



# A Comprehensive Review of Cloud Environments and Their Comparative Analysis

Ashima Narang<sup>1</sup>, and Nisha Charaya<sup>1</sup>

<sup>1</sup>Assistant Professor, Computer Science and Engineering, Amity University, Gurugram, Haryana, India

<sup>2</sup>Assistant Professor, Electronics and Communication Engineering, Amity University, Gurugram, Haryana, India

Correspondence should be addressed to Ashima Narang; [ashimanarang04@gmail.com](mailto:ashimanarang04@gmail.com)

Received: 4 March 2025

Revised: 17 March 2025

Accepted: 30 March 2025

Copyright © 2025 Made Ashima Narang et al. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

**ABSTRACT-** Cloud computing has transformed how data is stored, processed, and accessed. This paper provides an in-depth review of various cloud environments—public, private, hybrid, and multi-cloud. It compares them across parameters such as cost, scalability, security, and flexibility. Additionally, the paper interprets graphical and tabular comparisons in narrative form to aid understanding without requiring visual figures. The goal is to provide a clear and detailed understanding of the operational dynamics, benefits, and limitations of each cloud model.

**KEYWORDS:** Cloud Infrastructure, Cloud Security, Cloud Scalability, Cost Efficiency, Performance Evaluation, Comparative Analysis

## I. INTRODUCTION

Cloud computing represents a paradigm shift in IT resource management by delivering computing services over the internet. It offers infrastructure (IaaS), platforms (PaaS), and software (SaaS) as services to users on-demand. The increasing demand for scalable and cost-efficient IT solutions has led to the proliferation of different types of cloud environments, each catering to specific organizational needs. This paper explores these environments and compares their features based on critical performance and operational metrics.

Cloud computing has emerged as a transformative paradigm in the field of information technology, enabling on-demand access to computing resources such as servers, storage, applications, and services over the internet. This model shifts the traditional approach of maintaining local servers and data centers toward a more flexible, scalable, and cost-effective solution. The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources” that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

The core characteristics of cloud computing include broad network access, resource pooling, rapid elasticity, measured service, and on-demand self-service [1], [2]. These attributes have led to widespread adoption across sectors, from startups seeking rapid scalability to large enterprises pursuing digital transformation. The global cloud

computing market has witnessed exponential growth, driven by its ability to lower IT costs, increase business agility, and support remote work and globalization trends [3].

Cloud environments are typically classified into four deployment models: **public**, **private**, **hybrid**, and **multi-cloud**. Each model offers unique advantages and trade-offs in terms of cost, performance, security, and management complexity. The **public cloud**, offered by providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, allows organizations to rent computing resources hosted in large-scale, shared data centers [4]. The **private cloud**, in contrast, offers dedicated infrastructure for a single organization, often used in industries with strict compliance and security requirements [5]. **Hybrid cloud** combines both public and private environments, providing flexibility and control over data residency and workload distribution [6]. Finally, the **multi-cloud** model enables organizations to leverage multiple cloud service providers simultaneously, mitigating vendor lock-in and enhancing service diversity [7].

Despite the benefits, cloud adoption introduces challenges, including complex migration processes, data governance issues, security vulnerabilities, and the need for sophisticated orchestration tools [8], [9]. Hence, a comparative evaluation of cloud environments is essential for decision-makers aiming to align IT infrastructure with organizational goals.

This paper aims to provide a comprehensive review of the four major cloud environments, supported by comparative analysis across key performance indicators such as cost-efficiency, scalability, security, performance, and management complexity. By translating tabular and graphical data into narrative form, the paper seeks to offer an accessible yet rigorous foundation for understanding cloud deployment models.

## II. LITERATURE REVIEW

The evolution of cloud computing has been thoroughly examined by numerous scholars and industry experts. A foundational definition of cloud computing was established by **Mell and Grance** [1], who outlined five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), along with three service models (IaaS, PaaS, SaaS) and four deployment models (public, private, hybrid, and

community). This taxonomy has since become the standard framework for understanding cloud systems.

**Buyya et al. [2]** conceptualized cloud computing as the "fifth utility," predicting its role in delivering IT infrastructure similar to traditional utilities like water and electricity. Their work emphasized the economic and technological motivations for cloud adoption, particularly the utility computing model that underpins cloud services. This vision supports the scalability and elasticity characteristics seen prominently in public and multi-cloud architectures.

**Armbrust et al. [3]** provided a comprehensive perspective on the potential and pitfalls of cloud computing, particularly in relation to latency, availability, and security. Their analysis addressed the challenges of data lock-in, performance unpredictability, and debugging in distributed systems—issues especially pertinent to hybrid and multi-cloud deployments.

A more granular definition was presented by **Vaquero et al. [4]**, who examined the technical underpinnings of cloud computing. They highlighted cloud computing’s ability to abstract and virtualize resources, focusing on how this abstraction can affect management complexity. This is particularly relevant in multi-cloud scenarios, where orchestration across platforms increases operational challenges.

Security has been a consistent focus in the literature. **Grobauer et al. [5]** categorized cloud-specific vulnerabilities into structural and operational threats. Their analysis underscored the importance of understanding the unique security posture of different cloud models—public clouds are more exposed to multi-tenancy risks, whereas private clouds, while more secure, still face internal configuration issues.

**Marinos and Briscoe [6]** introduced the idea of community clouds as an extension of private cloud concepts, highlighting the need for shared but secure infrastructure among organizations with similar requirements. Though not as widely adopted as other models, this work laid the groundwork for hybrid and federated cloud models that balance resource sharing with autonomy.

**Gens [7]** emphasized practical insights from industry surveys, identifying top drivers for cloud adoption such as cost savings, flexibility, and speed of deployment. This business-oriented perspective complements academic views by framing cloud model selection in terms of organizational needs and financial considerations.

Further, **Subashini and Kavitha [8]** conducted a focused study on security issues in various service delivery models. They detailed vulnerabilities specific to IaaS, PaaS, and SaaS, reinforcing the argument that security management must be tailored to the chosen service and deployment model.

Lastly, **Petcu [9]** provided a detailed examination of multi-cloud systems. Their work analyzed architectural frameworks and interoperability challenges, arguing for the development of vendor-neutral cloud platforms to prevent lock-in and enable seamless workload migration—a

significant concern for enterprises managing heterogeneous cloud environments.

From the various researches made by the various researchers, **Table 1** given below gives a further clearer view about the ongoing and the types of clouds available in the consecutive years.

Table 1. Literature Survey of the types of Cloud Used

References	Focused Characteristics	Types of Cloud
Mell & Grance [1]	Definition, service models, deployment models	Public, Private, Hybrid, Community
Buyya et al. [2]	Utility computing, scalability, cost-efficiency	Public, Private
Armbrust et al. [3]	Scalability, availability, security challenges	Public, Private, Hybrid
Vaquero et al. [4]	Virtualization, abstraction, management	General cloud concepts
Grobauer et al. [5]	Security vulnerabilities, structural risks	Public, Private
Marinos & Briscoe [6]	Community cloud, shared infrastructure	Community, Hybrid
Gens [7]	Business benefits, cost, agility	Public
Subashini & Kavitha [8]	Security across service models	IaaS, PaaS, SaaS across cloud types
Petcu [9]	Multi-cloud architecture, interoperability	Multi-cloud

### III. COMPARISON ANALYSIS

Each cloud model is suited to specific scenarios:

- **Public cloud** is ideal for startups and small businesses looking for cost-effective and scalable solutions.
- **Private cloud** is preferred by enterprises handling sensitive data, such as healthcare and finance.
- **Hybrid cloud** fits organizations that need to comply with data sovereignty laws while leveraging cloud scalability.
- **Multi-cloud** supports companies requiring diverse services or aiming to avoid dependency on a single provider.

In a hypothetical use case distribution table, public cloud dominates cost-sensitive and rapid deployment categories, private cloud leads in compliance-heavy environments, hybrid cloud suits integration-intensive cases, and multi-cloud is prevalent in global and heterogeneous system deployments.

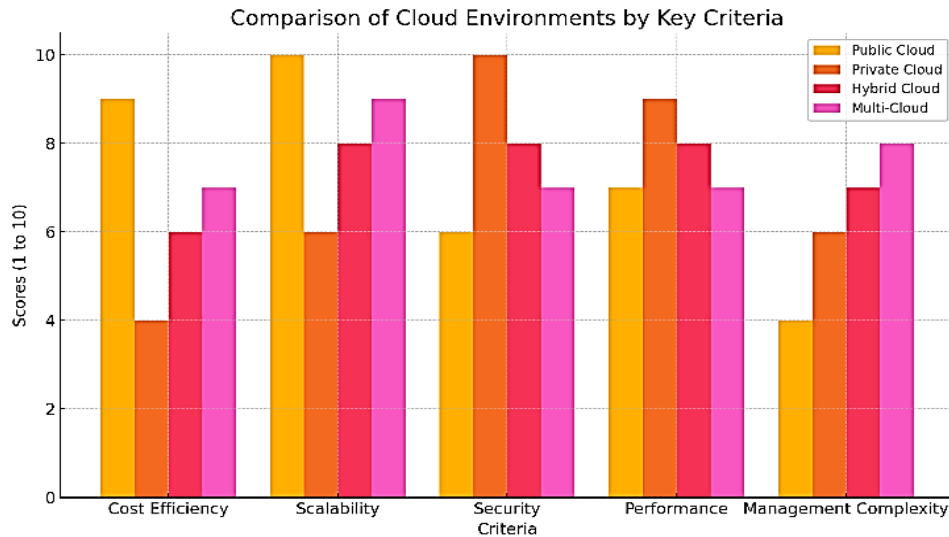


Figure 1. Comparison of cloud Environments

Here is the bar graph shown in figure 1 comparing cloud environments across five key criteria, alongside the corresponding data table given in Table 2:

Table 2. Comparison Table (Scores from 1 to 10)

Criteria	Public Cloud	Private Cloud	Hybrid Cloud	Multi-Cloud
Cost Efficiency	9	4	6	7
Scalability	10	6	8	9
Security	6	10	8	7
Performance	7	9	8	7
Management Complexity	4	6	7	8

**Key Observations:**

- **Public Cloud:** Best for cost and scalability, but lower in security and ease of management.
- **Private Cloud:** Highest in security and performance, with trade-offs in cost and scalability.
- **Hybrid Cloud:** Well-rounded scores, balancing control and flexibility.
- **Multi-Cloud:** Excellent scalability and flexibility, but requires more complex management.

**IV. CHALLENGES AND FUTURE DIRECTIONS**

While cloud computing continues to evolve, each model presents challenges. Public clouds face data privacy concerns; private clouds struggle with cost and scalability; hybrid and multi-clouds require complex orchestration and skilled management. Future developments are expected to

focus on improved automation, better interoperability, and enhanced security frameworks.

Artificial intelligence and edge computing are likely to reshape cloud strategies by decentralizing workloads and enabling smarter resource management. Unified cloud management platforms will be key in simplifying multi-environment orchestration.

Despite the numerous benefits associated with cloud computing—such as scalability, flexibility, and cost-effectiveness—organizations still face significant challenges when deploying and managing cloud environments. These challenges vary by deployment model and are often influenced by factors like data sensitivity, compliance requirements, resource management, and vendor ecosystems.

**Security and Privacy** remain among the foremost concerns, particularly in public and hybrid cloud environments. Public clouds, due to their multi-tenant nature, are more exposed to data breaches and unauthorized access. Ensuring compliance with data protection regulations like GDPR and HIPAA becomes more complex when data is stored across jurisdictions in cloud platforms. While private clouds offer enhanced control, they also require internal security policies and dedicated staff to manage and audit systems, which can be costly [5], [8].

**Vendor Lock-in** is another critical challenge, especially for organizations relying on proprietary services from a single provider. This limits portability and makes migration between cloud providers complex and costly. Multi-cloud environments are often adopted to mitigate this risk, but they introduce **interoperability and integration issues**, as different cloud platforms have varying APIs, tools, and service standards [9].

**Resource Management and Cost Optimization** are persistent concerns. Although cloud models promise cost savings, the lack of real-time visibility into usage patterns can lead to **unexpected billing** and underutilization of resources. Hybrid and multi-cloud setups add layers of complexity to monitoring and cost governance, often requiring advanced cloud management platforms (CMPs) and automation tools. Efficiency and cost are the essential

features for any cloud system and demand for a security mechanism [10].

**Performance Variability** is also a challenge, especially in public clouds where resource contention may lead to inconsistent latency and throughput. Applications requiring real-time processing or low-latency access must be carefully architected, often using edge computing or hybrid solutions to ensure optimal performance [3].

**Complexity of Management and Orchestration** increases as organizations move towards hybrid or multi-cloud strategies. Managing workloads across different infrastructures requires sophisticated orchestration tools and skilled IT teams. Moreover, achieving unified monitoring, security enforcement, and compliance across multiple environments remains a technological hurdle [4], [6].

Looking forward, future directions in cloud computing research and development are focused on several key areas. Edge computing is gaining momentum as a complementary paradigm to cloud computing, enabling real-time data processing at the network edge, thereby reducing latency and bandwidth usage. This is particularly relevant for IoT applications and smart infrastructure.

Artificial Intelligence (AI) and Machine Learning (ML) are being integrated into cloud platforms to enhance predictive analytics, automate resource provisioning, and optimize operational efficiency. AI-powered security monitoring and threat detection are also becoming more prevalent, addressing one of the core challenges in cloud adoption.

Serverless computing or Function-as-a-Service (FaaS) is another emerging trend that abstracts infrastructure management entirely, allowing developers to deploy code in response to events without managing servers. This model offers improved scalability and cost-efficiency, though it introduces new security and performance considerations.

Finally, standardization and interoperability frameworks are essential for the sustainable growth of multi-cloud ecosystems. Industry efforts such as the Open Cloud Computing Interface (OCCI) and initiatives by the Cloud Native Computing Foundation (CNCF) are pushing for open standards that can facilitate better workload portability and integration across platforms.

In conclusion, while cloud computing has revolutionized IT operations, addressing its inherent challenges requires continued innovation, standardization, and strategic planning. As organizations become increasingly digital and distributed, future cloud environments must prioritize agility, security, and resilience to meet the evolving demands of both enterprises and end-users.

## V. CONCLUSION

The choice of cloud environment depends on organizational needs, regulatory requirements, budget, and scalability goals. Public clouds offer unmatched cost benefits and scalability, private clouds provide superior security, hybrid clouds deliver a balance, and multi-clouds enhance flexibility and vendor independence. Understanding the comparative advantages and limitations of each model is crucial for strategic cloud adoption.

## CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest

## REFERENCES

- [1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *NIST Special Publication 800-145*, Sep. 2011. Available from: <https://csrc.nist.gov/pubs/sp/800/145/final>
- [2] R. Buyya et al., "Cloud computing and emerging IT platforms: Vision, hype, and reality," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009. Available from: <https://doi.org/10.1016/j.future.2008.12.001>
- [3] M. Armbrust et al., "A View of Cloud Computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010. Available from: <https://doi.org/10.1145/1721654.1721672>
- [4] L. Vaquero et al., "A Break in the Clouds: Towards a Cloud Definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, 2009. Available from: <https://doi.org/10.1145/1496091.1496100>
- [5] B. Grobauer et al., "Understanding Cloud Computing Vulnerabilities," *IEEE Security Privacy*, vol. 9, no. 2, pp. 50–57, 2011. Available from: <https://doi.org/10.1109/MSP.2010.115>
- [6] A. Marinos and G. Briscoe, "Community Cloud Computing," *CloudCom 2009*, pp. 472–484, 2009. Available from: [https://doi.org/10.1007/978-3-642-10665-1\\_43](https://doi.org/10.1007/978-3-642-10665-1_43)
- [7] F. Gens, "IT Cloud Services User Survey, pt. 2: Top Benefits & Challenges," *IDC Exchange*, 2008.
- [8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011. Available from: <https://doi.org/10.1016/j.jnca.2010.07.006>
- [9] D. Petcu, "Multi-cloud: Expectations and current approaches," *Proc. 2013 Int. Workshop on Multi-cloud Applications and Federated Clouds*, pp. 1–6, 2013. Available from: <https://doi.org/10.1145/2462326.2462328>
- [10] Narang A., Gupta D., Kaur A., "Biometrics-Based Un-Locker to Enhance Cloud Security Systems", *International Journal of Cloud Applications and Computing*, 10 (4), pp. 1-12, 2020. Available from: <https://doi.org/10.4018/IJACAC.2020100101>

## ABOUT THE AUTHORS



**Dr. Ashima Narang** is a distinguished Academician working as an Assistant Professor, with extensive experience of more than 13 years in the field of Computer Science and Engineering. She has contributed significantly to the research Field in the various Areas including Cloud Computing, Virtualisation and Artificial Intelligence. With a strong background in Academics in Computer Sciences, she has various research papers, conference papers and book chapters to her account and has been an active participant in various international conferences and a member of different professional bodies. Her ability to quickly adapt to new technologies, coupled with a creative approach to problem-solving, makes her an effective educator and mentor.



**Dr. Nisha Charaya** is a distinguished Academician working as an Assistant Professor, with extensive experience of more than 14 years in the field of Electronics and Communication Engineering. She has contributed significantly to the research Field in the various Areas including Biometrics, Security, Image Processing and Signal Processing. She has published various

research papers, conference papers and book chapters and has been an active participant in various international conferences and a member of different professional bodies. Her ability to quickly adapt to new technologies, coupled with a creative approach to problem-solving, makes her an effective educator and mentor.