A Comprehensive Study on the Cloud Computing Storage Security

Amit Kumar Bishnoi, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- amit.vishnoi08@gmail.com

ABSTRACT: The number of service providers has expanded as more data storage services use the cloud as their instrument of choice. With these options, businesses may choose from a variety of providers to migrate their data to the cloud. Maintaining the security of the sensitive data housed there, however, continues to be of utmost importance. In this paper, the author discusses the Data is stored, used, and backed up by a large number of servers via the internet in the very popular and adaptable cloud storage service model. Both businesses and individual users benefit from it. In recent years, several cloud storage companies have emerged, offering a range of features and services. The existing cloud offerings, however, do not always meet user needs, and choosing a storage platform is challenging because of the variety. In recent years, the idea of cloud computing has gained popularity. Data storage is a crucial and worthwhile area of study in cloud computing. In this work, cloud computing, cloud storage, and cloud storage architecture are first introduced.

KEYWORDS: Cloud Storage, Cloud Computing, Cloud Services, Security, Storage.

1. INTRODUCTION

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. One of the core concept of cloud computing is reducing the processing burden on user's terminals through continuously enhancing the clouds' handling capacity. Eventually user's terminals are simplified into a simple input and output devices. 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 [1].

Public, private, and hybrid clouds are the three main types of cloud storage. Public cloud storage typically has shared resource infrastructure and was designed for large-scale users. A private cloud, also referred to as internal cloud storage, caters to a particular user base. Private cloud storage, as opposed to public cloud storage, is housed in a controlled environment to meet safety and performance standards [2]. The last form of cloud storage is hybrid, which combines both public and private cloud storage. The fact that it caters to a certain user base is the main driver for this division of cloud storage kinds. The main problem is security. Without a guarantee that they may access their data whenever they want and that no one else can access it at all, users are reluctant to commit their data to a third-party organization. This makes it evident why multiple deployment techniques are used when deploying cloud services [3].

A solution called cloud storage offers features including data storage and corporate access. Through the use of application software, which would be based on the features of cluster programs, grid methods, distributed file systems, etc., it assembles several various kinds of storage devices. Storage medium may be thought of as a system for cloud computing that has huge capacity storage in addition to being just the storage in cloud computing [4]. Figure 1 illustrates the architecture of a cloud storage system, which primarily consists of a storage layer, a basic administration layer, an application interface layer, and an access layer.

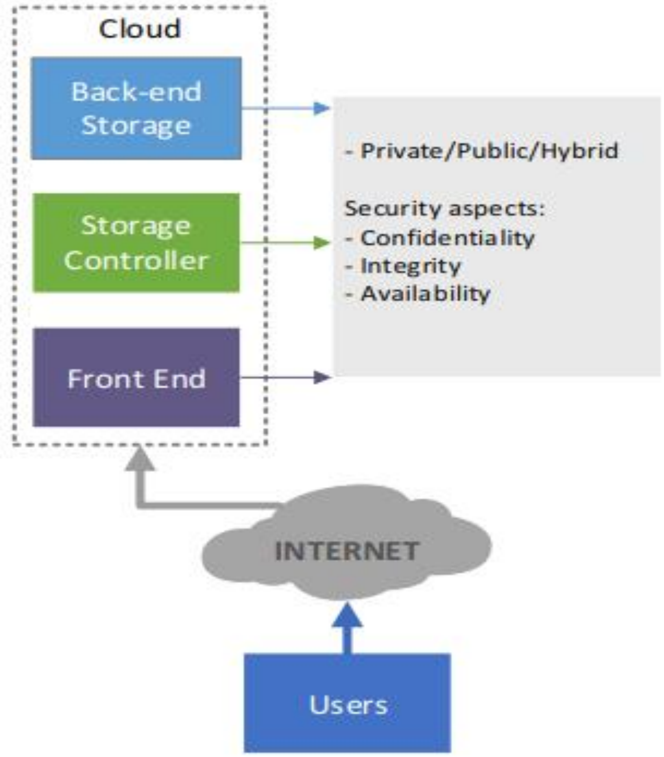

Figure 1: Illustrate the Generic cloud storage architecture [5]**.**

When using cloud storage, shared resources, data, and information are made available to computers and other devices on demand. In order to provide access to cutting-edge software applications, top-tier networks of server computers, and to describe a variety of computing concepts, it consists of a combination of hardware and software resources that are managed by third-party services [6]. Data centralized in any online medium is kept in the cloud. So that different users can access the same data. In this system, data may be stored in the cloud, and cloud-based software, services, and networks offer widespread network access. There are several benefits to cloud file storage. From any phone, tablet, or computer that is linked to the internet, a person or organization may access the documents [7]. Additionally, it enables users to download and play media files and share a safe link to a file with friends, family, or coworkers without having to worry about email file size restrictions or the security of sending a full-sized file. It also offers file backups. Therefore, information never vanishes due to lost devices, crashed computers, or lost phones. This research was created to help the most popular cloud storage providers by examining their strengths, weaknesses, performance, current level of security, and other factors.

2. DISCUSSION

Data utilization in computers has been growing day by day, both among individuals and businesses. Where should vital data be kept? How can it be shared? How can it be accessed globally? How can it be managed? How can it be made always accessible? And how can all of this be done affordably? Cloud computing provides the response to each of these queries. According to NIST, cloud computing is a concept for providing network access that is ubiquitous, practical, and on-demand to a shared pool of reconfigurable computing resources that can be quickly deployed and released with little administration labor or service provider involvement [8]. The three types of cloud services are software as a service, platform as a service, and infrastructure as a service. The "Pay-per-use" business model underpins each and every service.

- *Software as Service:* In SaaS, a customer accesses an application that is hosted by the service provider over the internet. These are mostly made for consumers. Customers may save down on installation and maintenance costs by not having to install the program on their local computer. The SaaS supplier is in charge of software updates. The majority of SaaS solutions use multitenant architecture. Customers may use the program at any time and location with only a web connection since the software is handled centrally. Google Apps, Quickbooks Online, Microsoft Office Live Business, Amazon, LinkedIn, Workday, and Netsuite are a few SaaS providers. When there is a significant a need mobile and otherwise web access, such as with mobile sales management solutions, when there is an interaction effect between the establishment and the outside world, such as with email, or when applications like tax or billing software are used only once a month, using SaaS is advantageous.

- *Platform as a Service:* With the help of these servicing facilities, software can be deployed in cloud infrastructure without the platform needing to be installed on the local system. The primary advantage of PaaS is that developers don't have to worry about platform updates or storage. PaaS providers are using these features. To save users from having to build anything from concept to completion, some PaaS providers offer prebuilt functionality. Some PaaS providers also offer an online forum where designers can discuss best business practices, get inspiration, and get guidance from other members. The way that PaaS is implemented varies from one supplier to another. A few of the PaaS providers are Google, OpenStack, Flexiscale, Appistry, Amazon Web Services, and LongJump.

- *Infrastructure as a Service:* IaaS, in contrast to SaaS and PaaS, offers hardware resources as a service. Memory, servers, networking equipment, and computing power are among the resources. The application is deployed using these. Infrastructure may be used by several users thanks to virtual computers. A governance system is needed to administer these virtual computers, which aids in preventing unauthorized access to critical user data. Utilizing this solution will assist in lowering the original hardware investment made by the business. The service has a "pay-per-use" business model. The greatest examples of an IaaS are Amazon Web Services' EC2 and S3.

2.1.Cloud Storage:

A cloud storage service makes data accessible to users over a network (via the internet) and continues to maintain, manages, and backs it up remotely. Numerous companies offer cloud storage. Most providers offer free storage up to a certain gigabyte limit. For instance, Google Drive, Box, Amazon, Apple Cloud, DropBox, and Microsoft SkyDrive all offer free storage up to 2GB, 5GB, and 7GB, respectively. If a customer exceeds the free space limit, they must pay a fee in accordance with their plan [9]. Maximum file size, auto backup, bandwidth, and upgrade for space constraints are features that vary from one provider to the next. For example, DropBox's maximum file size is 300MB, while Google Drive's maximum file size is 1TB. Customers that use cloud storage services may avoid investing in storage equipment and don't even need technical assistance for maintenance, storage, backup, or disaster recovery. When the client can store and handle the data at a cheap cost compared to using the cloud, the notion of cloud storage is not worthwhile. Therefore, the cloud should be created in a manner that is economical, autonomous, scalable, accessible, controllable, and efficient.

2.2.Cloud Storage Standards:

In 2009, the Storage Network Industry Association TM released CDMI. Both legacy and new apps are supported by this. Roles and duties for data ownership, retrieval, and archiving are defined by cloud storage standards. Additionally, this offers a uniform auditing procedure so that computations are performed consistently. These are beneficial to cloud storage providers, customers, developers, and service providers. Cloud storage users may quickly find the providers that meet their needs by utilizing CDMI. Additionally, the CDMI offers a standard interface for providers to promote their unique capabilities so that customers may quickly identify the providers [10].

2.3.Security Challenges:

Although cloud storage has certain built-in weaknesses, consumers have never been discouraged from taking advantage of its savings and flexibility. Users lose control over physical security when a cloud model is used. Users really share computer resources in a public cloud storage with other users. The three primary characteristics of security are confidentiality, integrity, and availability (CIA). These factors are the most important ones to take into account while creating a security solution to provide the most protection. This is shown by the vulnerability events that the CSA generated and are shown in Figure 2. In a nutshell, confidentiality includes preventing the leaking of data and information to unauthorized parties. Integrity refers to preventing unauthorized parties from altering data and information. On the other hand, availability ensures that the data and information are accessible to be used by the authorized individuals whenever necessary. The problems in this study are generated from the vulnerabilities that are already known. Access to protected data and information is limited to those with a certain level of authorization.

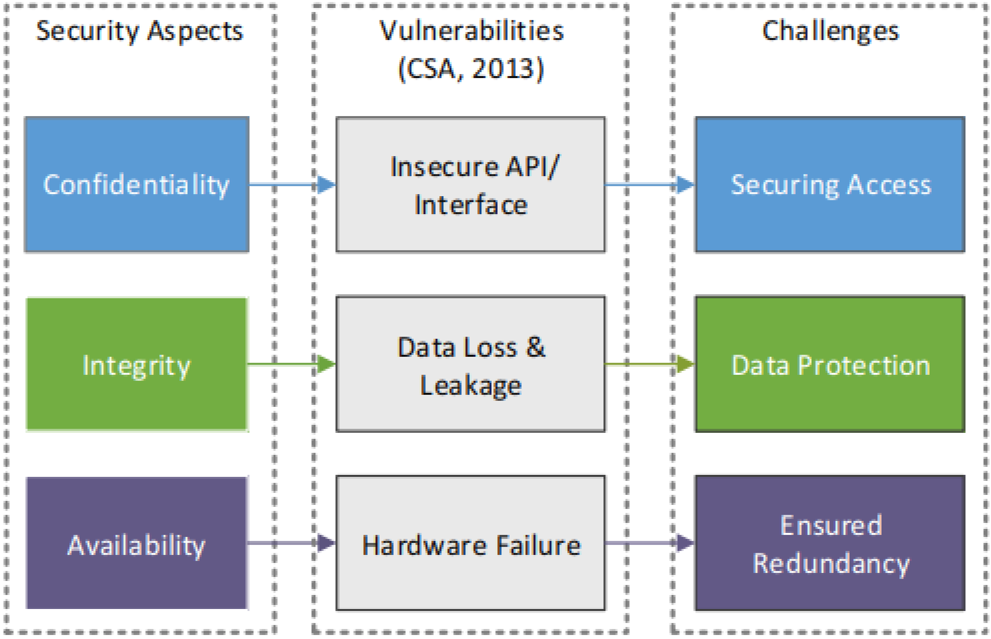

Figure 2: Illustrate the vulnerabilities incidents results [11]**.**

For this, controls to limit access to protected data must be in place. The level of complexity of the access control methods should correspond to the importance of the information being safeguarded; the more sensitive or priceless the information, the more robust the control measures must be. Authentication, authorization, and encryption provide the skeleton on which access control systems are constructed. Second, maintaining the integrity of several parties engaged in the provision of resources is necessary to prevent data from loss and leaking. To guarantee that the data and information stored in the cloud is not changed or deleted, certain plans and mechanisms are required. To enable verification, it is advised to employ auditing methods like proof-of-retrievability and proof-of-data-possession. Consequently, it's critical to maintain high hardware availability while access and data are safeguarded. The infrastructure that houses the services used to store data and information is called the hardware. The services cannot achieve the uptime requirements and adhere to service level managements without assuring failover.

3. CONCLUSION

With the growth of the internet comes cloud computing, which also expands the number of robust applications available online. The foundation of cloud computing is cloud data storage technology, which addresses the data storage issue in a cloud context. Author present the linked ideas of cloud computing and cloud storage in this paper. Then, using our PCs' eyeOS online operating system, we propose a cloud storage architecture. Experiments confirmed the system is working well. The development of cloud storage is advancing quickly. This essay examines the characteristics of several cloud storage options. According to the report, the major problem for company planning is security and processing enormous amounts of data on the cloud using a reasonable approach. To meet the difficulties of the future, recent performance, portability, scalability, and availability should be created. Therefore, attention should be placed on resource management, security, and virtualization.

REFERENCES

[1] V. R. Pancholi and B. P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES," *Int. J. Innov. Res. Sci. Technol.*, 2016.

[2] D. Alsmadi and V. Prybutok, "Sharing and storage behavior via cloud computing: Security and privacy in research and practice," *Comput. Human Behav.*, 2018, doi: 10.1016/j.chb.2018.04.003.

[3] A. Ait, N. Ammari, A. Abou, A. Ait, and M. De, "New mechanism for Cloud Computing Storage Security," *Int. J. Adv. Comput. Sci. Appl.*, 2016, doi: 10.14569/ijacsa.2016.070773.

[4] J. Wu and J. Chen, "The Homomorphic Encryption Method for Cloud Computing Storage Security," *Int. J. Secur. Its Appl.*, 2017, doi: 10.14257/ijsia.2017.11.1.11.

[5] A. A. El Mrabti, N. Ammari, A. A. El Kalam, A. A. Ouahman, and M. De Montfort, "New mechanism for Cloud Computing Storage Security Fragmentation-redundancy-scattering as security mechanism for Data Cloud Computing," *Int. J. Adv. Comput. Sci. Appl.*, 2016.

[6] Q. Kanaan, H. Sadeq, and H. A. Ail, "Storage Architecture for Network Security in Cloud Computing," *Diyala J. Pure Sci.*, 2018, doi: 10.24237/djps.1401.205c.

[7] L. Wei *et al.*, "Security and privacy for storage and computation in cloud computing," *Inf. Sci. (Ny).*, 2014, doi: 10.1016/j.ins.2013.04.028.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, 2011, doi: 10.1109/TPDS.2010.183.

[9] T. Gaur and N. Kharb, "Security of Data Storage in Cloud Computing," *Int. J. Comput. Appl.*, 2015, doi: 10.5120/19352-1023.

[10] B. Fang *et al.*, "The contributions of cloud technologies to smart grid," *Renewable and Sustainable Energy Reviews*. 2016. doi: 10.1016/j.rser.2016.01.032.

[11] P. B. Godhankar and D. Gupta, "Review of Cloud Storage Security and Cloud Computing Challenges," *Int. J. Comput. Sci. Inf. Technol.*, 2014.