to data security and data management. The cloud storage architecture consists of security things (e.g., confidentiality, integrity, access, authentication, authorization, and data breaches) and data management issues (e.g., dynamics, data segregation, backup, and virtualization). To avoid these threats, various measures are proposed in the literature. To enhance the security of cloud storage various techniques like strong encryption and decryption techniques can be used. In the last section future of cloud storage and opportunities is discussed We can say that cloud storage is designed to be a highly scalable and conveniently manageable storage system rather than only a file system. Finally, it can be concluded that cloud computing (along with integrated technologies) is a fast-growing technology which rapidly changing traditional computing. Efforts are being made by different cloud storage providers to provide the best secure cloud storage environments to clients.

## REFERENCES

[1]Bajaj, S. B., Jatain, A., Chaudhary, S., & Nagpal, P. (2021). Cloud Storage Architecture: Issues, Challenges and Opportunities. International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN, 2347-5552.

[2] Ghani, A., Badshah, A., Jan, S., Alshdadi, A. A., & Daud, A. (2020). Cloud storage architecture: research challenges and opportunities. computing, 1, 1.
[3] S S, Manikandasaran. (2016). Cloud Computing with Data Confidentiality Issues. IJARCCE. 5. 97-100. 10.17148/IJARCCE.2016.5123.https://medium.com/intuition/issues-and-challenges-in-cloud-storage-d3c7b7826dd0
[4]https://www.researchgate.net/publication/294730319_Cloud_Computing_with_Data_Confidentiality_Issues
[5] Sudhir Juare. Survey on Data Security and Integrity Issues in Cloud Computing IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 59-62 https://www.iosrjournals.org/iosr-jce/papers/conf.15013/Volume%202/14.%2059-62.pdf
[6] Tudor, G., Andrei, C. C., Madalina, A. C., & Alexandru, Z. (2019). Cloud storage. a comparison between centralized solutions versus decentralized cloud storage solutions using blockchain technology. In 54th International Universities Power Engineering Conference (UPEC). IEEE (pp. 16-32).
[7]Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditabil- ity and data dynamics for storage security in cloud computing," IEEE transactions on parallel and distributed systems, vol. 22, no. 5, pp. 847– 859, 2011.