Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549411

COMPARATIVE STUDY OF FRAMEWORKS OF CLOUD

Anuj Singh Tomar
Amity Institute of Information Technology, Amity University, Noida, AIIT
anuj.tomar1@s.amity.edu

Monika Sharma
Amity Institute of Information Technology, Amity University, Noida, AIIT
msharma5@amity.edu

ABSTRACT- In this paper, we contrast the three primary cloud service platforms: Amazon Web Services (AWSs), Google Cloud Platform, and Microsoft Azure. The three major players in the field are briefly introduced in the opening paragraphs of the essay before their likes and dislikes are contrasted. This study examines various cloud computing frameworks that offer an organized method of addressing issues including scalability, security, and interoperability. But as cloud computing becomes more popular, it's important to comprehend the underlying frameworks that enable the delivery of these services. Examining several cloud computing frameworks, including their architectures, deployment methodologies, and service models, is the goal of this research article.

Keywords- Cloud computing, Content Delivery Network, Application Programming Interface.

1. INTRODUCTION

In simple terms, cloud computing means storing and accessing information and programs on the Internet instead of our computer's hard drive. The cloud is just one example of the Internet. In computer communication, we usually represent the Internet as a cloud, as shown in the figure.

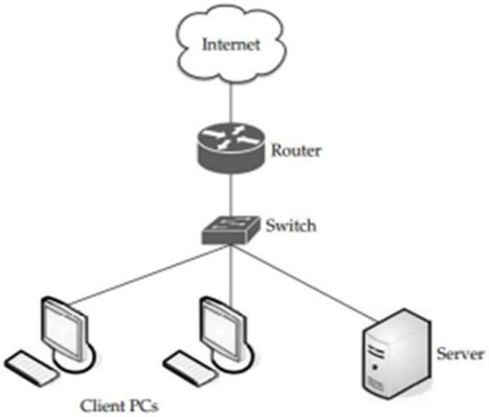


Fig1: Internet is represent by a cloud in a meshwork

Cloud computing revolutionizes the delivery of services by utilizing hardware and software over the internet, enabling users to access information and applications from any internet-connected device [1]. This model allows for the seamless integration of computing resources, which can be rapidly provisioned and released with minimal effort or commercial assistance, encompassing five main features, three service models, and four deployment models [2]. Cloud service providers (CSPs), such as Google, Microsoft, and Amazon, act as vendors offering cloud computing services to both cloud users and network providers, tailoring their offerings based on customer needs and business models [3]. These services span diverse fields like business, education, and management, accessible online through web browsers. The data and software associated with these services are stored on cloud servers housed within data centers Cloud computing has been pivotal in advancing computing capabilities, effectively transforming the landscape. It has played a crucial role in addressing infrastructure requirements and meeting the growing demand. The true potential of cloud computing lies in its ability to deliver hardware and software resources seamlessly across networks, with numerous options available for on-demand rental [4]. Clouds can be broadly categorized based on their characteristics and deployment models.

1. Private cloud: Private clouds are specifically designed for individual organizations or businesses, providing a dedicated and customized infrastructure for their specific needs.

2. Public cloud: Public clouds, offered by major providers like Google, Amazon, and Microsoft, are accessible to the general public and organizations alike. They offer shared infrastructure and services, allowing hundreds or thousands of users to utilize the same resources.

3. Community cloud: Community clouds cater to organizations with shared interests, providing services and infrastructure tailored to their specific community's requirements. It fosters collaboration and resource sharing among organizations within the community.

4. Hybrid cloud: Hybrid clouds combine elements of both private and public clouds, allowing organizations to leverage the benefits of each. While interconnected, private and public clouds maintain their separate identities, enabling organizations to balance control and flexibility according to their needs.

2. LITERATURE REVIEW

Cloud computing is a transformative technology that revolutionizes the management and utilization of hardware and software. It enables organizations to share both physical and non-physical IT infrastructure through the adoption of service-oriented architecture (SOA). This shift toward cloud computing facilitates the reusability of computing resources, leading to cost savings and reduced operational expenses and upfront investment costs. Within the e-business industry, cloud computing plays a crucial role in information exchange and communication technologies [5]. A widely accepted definition characterizes cloud computing as a model that provides network access to integrated computing resources [6]. This model offers low-effort service delivery and encompasses four deployment patterns (public, private, community, and hybrid) and three service models (software-as-a-service, platform-as-a-service, and infrastructure-as-a-service) [7]. Recent years have witnessed significant transformations in information technology, with cloud computing contributing substantially by providing users with increased storage capacity. However, this technological advancement also brings certain risks and threats. The Cloud Security Alliance report highlights various dangers associated with cloud computing and APIs, including abuse, harmful interference, and malicious use [8]. Maintaining information security involves upholding three primary objectives: integrity, confidentiality, and usability. However, longstanding privacy concerns present security risks to these objectives, and both current and previous encryption standards are considered insecure. Additionally, vulnerabilities in data disclosure pose further risks to data privacy. Data tampering also threatens the privacy and integrity of data [9].As technology continues to evolve to meet user needs, threats to cloud security are on the rise. These threats manifest in various forms, including covert misuse of cloud services and related interventions, emphasizing the importance of real attack and defense capabilities. Both cloud customers and cloud service providers face challenges due to the prevalence of unsecure interfaces [10]. Addressing these security vulnerabilities requires collective efforts from all stakeholders involved.

3. METHODOLOGY

(1) What is the future relevance of frameworks cloud computing?

(2) What is the need of frameworks of cloud and how they are affective?

(3) Benefits and service provided by the frameworks.

4. FRAMEWORKS OF CLOUD

There are several popular cloud frameworks available in the market, each with its unique features and capabilities. Some of the most commonly used cloud frameworks include:

- Amazon Web Services (AWS): AWS is one of the most popular cloud frameworks, offering a wide range of services such as compute, storage, databases, and more. It allows users to deploy and manage applications on a global scale.
- Microsoft Azure: Azure is a platform for cloud computing that offers services like virtual machines, databases, analytics, and more. The tools it offers developers allow them to create, test, and publish apps.
- Google Cloud Platform (GCP): Users get access to infrastructure, data storage, and analytics tools thanks to the GCP suite of cloud computing services. Scalable computing, machine learning, and data analytics are some of its features.
- IBM Cloud: IBM Cloud provides a range of services, including infrastructure, software, and platform as a service. It also offers tools for developers to build and deploy applications.
- OpenStack: Networking, storage, and computing services are all provided via the free and open-source OpenStack cloud computing platform. It can be used to build hybrid, private, or public clouds.

4.2 Overcoming Frameworks Limitations

Amazon Web Services

Cost Prohibitive: AWS offers a pay-as-you-goo pricing approach, allowing you to only pay for the services you really utilize. Utilize Reserved Instances for long-term workload commitments or Spot Instances for transient or interruptible workloads to cut costs. You may also analyze and optimize your spending with AWS Cost Explorer.

Usage is not Facile: To assist users in comprehending and making use of its services, AWS offers a wealth of documentation, tutorials, and assistance. To enhance your abilities and boost your confidence in using AWS, you can also benefit from the training and certification programs offered by AWS.

Stewardship of Price: AWS provides a number of tools for controlling costs and keeping tabs on spending, including budget alerts, cost allocation tags, and AWS Organizations for centralized billing and account management.

Overcoming: AWS has a sizable and vibrant user and developer community that exchanges knowledge and best practices. For assistance with identifying and fixing problems, you can also contact AWS Support.

Technical Support Fee: To assist you get the support you require, AWS offers a range of support options at different price points, including a free Basic plan. You can use the documentation, forums, and other tools in the AWS Support Centre to troubleshoot and solve problems.

Microsoft Azure

Imperfect Management Devices: To assist you in effectively managing your resources, Azure offers a range of management tools, like as the Azure interface, Azure CLI, and Azure PowerShell. Additionally, Azure provides third-party integrations and tools, like Terraform and Ansible, that can simplify your administration tasks.

Comparatively Hard to Use: Azure provides a wealth of tools and documentation to assist users in comprehending and utilising its services. In order to make the process of deploying and maintaining resources simpler, Azure also offers a variety of user-friendly interfaces and tools, such as Azure Resource Manager templates and Azure Advisor.

Expensive Data Transfer Cost: To reduce data transfer expenses, you can create a private connection between your on-premises infrastructure and Azure using Azure ExpressRoute. The Azure data transfer pricing calculator can also be used to determine costs and optimise use.

Require Platform Expertise: Azure offers a number of options to learn, including Azure Certification courses and Azure Learn, a free online learning environment with interactive tutorials and labs. In order to assist you in troubleshooting and resolving difficulties, Azure also provides a vast array of support alternatives, such as Azure Support plans, forums, and documentation.

Google Cloud Platform

Safety and Privacy: Google Cloud offers advanced security features and certifications, such as ISO 27001, SOC 2, and HIPAA compliance, to ensure the safety and privacy of your data. Additionally, Google Cloud provides tools like Cloud Data Loss Prevention and Cloud Key Management Service to help you manage and protect your data.

Bounded Control and Flexibility: Google Cloud provides a wide range of services and deployment options, including Compute Engine, Kubernetes Engine, and App Engine, to give you more control and flexibility over your infrastructure. Additionally, Google Cloud offers Cloud Functions, Cloud Run, and Cloud Build for server less and containerized computing.

Vendor Pin-Down: Google Cloud provides an open and interoperable platform that enables you to use multiple cloud providers and technologies. Additionally, Google Cloud offers solutions like Anthos and Cloud Run for Anthos to help you manage and run your applications across multiple clouds and on-premises environments.

Insufficient Characters or Services: Google Cloud provides a wide range of services and solutions, including compute, storage, networking, security, and AI/ML, to meet the diverse needs of different industries and use cases. Additionally, Google Cloud partners with third-party vendors and offers solutions like Google Cloud Marketplace to help you extend and customize your applications.

4.3 CHALLENGE FACED BY AWS, GCP AND AZURE

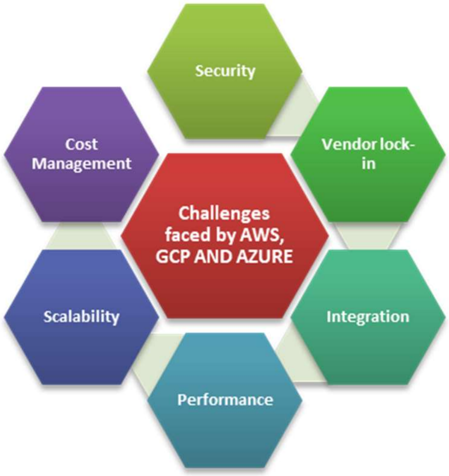


Fig 2: Challenges faced by AWS, GCP AND AZURE

Security: One of the biggest concerns for any cloud computing platform is security. AWS, GCP, and Azure all offer security features, but they are still vulnerable to data breaches and other security threats.

Cost Management: Another common challenge faced by all three frameworks is cost management. While cloud computing can offer significant cost savings compared to on-premises solutions, it can also become costly if not managed properly.

Scalability: As businesses grow, they need to be able to scale their infrastructure quickly and efficiently. All three frameworks offer scalability features, but they can be difficult to manage, especially for businesses that are new to cloud computing.

Complexity: Cloud computing can be complex, and this is especially true for businesses that are new to it. AWS, GCP, and Azure offer many different services and features, and it can be challenging to understand how they all fit together.

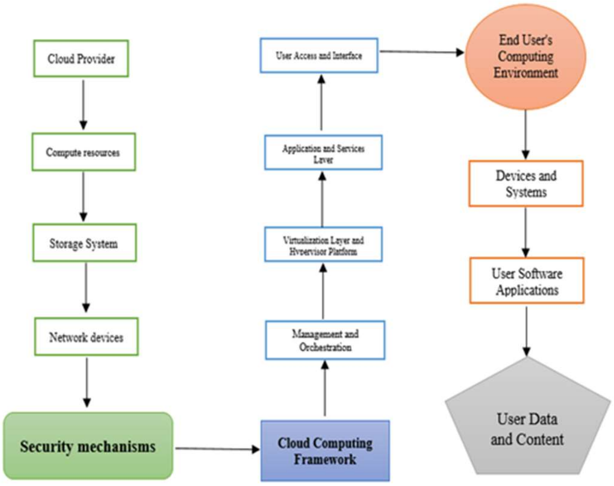
Vendor lock-in: Using a particular cloud computing platform can make it difficult to switch to another platform in the future. Businesses need to be aware of the potential for vendor lock-in and plan accordingly.

Integration: Integrating cloud services with on-premises solutions can be a challenge. This can be especially true for businesses that have legacy systems that are not cloud-compatible.

Performance: Finally, performance can be a challenge for cloud computing platforms. All three frameworks offer high-performance options, but businesses need to ensure that their applications are optimized for the cloud environment to achieve maximum performance.

4 PROPOSED FRAMEWORK

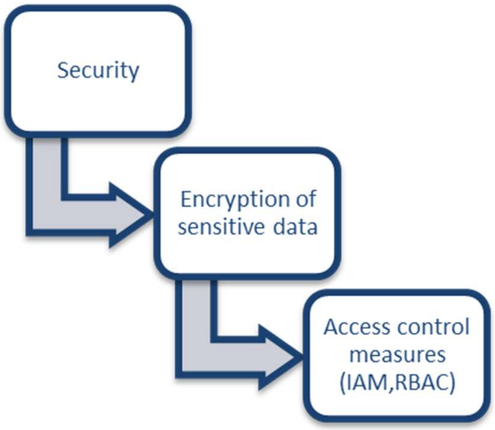
Cloud computing platforms such as AWS, GCP, and Azure have become an integral part of modern businesses. However, they come with several challenges that need to be addressed to maximize their potential. In this research paper, we propose a comprehensive framework to address the common challenges faced by cloud computing platforms. Our framework addresses seven key challenges: security, cost management, scalability, complexity, vendor lock-in, integration, and performance. We present strategies and best practices for each of these challenges and demonstrate their effectiveness through case studies of AWS, GCP, and Azure. By adopting our framework, businesses can optimize their cloud infrastructure, reduce costs, and ensure high levels of security, scalability, and performance.


Cloud Provider
Compute resources
Storage System
Network devices
Security mechanisms
Cloud Computing Framework
Management and Orchestration
Virtualization Layer and Hypervisor Platform
Application and Services Layer
User Access and Interface
End User's Computing Environment
Devices and Systems
User Software Applications
User Data and Content

1. Security: Implement a comprehensive security framework that includes:

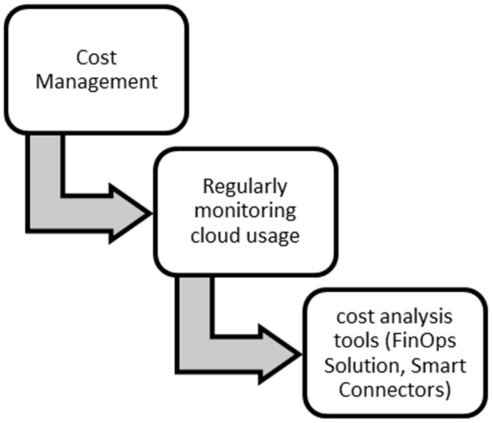
- Access control measures such as identity and access management (IAM), multii-factor authenntication, and role-based access control (RBAC).
- Encryption of sensitive data at rest and in transit using industry-standard encryption protocols.
- Continuous monitoring of cloud infrastructure using third-party security tools to detect and respond to security incidents quickly.

STEP 1


Security
Encryption of sensitive data
Access control measures (IAM,RBAC)

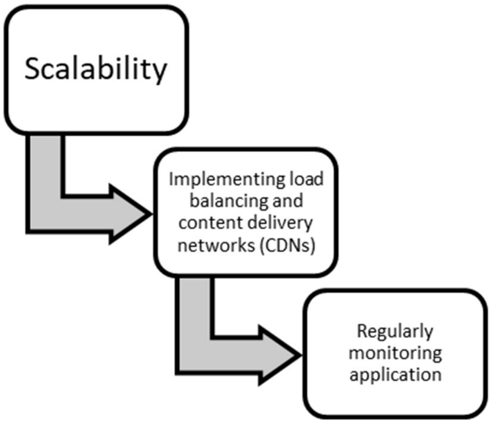
2. Cost Management: Implement cost optimization strategies that include:
- Regularly monitoring cloud usage and identifying areas where costs can be optimized.
- Using cost management features offered by cloud providers, such as reserved instances, spot instances, and autoscaling.
- Implementing resource tagging and tracking to identify unused or underutilized resources.
- Utilizing cost analysis tools to forecast future cloud spend and identify opportunities for cost savings.

STEP 2


Cost Management
Regularly monitoring cloud usage
cost analysis tools (FinOps Solution, Smart Connectors)

3. Scalability: Implement a scalable infrastructure by:
- Designing applications to be cloud-native, using cloud-specific services and tools to take advantage of elastic scaling and high availability.
- Utilizing autoscaling features to automatically adjust resources based on demand.
- Implementing load balancing and content delivery networks (CDNs) to ensure high availability and fast performance.
- Regularly monitoring application performance and adjusting resources as needed to ensure scalability.

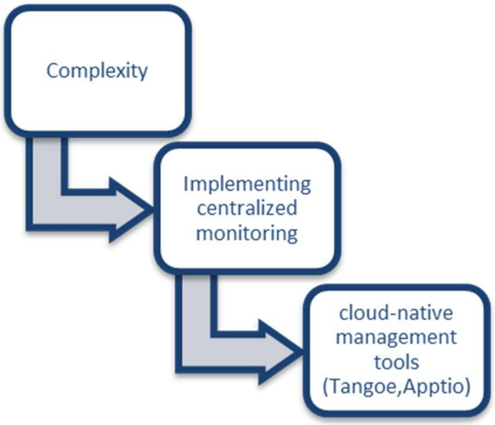
STEP 3


Scalability
Implementing load balancing and content delivery networks (CDNs)
Regularly monitoring application

4. Complexity: Simplify cloud management by:

- Standardizing cloud infrastructure using templates and automation tools to reduce manual configuration and reduce errors.
- Implementing centralized monitoring and management tools to provide a single view of all cloud resources.
- Utilizing cloud-native management tools to simplify management and reduce complexity.

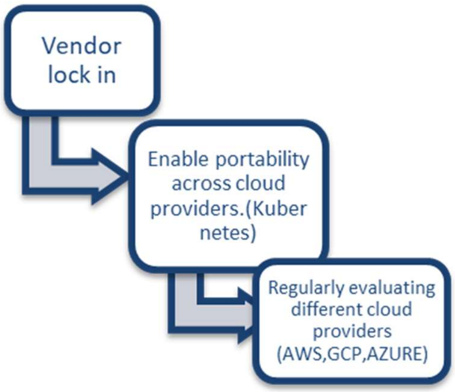
STEP 4


Complexity
Implementing centralized monitoring
cloud-native management tools (Tangoe,Apptio)

5. Vendor Lock-In: Avoid vendor lock-in by:

- Designing applications to be cloud-agnostic, using open-source tools and services wherever possible.
- Leveraging containerization and Kubernetes to enable portability across cloud providers.
- Regularly evaluating different cloud providers to ensure the best fit for business needs.

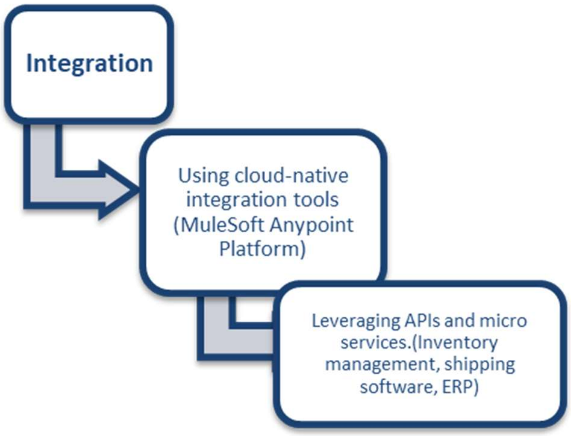
STEP 5


Vendor lock in
Enable portability across cloud providers.(Kuber netes)
Regularly evaluating different cloud providers (AWS,GCP,AZURE)

6. Integration: Simplify cloud integration by:

- Using cloud-native integration tools and services to streamline integration with on-premises systems and applications.
- Leveraging APIs and micro services to enable seamless integration between cloud services and applications.

STEP 6


Integration
Using cloud-native integration tools (MuleSoft Anypoint Platform)
Leveraging APIs and micro services.(Inventory management, shipping software, ERP)

7. Performance: Optimize cloud performance by:

- Designing applications to be optimized for the cloud environment, utilizing cloud-specific services and tools to take advantage of elastic scaling and high availability.
- Regularly monitoring application performance and identifying opportunities for optimization.
- Leveraging CDNs and other caching strategies to improve application performance.

5 CONCLUSION

In this research paper, we explore various service providers and their respective platforms. The focus is on the cost analysis of our preferred service provider's pall platform, as well as comparing it with the original costs of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. These platforms aim to provide convenience to users by allowing them to concentrate on their work rather than the technical aspects. One common feature among all three platforms is the provision of on-demand services, flexibility, support, and security. AWS, being the first to enter the market, has become a popular choice for customers seeking a reliable solution to meet their technological requirements. Microsoft has built a reputation as the most trusted brand in the industry, thanks to the trust and confidence customers have in the quality of their services. On the other hand, Google Cloud offers a wealth of innovative features and is actively involved in various small-scale development projects. This aspect attracts smaller companies, while larger enterprises may find themselves with limited options. In summary, this research paper examines the cost considerations associated with different service providers' platforms, with a specific focus on our preferred pall platform. Additionally, it compares the original costs of AWS, Microsoft Azure, and Google Cloud Platform, highlighting the common features and unique strengths of each provider.

7. REFERENCES

[1] Shirazi,F., and Tehrani,S.R.(2014). The relinquishment of pall computing by small and medium- sized businesses(SMEs) is told by a number of factors. mortal Interface and the operation of Information, edited byS. Yamamoto. Information and moxie in services and operations.

[2] Radu Prodan and Simon Ostermann's paper," A Survey and Taxonomy of structure as a Service and Web Hosting Cloud Providers", was presented at the 10th IEEE/ ACM International Conference on Grid Computing in 2018.

[3]http//en.wikipedia.org/wiki/Cloud gci 1287881,00. html

[4]http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_ gci1287881,00.html

[5]Abedi, Mohammad & Fathi, Mohamad Syazli & Rawai, Shakila.(2012). pall Computing Technology for Collaborative Information System in Construction Industry.

[6]P. Mell andT. Grance(2011) The pall calculating description handed by NIST. NIST Special Publication 800- 145, National Institute of norms and Technology. Technology and norms, 2017. https//nvlpubs.nist.gov(recaptured on November 20, 2018)

[7] Abbas, Zaigham & Hammad, Muhammad & Javaid, Arslan.(2022). pall COMPUTING.

[8]C.S. Alliance, ‘‘ Top pitfalls to pall computing v1. 0, ’’ Cloud Secur. Alliance, Bellingham, WA, USA, White Paper 23, 2019.

[9]S.M. Habib,S. Ries, andM. Muhlhauser, ‘‘ pall computing geography and exploration challenges regarding trust and character, ’’ in Proc. 7th Int. Conf. Ubiquitous Intell. Comput. 7th Int. Conf. Autonomic TrustedComput.,Oct. 2019,pp. 410 – 415.

[10]" Cloud security defence to cover pall computing against HTTP- DoS and XML- DoS attacks," byA. Chonka,Y. Xiang,W. Zhou, andA. Bonti.J. Networked Computing Applications,vol. 34,no. 4, 2021,pp.
1097 – 1107.