A Survey on Hybrid Cloud

# Abstract

The innovation that has lately emerged is cloud computing. Every organization must connect to the cloud computing environment. In the context of cloud computing, a study of unique hybrid cloud organization models and cloud benefit models is covered. An industry trend has been identified where the use of hybrid cloud architecture can support upcoming industry challenges by providing an efficient means of storing their information in the cloud. This is done by combining both public and private clouds, giving the office the option to store sensitive information on private clouds and less critical information on public clouds where large amounts of storage can be made The hybrid cloud is especially lucrative for workloads that are dynamic or very flexible. This essay describes the cloud computing overview, service model, attributes, provider storage, and problems.

**Keywords:** Cloud Computing, Private Cloud, Public Cloud, Hybrid Cloud, SaaS, PaaS, IaaS, Cloud Security

# INTRODUCTION

Diagram

Description automatically generatedIn the modern world, innovation is advancing quickly and provides customers with a variety of services that are paperless and available online, such as e-charging, email, e-messages, e-transactions, and so forth. A digital information exchange is necessary for all of these accessible agencies. The ability to access information in the cloud is the biggest leap in computing, but there are a lot of other factors to consider as well. When compared to its disadvantages, cloud computing has a few benefits, according to many creators. However, it was discovered that as information association grows, information security increasingly becomes a problem, despite the fact that we must find a way to combine everything you need with a particular administration. The most recent technological breakthroughs, such as distributed computing and hardware virtualization, have given rise to cloud computing. The benefit of cloud computing is that, by utilizing the potential of virtualization, the processing approach may continue to execute on one or more associated PCs in the meantime.

FIGURE 1 Pros and Cons

Figure 1 outlines the pros and drawbacks of cloud computing. Three service models, four deployment types, and six key characteristics of cloud computing make up the cloud model. The cloud offers a variety of service models, including IaaS, PaaS, and SaaS. It is possible to send it using a variety of deployment types, including public, private, hybrid, and community clouds

# SERVICE OF CLOUD

## Software-as-a-Service (SaaS)

The term "Software-as-a-Service" (SaaS) denotes licenses for using software programmers to support end users. As being the most popular and easiest to understand and use. These cloud application services, in their most basic form, deliver apps via the Web. The concerned customer is supplied these services by a third-party provider. Customers don't need to install or download anything onto their own PCs or servers because most of these applications may be created specifically from a Web programmed. In this case, the cloud provider oversees managing all the servers, storage, virtualization, servers, apps, data, and runtime. Making use of SaaS makes it simple for businesses to maintain their frameworks because a significant amount of the information is managed by the external provider.

* 1. ***Platform-as-a-Service (PaaS)***

A platform-as-a-service (PaaS) provides applications, development and configuration tools, and other tools with the runtime environment. Of the three service models, this one is the most challenging to manage. The resources supplied here are provided through a platform, as the name suggests. Following that, developers use this platform to create and modify applications using the available framework. PaaS makes it easier to build, test, and organise applications on a basic server, storage, runtime, middleware, and networking, provided that the business has a productive development team. However, it is up to the customer to manage applications and data.

* 1. ***Infrastructure-as–a-Service (IaaS)***

The most crucial level of service is Infrastructure-as-a-Service (IaaS).the lowest tier of service.Therefore, the key difference between SaaS and PaaS is the certainty that both the client or customer and the provider share responsibility for managing the framework. As IaaS provides access to important resources like physical machines, virtual machines, virtual capacity, and more in this case, providers are still in charge of it. In essence, this service offers computational infrastructure, such as networking, storage, and virtualization. Customers can purchase fully outsourced services, which are then billed based on the resources used. In this instance, the supplier levies a rent fee for setting up the clients' virtual servers on their own IT infrastructure. The consumer must deal with information, applications, runtime, and middleware, while the merchant is in responsible of managing virtualization, servers, storage, and networking. Customers can introduce any platform as needed, depending on the framework type they choose. As the demand for accessibility grows, they will also need to monitor the upgrading of more recent forms.

# LITERATURE REVIEW

The article "Hybrid Cloud Computing for Data Security System" published in 2021 by Surabhi Saxena et al explores the use of hybrid cloud computing for implementing data security systems. The paper begins by discussing the importance of data security and the challenges that organizations face in securing their data. It then explains the concept of hybrid cloud computing and how it can address these challenges. The paper highlights the advantages of hybrid cloud computing, including the ability to combine the benefits of both on-premises and public cloud environments. It also discusses the challenges associated with implementing a hybrid cloud environment, such as data integration and security concerns. The article then delves into the specifics of implementing a hybrid cloud data security system, including the use of encryption and access controls to protect data in transit and at rest. It also discusses the importance of monitoring and auditing to ensure the security of the system. The paper concludes by emphasizing the importance of careful planning and risk assessment when implementing a hybrid cloud data security system. It also highlights the need for ongoing monitoring and evaluation to ensure the continued effectiveness of the system. Overall, the article provides a comprehensive overview of the use of hybrid cloud computing for data security systems, and highlights the benefits and challenges associated with this approach. It offers useful insights and guidance for organizations considering the adoption of hybrid cloud computing for their data security needs.[1]

The article "Secure hybrid cloud computing: Approaches and use cases" published in 2014 by Kapil Bakshi et al discusses the challenges and approaches to achieving secure hybrid cloud computing. The paper begins by defining hybrid cloud computing and the need for security in hybrid cloud environments. It then presents the challenges of secure hybrid cloud computing, including data privacy, data integrity, and data availability. The article goes on to present various approaches to achieving secure hybrid cloud computing. These include secure data migration techniques, secure data storage and retrieval, and secure access control mechanisms. The paper also discusses the importance of secure communication protocols and the use of encryption to protect data in transit. In addition, the article presents several use cases for secure hybrid cloud computing, including disaster recovery, data backup and recovery, and high-performance computing. It provides examples of how organizations can use hybrid cloud computing to achieve their security goals in these scenarios. The paper concludes by emphasizing the importance of a risk-based approach to secure hybrid cloud computing, where organizations assess their security needs and implement appropriate security controls based on their risk profile. It also highlights the need for ongoing monitoring and evaluation to ensure the effectiveness of the security controls. Overall, the article provides a comprehensive overview of the challenges and approaches to achieving secure hybrid cloud computing. It offers useful insights and guidance for organizations considering the adoption of hybrid cloud computing for their security needs.[2]

The article "Towards the Modelling of Hybrid Cloud Applications” published by Kyriakos Kritikos in 2019 presents a framework for modelling hybrid cloud applications. The paper begins by defining hybrid cloud computing and highlighting its benefits and challenges. It then presents the need for a modelling framework to facilitate the design, deployment, and management of hybrid cloud applications. The paper proposes a framework for modelling hybrid cloud applications, which includes a set of building blocks that can be used to represent various aspects of the application, such as the application components, data flows, and security requirements. The framework also includes a set of relationships between the building blocks to capture the dependencies and interactions between them. The article discusses the benefits of the proposed modelling framework, including the ability to capture the complex dependencies and interactions between the components of a hybrid cloud application. It also highlights the potential for the framework to facilitate the automated deployment and management of hybrid cloud applications. The paper concludes by presenting a case study to demonstrate the application of the modelling framework. The case study involves the design and deployment of a hybrid cloud application for image processing and shows how the framework can be used to capture the application requirements, design the application architecture, and automate the deployment of the application. Overall, the article provides a useful framework for modelling hybrid cloud applications and highlights the potential benefits of such a framework for the design, deployment, and management of these applications. It also provides a practical example of the application of the framework, which can help organizations understand how to apply it in their own contexts.[3]

The paper titled "Hybrid Cloud: A Solution to Cloud Interoperability" by Dr.M.P.Dhore in 2018 presents a novel approach for addressing the interoperability challenges in cloud computing. Cloud interoperability is a challenge that organizations face when adopting cloud computing services. Hybrid cloud architectures have emerged as a solution to address this challenge. Hybrid clouds allow organizations to use a combination of public and private clouds, enabling them to leverage the benefits of both. Several studies have investigated the use of hybrid clouds for different applications, including disaster response, healthcare, and secure data sharing. However, challenges related to data security and privacy, data management, and network latency need to be addressed for successful hybrid cloud adoption. In conclusion, the use of hybrid cloud architectures is a promising approach for addressing cloud interoperability challenges. Future research works should focus on addressing the challenges associated with hybrid cloud adoption and developing standards for hybrid cloud interoperability. [3]

"Hybrid Cloud Computing: Security Aspects and Challenges" explores the security considerations and challenges associated with hybrid cloud computing. Hybrid cloud computing presents a combination of public and private cloud infrastructures, aiming to harness the advantages of both environments. The security aspects of hybrid cloud computing encompass various factors.

Firstly, data protection becomes a critical consideration, ensuring the confidentiality and integrity of data during transit and storage across both public and private clouds.

Secondly, implementing robust identity and access management mechanisms is crucial for controlling user access to cloud resources and preventing unauthorized usage. Compliance with regulatory requirements and legal obligations related to data privacy and residency is another aspect to address. Network security measures are essential for safeguarding the infrastructure connecting public and private cloud components. Data segregation is crucial to isolate sensitive data from other users or applications within the hybrid cloud. Lastly, incident response and recovery strategies must be developed to efficiently handle security incidents and mitigate potential disruptions. However, challenges like managing security across multiple cloud providers, maintaining consistent security policies and controls, addressing interoperability issues, and keeping up with emerging security threats pose significant obstacles in hybrid cloud environments.[4]

"Hybrid Cloud Security Measures and Research Challenges" published in 2021 by V.Ambica, Dr.A.Viji Amutha Mary focuses on the security aspects and research challenges associated with hybrid cloud computing. Hybrid cloud security measures refer to the strategies and practices implemented to protect data and resources in a hybrid cloud environment, which combines both public and private cloud infrastructure. Hybrid cloud security measures involve several key aspects. Data encryption is employed to safeguard data during transit and storage, ensuring confidentiality and integrity. Access control mechanisms are implemented to authenticate and authorize users, controlling their access to cloud resources and preventing unauthorized usage. Network security measures, such as firewalls and intrusion detection systems, protect the infrastructure connecting public and private cloud components. Data segregation techniques are employed to separate sensitive data from other users or applications within the hybrid cloud environment. Compliance and legal requirements are addressed to ensure adherence to regulations regarding data privacy, protection, and sovereignty. Effective incident response and recovery plans are developed to handle security breaches and disruptions in the hybrid cloud environment. By implementing these measures, organizations can enhance the security of their hybrid cloud deployments. The research challenges addressed in the paper may include emerging security threats, privacy concerns, interoperability issues between different cloud environments, and the complexity of managing security across multiple cloud providers. [5]

The article "Hybrid Cloud Computing: A Perspective" published in 2022 by Amit Jain provides a comprehensive overview of hybrid cloud computing. The paper begins by defining hybrid cloud computing and its benefits over traditional cloud computing models. It discusses the various types of hybrid clouds, including public-private hybrid clouds, private-community hybrid clouds, and public-multicloud hybrid clouds.

The article goes on to present the advantages and challenges of hybrid cloud computing, including the ability to balance cost, performance, and security requirements. It also highlights the challenges of hybrid cloud computing, such as data privacy, security, and compliance. The paper discusses the various components of hybrid cloud architecture, including the cloud provider, the network, and the management and orchestration layer. It also presents the different types of hybrid cloud integration models, including API-based integration, virtual machine-based integration, and container-based integration.

The article concludes by discussing the future of hybrid cloud computing, including the potential for the adoption of edge computing and the growth of IoT. It also emphasizes the importance of careful planning and risk assessment when adopting hybrid cloud solutions. Overall, the article provides a comprehensive perspective on hybrid cloud computing, including its benefits, challenges, architecture, and integration models. It can serve as a valuable resource for organizations considering the adoption of hybrid cloud solutions. [6]

The article "A Survey on Cloud Computing and Hybrid Cloud" published in 2019 provides an overview of cloud computing and hybrid cloud. The paper begins by defining cloud computing and its various service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). It then discusses the benefits and challenges of cloud computing. The article goes on to introduce hybrid cloud computing and its advantages over traditional cloud computing. It discusses the different types of hybrid clouds, including private-public hybrid clouds, private-community hybrid clouds, and public-multicloud hybrid clouds. The paper presents the benefits of hybrid cloud computing, such as cost savings, scalability, and flexibility. It also highlights the challenges associated with hybrid cloud computing, such as data privacy, security, and compliance. The article concludes by discussing the future of cloud computing and hybrid cloud, including the potential for the adoption of edge computing and the continued growth of the Internet of Things (IoT). It also emphasizes the importance of careful planning and risk assessment when adopting cloud computing and hybrid cloud solutions. Overall, the article provides a useful overview of cloud computing and hybrid cloud, including their benefits, challenges, and future potential. It can serve as a valuable resource for organizations considering the adoption of cloud computing and hybrid cloud solutions.[7]

# 4. HYBRID CLOUD MODEL

## The hybrid cloud model consists of two or more cloud environments that are connected through a single network. These environments can be a combination of public, private, or on-premises clouds, each offering its unique benefits. In a hybrid cloud model, organizations can choose which workloads to store and process in which cloud environment based on their security, compliance, and performance requirements.

## Diagram Description automatically generated

FIGURE 2 Hybrid cloud Services Model

## 5. ADVANTAGES

## Flexibility: Hybrid cloud provides the flexibility to deploy workloads in different cloud environments based on their specific requirements. For example, sensitive data can be stored on a private cloud, while less sensitive data can be stored on a public cloud.

## Cost savings: By using a hybrid cloud, organizations can save costs by using a public cloud for less sensitive data or applications and a private cloud for more sensitive data or applications that require higher levels of security and compliance.

## Scalability: Hybrid cloud allows organizations to scale their infrastructure up or down as per their business needs. This flexibility helps organizations to handle sudden spikes in traffic or demand.

## Disaster recovery: Hybrid cloud provides better disaster recovery options as it allows organizations to replicate data across multiple cloud environments. This ensures that data is always available, even if one cloud environment fails.

## Security: Hybrid cloud provides better security options for organizations. By keeping sensitive data on a private cloud, organizations can ensure that it is protected by robust security measures such as firewalls, intrusion detection systems, and encryption. Public clouds also provide security measures, but they may not meet the stringent security requirements of some organizations. The hybrid cloud model allows organizations to have the best of both worlds by leveraging the strengths of private and public clouds.

## Compliance: Many industries, such as healthcare and finance, have strict compliance regulations that they must follow. The hybrid cloud model allows organizations to store and process data in compliance with these regulations. For example, sensitive patient data can be stored on a private cloud that meets HIPAA regulations, while less sensitive data can be stored on a public cloud.

## Performance: Hybrid cloud provides better performance options for organizations. By leveraging the scalability of public clouds, organizations can handle sudden spikes in traffic or demand. At the same time, they can ensure that critical workloads are processed on a private cloud that provides better performance.

## Disaster recovery: Hybrid cloud provides better disaster recovery options for organizations. By replicating data across multiple cloud environments, organizations can ensure that data is always available, even if one cloud environment fails. This can be critical for industries such as finance and healthcare, where downtime can be costly or even life-threatening.

## Cost savings: Hybrid cloud provides cost savings for organizations. By using a public cloud for less sensitive data or applications and a private cloud for more sensitive data or applications that require higher levels of security and compliance, organizations can save costs. They can also avoid the costs of building and maintaining their own

## data centers.

## 5. Implementing Hybrid Cloud:

## To implement a hybrid cloud, organizations need to follow a few key steps:

## 1. Identify workloads: Organizations need to identify which workloads will be deployed in which cloud environment based on their security, compliance, and performance requirements.

## 2. Choose cloud providers: Organizations need to choose the public and private cloud providers that best suit their needs. They should consider factors such as pricing, security, and compliance when making this decision.

## 3. Connect cloud environments: Organizations need to establish a connection between their public and private cloud environments. This can be done using a virtual private network (VPN) or other secure connection methods.

## 4. Manage and monitor: Organizations need to manage and monitor their hybrid cloud environment to ensure that it is running smoothly. This includes monitoring for security threats, performance issues, and compliance requirements.

## 6. CONCLUSION:

## Hybrid cloud is a powerful cloud computing model that offers many benefits to organizations. It provides the flexibility to deploy workloads in different cloud environments based on their specific requirements, cost savings, scalability, and disaster recovery options. Implementing a hybrid cloud requires careful planning and management, but the benefits can be significant for organizations of all sizes

**HOME ASSIGNMENT-CLOUD COMPUTING**

**Survey and blog on Hybrid Cloud**

**TY-CS-A**

**Group 20**

|  |  |
| --- | --- |
| Rushikesh Dhurat | 63 |
| Disha Khater | 64 |
| Eeshan Umrani | 66 |
| Shreyas Gaikwad | 72 |

Question 1

Chart, pie chart

Description automatically generated

Question 2

Chart, pie chart

Description automatically generated

Question 3

Chart, bar chart

Description automatically generated

Question 4

Graphical user interface, application

Description automatically generated

Question 5

A picture containing graphical user interface

Description automatically generated

Question 6

Chart, pie chart

Description automatically generated

Question 7Graphical user interface, chart

Description automatically generated

Question 8

Chart

Description automatically generated with low confidence

Question 9

Chart

Description automatically generated

Question 10

Chart, pie chart

Description automatically generated