*Academic Guru Publication House*

**Advances in Cloud Computing Security**
**Techniques and Applications**
Volume 1
Year: 2021

AG PH Books

# Hybrid cloud computing: Security Aspects and Challenges

Dr. Umakant Bhaskar Gohatre[1*]

[1]*Assistant Professor, Smt. Indira Gandhi College of Engineering, Navi Mumbai*

## Abstract

Innovative business results may be achieved via the growth of cloud infrastructures to hybrid cloud models, which are driven by the need for increased Information technology (IT) agility and overall cost-control constraints Hybrid cloud solutions integrate advantages of both public and private cloud infrastructures. Different security risks have been proven to be addressed in order to get the most out of the hybrid cloud approach. The security of hybrid clouds for major corporations and governments is the subject of this article. It explores numerous security types inside the IaaS and SaaS concepts, different authentication and security principles, and security difficulties in this field. In this case, a comparative assessment of several current solutions and the common issue areas and security threads are the focus of this work.

*Keywords:* Migration; Hybrid cloud; security issues; security techniques.

## 1. INTRODUCTION

The phrase "Cloud Computing" has gained a lot of traction recently in the IT sector. People on the internet use it a lot, and various writers have given it many diverse interpretations. When it comes to software development, cloud computing is reshaping the industry. Personal and professional elements of life and work are trending toward the idea that everything can be found on the internet. Big online-based corporations like Google and Amazon have come up with a concept called "Cloud Computing," which

* ISBN No. 978-81-955340-6-7

is the sharing of web infrastructure to cope with the storage, scalability, and calculation of Internet data. Using this trend Customer-specific hardware and software services are provided through the internet via the cloud computing concept. Cost and maintenance are reduced by using cloud computing. When it comes to cost-saving IT cloud solutions, many companies are turning to hybrid clouds, which combine advantages of constructing private and public clouds and also using the scalability inherent in their current Information technology (IT) infrastructure. Numerous companies are now quickly implementing a multi-cloud strategy that makes use of a variety of cloud service providers for supporting their IT infrastructure [1]. 58 % said they use Microsoft Azure as their cloud platform provider, while 52% said they use Amazon Web Services. A further 19 % goes to Google Cloud; a further 9 % goes to Oracle Cloud; and a last 7.3 % goes to RackSpace.

## 2. OVERVIEW OF HYBRID CLOUD

Hybrid cloud computing discuss about aggregating and incorporating computer, connectivity, applications and storage into a unified management framework that allows enterprise IT and developers to leverage the scale, flexibility and cost savings of existing in-house IT investment tools and systems to manage in data of enterprise centre with their newly adopted cloud services. More than 80% of IT organisations are expected to use hybrid architectures, according to an IDC survey. Figure 1 shows Hybird prototypes.

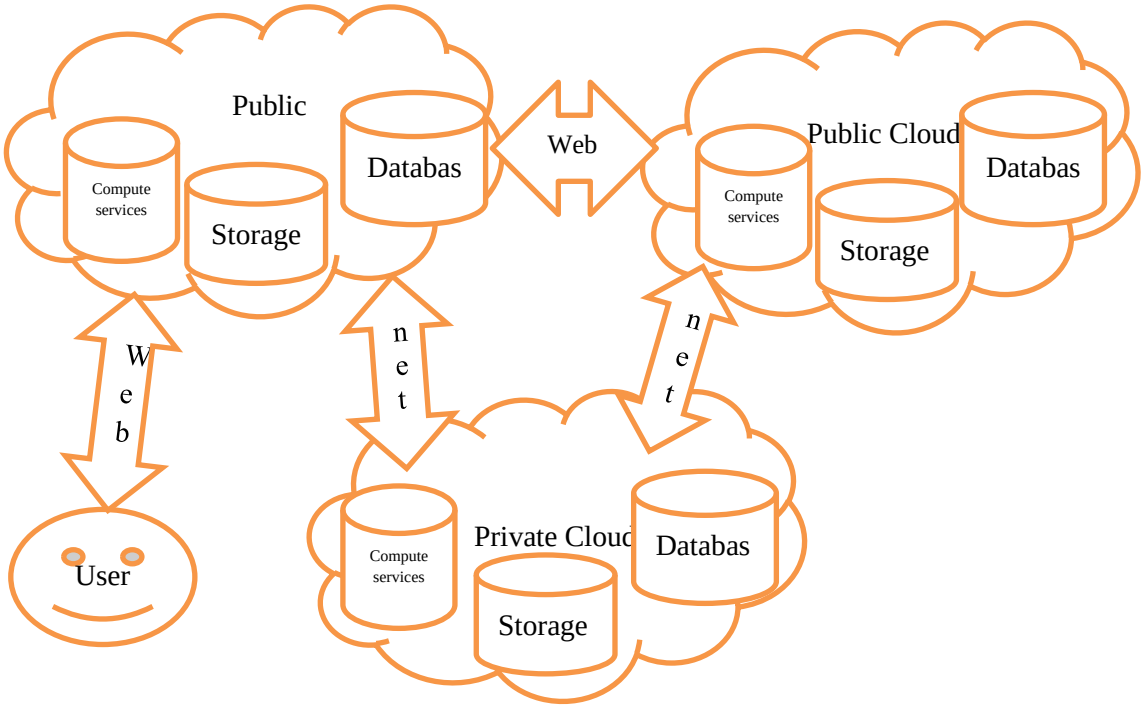


Figure:1 Hybrid cloud Services Model

Some features that a Hybrid cloud includes are discussed below.

- *Infrastructure Integration and Application Environment:* Workloads or virtual machines may be created in both private and public clouds with the use of a hybrid cloud platform.
- *Interconnectivity*: When two separate environments can communicate and interact with one other, the data, virtual machines, and applications they contain are more likely to be interconnected.
- *Applications Portability:* System components may be reused across several cloud environments using cloud-aware development.
- *Monitoring and Management:* The ability to keep track of and manage several cloud environments is essential nowadays. System health monitoring and management are critical in a hybrid cloud environment since it allows for cross-cloud insight into the overall health of the hybrid cloud system.

Some cloud computing resources are supplied and managed inside the company while others are outsourced to a hybrid cloud. It's possible that a firm uses Amazon Simple Storage Service (Amazon S3) for archived data but keeps its operating customer data on-premises. Ideally, a hybrid strategy enables a company to take benefit of the scalability and cost-effectiveness of public cloud computing environment without exposing mission-critical programmes and data to third-party risks. The term "hybrid IT" is also used to describe this form of hybrid cloud.

This specific topic is being concentrated on by a couple of the primary unique and cloud suppliers and providers. Several hybrid cloud storage providers are shown in Figure 2.

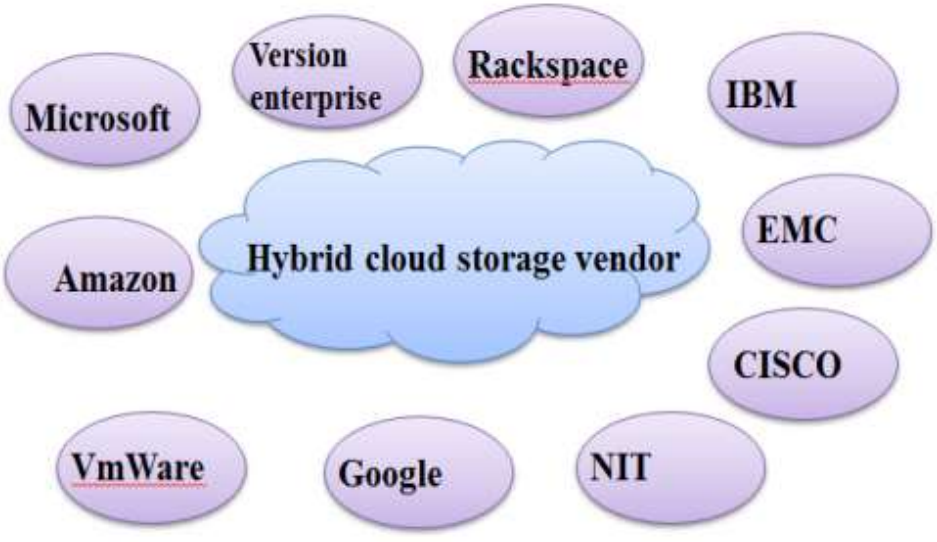


Figure 2. Hybrid Cloud Storage Vendors

## 3. HYBRID CLOUD COMPUTING CHALLANGES

Some challenges to consider when setting up hybrid clouds are:

i. ***Startup and Shutdown of On Demand*:** Cloud nodes must be able to be started and shut off on demand by your infrastructure. Cloud nodes must be started or stopped based on some kind of policy that takes into account the features of your application. With this method, you may launch new nodes if the main cloud becomes overcrowded and shut them down if it becomes underloaded by reacting to CPU consumption in either direction.

ii. ***Cloud-based Node Discovery:*** It is difficult to set up normal discovery protocols in the cloud since many cloud providers do not support IP Multicast (including Amazon and Go Grid). TCP would be required for your node discovery mechanism to function. However, you are also unaware of IP addresses of newly created nodes in cloud. If you want to avoid this, you should keep the IP addresses of new nodes in a cloud storage service like Amazon S3 or Simple DB.

iii. ***One-Directional Communication:*** It's a difficulty for large organisations to open up additional ports in firewalls to connect to cloud services. You may only be able to connect to a cloud in an outgoing fashion rather often. Such scenarios should be supported by your middleware. On top of that, you may come into a situation where A cloud can speak to B cloud, and the b cloud can talk to the other C cloud, but the A cloud cannot talk to the C cloud. Ideally, cloud A should be able to communicate with cloud C through cloud B.

iv. ***Latency Communication:*** Latency Cloud communication may take longer time than communication between nodes inside same cloud. Cloud-to-cloud connectivity, on the other hand, is sometimes substantially slower than cloud-to-local data centre connection. In order to avoid breaking down the cluster, your middleware layer should be able to respond and manage delays.

v. ***Reliability and Atomicity:*** On the cloud, many operations are unstable and non-transactional. F or example, when you store anyrthing on Amazon S3 storage, it doesn't guarantee that another programme will be able to access the data you've put there immediately. Data can't be protected from being overwritten, and file locking isn't possible. It is only possible to provide this functionality at the application or middleware levels.

## 4. ADVANTAGE OF HYBRID CLOUD

(1) In terms of wording, it’s more diverse since it includes both private and public cloud.

(2) As a result of this, the organization's demands may be met quickly with a hybrid cloud, as described in [5][6]. When an organization's in-house server can't manage a project that requires

a lot of computing power, a cloud-based solution is ideal. It would also save the company money by avoiding the need to purchase high-end server hardware, which is essential.

(3) From anywhere in the globe, a hybrid cloud may be used to work on a project at any time. Having a global presence enables them to serve enterprises who need to extend their impact beyond local boundaries. It's a safe haven for private information as well as a useful public resource.

(4) Due to the obvious allocated private cloud, it consistently offers the highest degree of security. Depending on the situation, it may be able to reduce and manage costs.

(5) Hybrid cloud may be quite expensive for a company if it choose to invest resources into a hosting provider or outsource the same. However, this innovation may be obtained for very low costs, making it a far better investment for the charitable organisation in the long run.

## 5. TRAITS OF HYBRID CLOUD

- *Security*: Keeping one's personal information safe is a constant concern. In addition to access control measures while data is stored, safeguarding efforts are put in place when it is transferred between storage locations and on-premises places [6]. The storing of documents should also be safe.
- *Reliability*: When it comes to data integrity, the hybrid cloud is also a factor. There must be no tampering with t data sent from person A to person B In the cloud, the data would be indexed by the cloud service. Likewise, its integrity should endure even if it isn't around anymore. For example, When indexes are damaged, the data is lost.
- *Business Coherence*: Scheduled and unscheduled downtime may have a negative impact on businesses' ability to function effectively. Capacity providers must offer backup mechanisms like snapshots, replication, and reinforcements, as well as quick recoveries in the event that their own infrastructure goes down.
- *Reporting And Charge-Back:* A cloud storage may be a compensatory pay-you-pay model, in which the bill is due at the conclusion of the charge cycle. This may serve as an example of any value-based fees that a provider can impose in addition to the capacity expenses.
- *Management*: The customer should be ready to cope with the circumstances in a hybrid cloud environment if they want to keep part of their data on-premises and some in the cloud.

## 6. CONCLUSION

Security and privacy are of the utmost importance in the cloud computing data storage. Despite fact that cloud storage & administration provides more flexibility and convenience, there are still risks of intruders and criminal behaviour. Cloud servers can provide more protection and privacy for data kept there.

Hybrid Cloud computing is an inevitable paradigm in which private and public clouds may be used simultaneously. Any new technology should take into account the many security risks that might be associated with it. In light of the different security concerns, cloud users and hybrid cloud providers alike will be better equipped to deal with these risks. In addition, a study of hybrid models has exploited and targeted with issue concerns a framework for security and a necessity for cloud security. It lessens the load on users of the majority of cost savings and complexity. Organizations are confident in the safety of their data in the face of security threats and system failures. For service delivery needs, it recommends a modernised IT operational agility.

Cloud computing and the security challenges that arise as a result of its fertilised, shared, public, private, and hybrid nature have been the subject of this study. There are a numerous ways to deal with cloud computing security concerns, and this article outlines some of them.

## REFERENCES

1. Nitin Kumar, Shrawan Kumar Kushwaha and Asim Kumar, “Cloud Computing Services and its Application,” Advance in Electronic and Electric Engineering, Volume 4, Number 1 (2014), pp. 107-112.
2. Caifeng Zou, Huifang Deng and Qunye Qiu, “Design and Implementation of Hybrid Cloud Computing Architecture Based on Cloud Bus,” IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks, 2013.
3. M. Posey, “Journey to the Hybrid Cloud,” White Paper Sponsored by: VMware, IDC #242798R2, September 2015.
4. “Hybrid Cloud 101: Hybrid Cloud Computing - Intel” Intel IT Center Solution Brief | The Path to Hybrid Cloud, September 2013.
5. Rahul Khurana1, Himanshu Gupta, A Hybrid Model on Cloud Security 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) ,Volume.16,pp:347-352, ,2016.

6. Saurabh Singh, Young-Sik Jeong, Jong Hyuk park, A Survey on Cloud Computing Security: Issues, Threats, and Solutions ,Journal of Network and Computer Applications, SI1084-8045, ,2016.