International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
September-October-2015 Volume 2, Issue-5
Email: editor@ijermt.org www.ijermt.org

DESIGN AND IMPLEMENTATION OF NEXT-GENERATION CLOUD ARCHITECTURE FOR OPTIMIZED INTERNET-BASED EXECUTION

M E Purushoththaman, Research Scholar, Sunrise university, Alwar

Dr. R. K. Pandey, Professor, Sunrise university, Alwar

ABSTRACT

With its unparalleled scalability and flexibility, cloud computing has completely transformed the IT industry. Nevertheless, there is still a long way to go before cloud performance optimization is achievable. This in-depth research looks at many approaches to improving the efficiency of cloud computing, including DevOps methods, security, architectural design, and resource management.

Keywords: Confidential, data, technology, Resources, DevOps

INTRODUCTION

Computing in the cloud refers to a model wherein users have on-demand access to shared resources like software, platforms, storage, and data over the Internet. Cloud computing refers to a system that allows users to share and access many types of computer resources, such as data, programs, and business processes. In cloud computing, many computers share a single virtual pool of resources. Through the internet, it makes available a pool of computer resources to users. Transparently sharing storage, compute, and services across several users is the goal of cloud computing, a new paradigm in computing. The present state of cloud computing platforms severely restricts the ability to safeguard users' personal information. A significant risk of unauthorized exposure of users' sensitive data by third party service providers exists due to the fact that users' data is sent in an unencrypted format to distant workstations owned and maintained by these providers.

Many methods exist for preventing unauthorized parties from gaining access to users' personal information. Provided is a method for preventing service providers from gaining access to sensitive user information in the course of processing and storing such information in the cloud. Data storage and other services are made available across the internet using cloud computing platforms. Because of its many advantages, such as its low cost, great scalability, and flexibility. In recent years, cloud computing has emerged as a promising new model of distributed computing, particularly in the realm of business, thanks to the proliferation of the Internet and other related factors. Worries over "Internet Security" have only grown in tandem with the advent of the "Cloud Computing" age.

Businesses that want to grow while keeping their cloud expenses low should prioritize cloud optimization. Although it should not be the exclusive emphasis, optimizing cloud costs is an essential part of any successful cloud optimization approach. Optimization in the cloud also includes ways to enhance software quality, communication across teams, application performance, and continuous feedback across the company. You may increase the likelihood of a positive return on investment (ROI) from your cloud migration investment with a solid cloud optimization plan. It bolsters the transition of company processes from an on-premises setting to a cloud one and helps developers become more productive overall.

LITERATURE REVIEW

Zhang (2010) provided a comprehensive overview of next-generation cloud computing architectures, focusing on scalability, elasticity, and cost efficiency. Their work emphasized the importance of virtualization technologies and resource pooling in optimizing internet-based execution. The study also highlighted challenges like latency and security vulnerabilities, proposing solutions for enhanced cloud infrastructure performance.

Armbrust (2010) examined the architectural requirements for cloud computing to support large-scale internet applications. Their research introduced key design principles, such as automated resource allocation and dynamic load balancing, that became foundational for optimizing cloud execution. The study outlined potential future advancements, including energy-efficient data centers and user-centric cloud models.

Buyya (2011) explored the concept of federated cloud computing, where multiple cloud providers collaborate to enhance resource availability and performance. The research introduced a framework for inter-cloud resource management, emphasizing reduced costs and improved execution times for internet-based services.

Fox (2012) analyzed the role of data-intensive computing in shaping next-generation cloud architecture. Their work highlighted the integration of big data analytics into cloud environments, enabling optimized execution for internet-based applications. They proposed a layered approach to cloud architecture, focusing on data storage, processing, and application-level services.

Li (2015) focused on the security and efficiency challenges of next-generation cloud systems. Their research proposed an adaptive framework that combines encryption and compression techniques to optimize data transmission and execution over the internet. The study emphasized the need for robust security mechanisms in highly scalable cloud architectures.

CLOUD ARCHITECTURE

An example of a cloud computing environment is the "cloud architecture" that details the structure and organization of the many cloud service providers' shared resources, applications, and services. It is impossible to have a cloud computing environment without cloud architecture, which guarantees scalability, reliability, and security. To understand and make good use of cloud computing, one must first realize that it is basically a simultaneous service. The safe storage, protection from natural catastrophes, and simple and secure flow to and from the user are all essential requirements for valuable resources such as data, information, and knowledge.

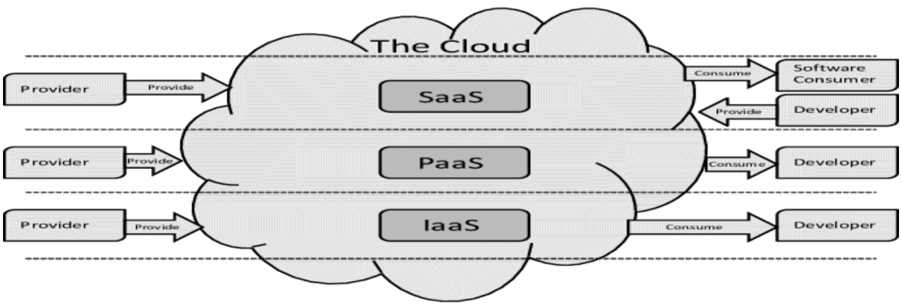

Figure 1: Cloud Computing Architecture

Cloud services have made it possible to efficiently carry out a wide range of IT activities, including storage, compute, databases, and application services, as well as large-scale computing jobs. An essential aspect of the knowledge is the architecture, which includes the components, subcomponents, and general structure of the cloud computing system [6]. A wide variety of cloud computing designs and infrastructures exist, each with its own set of advantages and disadvantages. The goal of these designs is to provide guidelines and best practices for developing and deploying applications in the cloud [20]. The following are the main components of cloud architecture:

i. Models for Cloud Services:

IaaS provides virtualized computing services via the internet, including storage, networking, and virtual PCs.

Consumers may build, operate, and manage apps on a platform as a service (PaaS) without being concerned about infrastructure limits.

• SaaS, or software as a service, removes the need for users to install, maintain, and control software programs locally by offering them over the internet.

ii. Models for Deployment:

• Public Cloud: The resources are made available to everyone who wants to utilize them over the public internet.

Services provided over a private network, often inside an enterprise, allow for more control and personalization. This is known as a private cloud.

To facilitate app and data sharing across them, a hybrid cloud integrates features of both public and private clouds.

iii. Elements of the Cloud Infrastructure:

• Hardware and Software: Server-less computing, virtual machines, and containers can process and execute software.

• Storage: Options other than scalability and permanent data retention, include object, block, and file storage.

• Networking: The framework that allows various cloud services and components to connect to one another.

iv. Virtualized Hosting:

IAM, or Identity and Access Management, prevents unauthorized users from gaining access to sensitive cloud resources by managing their identities and permissions.

Controlled databases provide reliable and expandable data storage; database services assist with this.

• Security Services: Tools and services to make sure data, applications, and infrastructure are safe.

• Logging and Monitoring: Services to track the use, status, and efficiency of cloud resources.

v. Conducting and Supervision:

• Automation: Tools and services that streamline operations, increase output, and reduce human intervention.

To make sure everything runs well while using many cloud services, it's important to have an orchestrator.

vi. Flexibility and scalability:

A system's scalability may be defined as its ability to take on more work by adding more resources.

• Elasticity: the ability to autonomously regulate resources according to needs. Section

vii. Reliability and Uptime:

• Redundancy: A backup copy of critical components is kept on hand to ensure that the system can continue to function in case of a disruption.

• Load balancing: avoiding a single point of failure by spreading network traffic across several servers.

viii. Oversight and Administration of Data:

• Encryption of Data: Making use of encryption to ensure the safety and security of data.

• Data Governance: Plans and processes for handling data at various stages of its lifespan.

Cloud architecture is dynamic and adaptable, always evolving to accommodate new technologies. When designing their cloud architectures, businesses consider their own needs in terms of efficiency, effectiveness, cost-effectiveness, and compliance. Remember that there isn't a common architecture or even fundamental design principles for cloud-based applications just yet. Building a controlled and scalable cloud architecture was the foundation for cloud computing's success, as previously stated. Market demands, fluctuations in the supply and demand for cloud resources, and the ability to readily grow to meet changing service levels should all inform this architecture's design.

Multi-Cloud

One way to distribute workloads across several environments is via multi-clouding, which involves using multiple cloud computing services from different suppliers [21]. In order to meet their diverse range of demands, businesses use the capabilities of many cloud platforms instead of relying on just one cloud service provider. This technique has many benefits, such as improved resilience, increased flexibility, and cost optimization. Some important parts of multi-cloud are:

i. Adaptability and Independence from Vendors: When it comes to specific needs, customers may choose the best services from several providers with multi-cloud configurations. This vendor-neutral method aids businesses in avoiding provider over-reliance by preventing vendor lock-in.

ii. Resilience and Risk Mitigation: Spreading workloads across many cloud providers improves resilience by reducing the effect of potential service disruptions or outages. To ensure business continuity and minimize downtime, workloads may be transferred to another cloud provider in the event of issues with the first one.

iii) Cost Optimization: When companies use multi-cloud solutions, they may compare and choose the most cost-effective services from many vendors, allowing them to maximize their costs. Thus, firms may reduce expenses by taking advantage of sales and discounts offered by different cloud service providers.

iv. Compliance and Global Reach: Businesses may overcome data residency and local law compliance concerns by distributing resources across many geographical regions, made possible by multi-cloud installations. For businesses with operations in more than one country, this is of paramount importance.

iv. Top-Notch Solutions:

When it comes to storage space, processing speed, or specialized services, various cloud service providers excel at different areas. With a multi-cloud approach, companies may build an efficient and customized infrastructure by choosing the best-of-breed solutions for each individual requirement.

vi. Innovation and Proof of Concept: By embracing a strategy that leverages many clouds, enterprises may take advantage of the innovations made by various providers. Also, with this setup, companies can be confident that their infrastructure will be able to handle the ever-evolving cloud landscape and adopt new services and technologies with ease.

vii. Orchestration and Management: When it comes to managing multi-cloud settings, resilient solutions are a must. Automating processes across many cloud providers, optimizing operations, and monitoring performance are all made easier using platforms for cloud administration.

viii. Factors regarding safety:

Safety measures are an integral part of any cloud computing plan. Organizations using a multi-cloud approach must ensure the security of their data and applications by implementing robust security measures, including encryption, compliance controls, and identity and access management. To get the most out of multi-cloud computing and keep risks to a minimum, businesses need to design and manage their installations well. Effective administration and monitoring processes, standard security protocols, and data interchange.

Architecture of Multi Cloud

A multi-cloud architecture makes use of a number of different cloud computing services offered by different vendors. This approach aims to offer enterprises with more flexibility, redundancy, and resource optimization by reducing relying on a single cloud provider. Two major architectural options within the multi-cloud paradigm that are often discussed are the hybrid cloud and the federated cloud.

a. Hybrid Cloud Architecture: This kind of cloud architecture combines resources from internal infrastructure with those from external public cloud providers. It sets up a unified framework that lets on-premises and cloud environments share data and apps without any hitches.

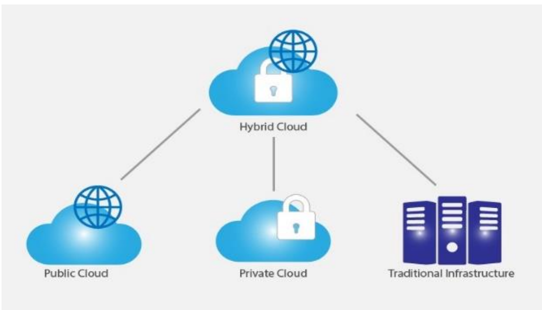

Figure 2: Hybrid Cloud Architecture

i. On-Premises Infrastructure:

Owning and operating one's own data center with proprietary infrastructure has long been the norm for enterprises.

ii. Infrastructure in the Public Cloud: Utilizes resources from several public cloud services, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform.

iii. Connectivity: Virtual private networks (VPNs) or customized network links allow for the creation of quick and secure connections between on-premises and cloud environments.

iv. Orchestration and Management: Tools and platforms for software that provide consistent resource management across on-premises and public cloud settings.

v. Data Integration: Tools and services that facilitate the seamless transmission and integration of data between systems hosted in the cloud and those on-premises.

vi. Security and Compliance: Robust security mechanisms and compliance frameworks are necessary to guarantee data protection and regulatory compliance in hybrid contexts.

b. Federated Cloud Architecture: This structure utilizes a network of interconnected cloud service providers to provide a unified and collaborative framework. The goal is to make it possible to access resources across several clouds with a consistent picture.

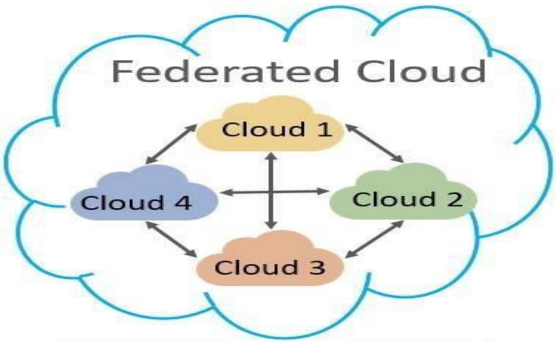

Figure 3: Federated Cloud Architecture

i. Collaborating With Various Cloud Providers: Necessitates coordinating efforts with a wide variety of cloud providers, each of which offers something a little bit different.

ii. Federation Middleware: Middleware is a kind of software that allows different cloud environments to communicate, share resources, and authorize each other.

iii. Directory of Global Resources: A register or directory that provides a unified view of resources available across federated clouds.

iv. Identity and Access Management: Systems for unified authentication and permissions that allow federated clouds to share resources easily and securely.

v. Data Interoperability: Standards and guidelines that support the sharing of data across different cloud services. In conclusion, hybrid and federated cloud architectures provide enterprises with the flexibility and scalability they need to meet their ever-changing business objectives. Which of these models is ideal depends on a lot of factors, such as how sensitive the data is, whether or not the business must comply with regulations, and its specific goals.

Statistics with No Extraction

Cloud Architectures for Distributed Multi-Cloud Computing is a vast and varied field, and this article's charts provide a visual picture of the many methods, designs, algorithms, and tools used in this field. By offering a snapshot of the changing terrain and illuminating the intricate relationship between field approaches, these visual aids are priceless resources for researchers. The charts illustrate the different architectural frameworks, computational models, and technical tools used in different multi-cloud computing cases via detailed classification and discussion.

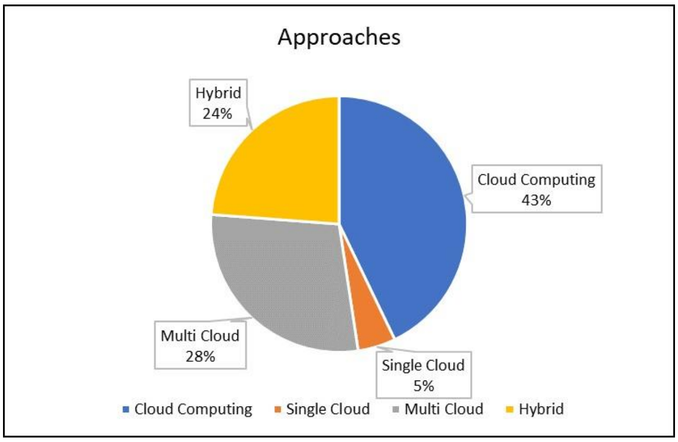

Figure 4: Statistic Chart of Approaches used by Previous Works

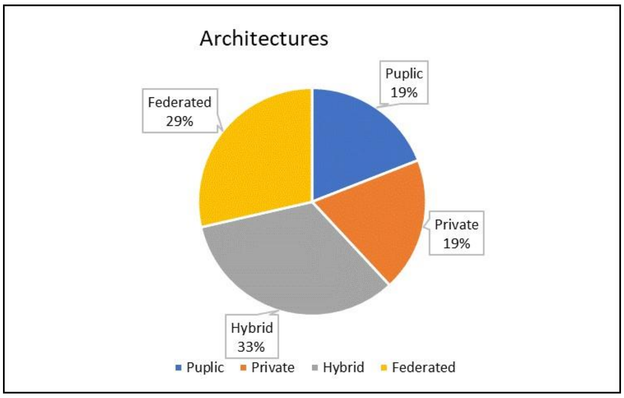

Figure 5: Statistic Chart of Architectures used by Previous Works

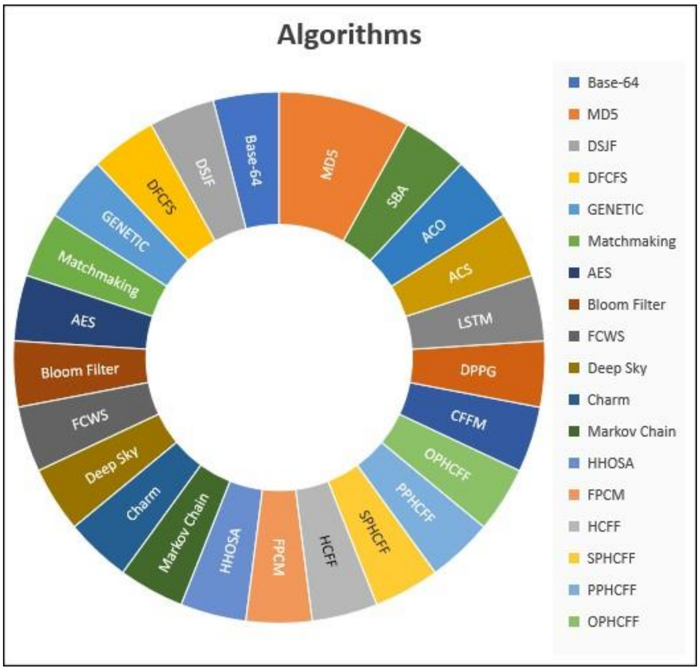

Figure 6: Statistic Chart of Algorithms used by Previous Works

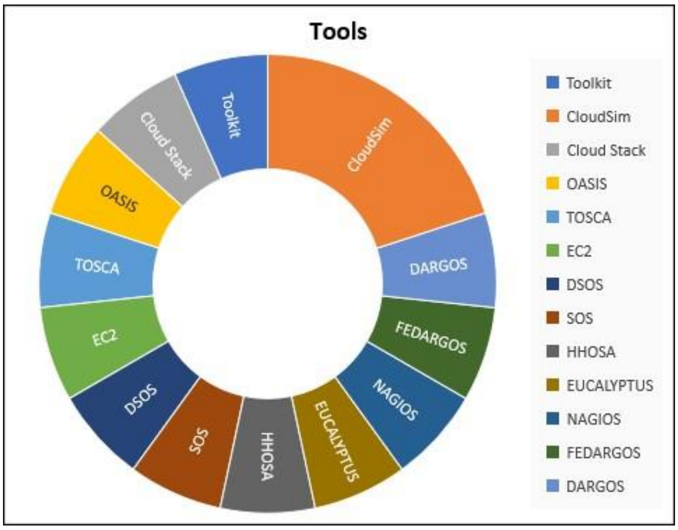

Figure 7: Statistic Chart of Tools used by Previous Works

Direct Connect and Dedicated Connections

A dedicated connection or direct connect service provides substantial benefits for businesses that need constant, high-bandwidth access to cloud resources:

1. Services from Cloud Providers: Tools such as Amazon Web Services (AWS) Direct Connect, Microsoft Azure ExpressRoute, and Google Cloud Interconnect provide for private connections between on-premises systems and cloud servers.

Dedicated connections have two main advantages:

Network expenses for large data transfers are decreased. - Network performance is more stable. - Security is enhanced since the public internet is not used. - Latency is lower than with internet-based connections.

3. Hybrid Cloud Connectivity: Dedicated connections, which allow for smooth integration between on-premises and cloud systems, are especially useful in hybrid cloud settings.

4. Strategies for Using Multiple Clouds: To enable multi-cloud architectures, some firms use dedicated connections to establish high-performance linkages between various cloud providers.

Throughput, packet loss, and jitter are some of the key performance indicators that should be considered while assessing dedicated connection options, as discussed by Aslanpour.

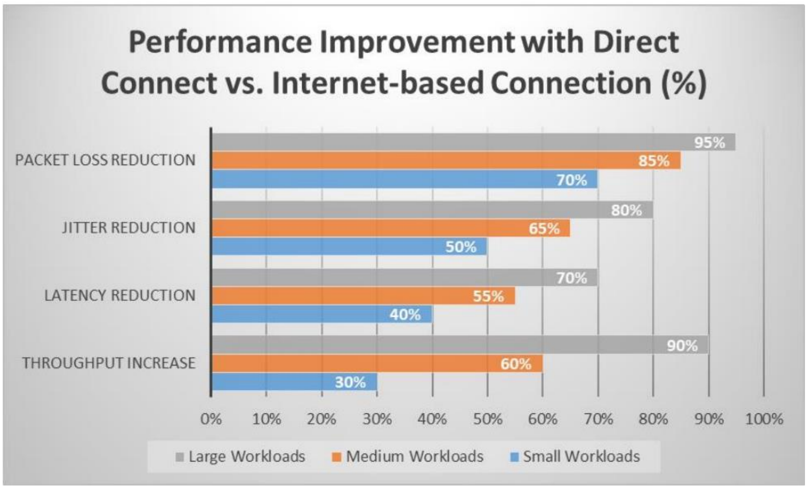

Fig. 2: Performance Improvement with Direct Connect vs. Internet-based Connection (%)

CONCLUSION

An exhaustive literature search on federated and multi-cloud ecosystems reveals a complicated setting with innovative solutions and challenges. The studies provide a structured view of the complex cloud computing world by highlighting the many issues related to service level agreement breaches, operational complexity, vendor lock-in, and security. Strategic planning and governance are essential for the construction of efficient cloud federations, as shown by the research of several architectural types, including public, private, hybrid, and multi-cloud models.

REFERENCES

1. K. Indira and M. K. KavithaDevi, "Effective integrated parallel distributed processing approach in optimized multi-cloud computing environment," in *2014 Sixth International Conference on Advanced Computing (ICoAC)*, Chennai: IEEE, Dec. 2014, pp. 19–22. doi: 10.1109/ICoAC.2014.7229718.

2. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6

3. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

4. Buyya, R., Ranjan, R., & Calheiros, R. N. (2011). InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services. *Cluster Computing, 13*(3), 287–311. https://doi.org/10.1007/s10586-010-0138-8

5. Fox, G. C., Bae, S. H., & Qiu, J. (2012). Cloud computing: Challenges and research directions. *Journal of Cloud Computing: Advances, Systems and Applications, 1*(1), 1–13. https://doi.org/10.1186/2192-113X-1-1

6. Li, X., Qiu, M., Ming, Z., Quan, G., Qin, X., & Gu, Z. (2015). Online optimization for scheduling preemptive tasks on IaaS cloud systems. *Journal of Parallel and Distributed Computing, 72*(5), 666–677. https://doi.org/10.1016/j.jpdc.2012.01.012

7. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology Special Publication 800-145*. https://doi.org/10.6028/NIST.SP.800-145

8. Marinos, A., & Briscoe, G. (2011). Community cloud computing. In *2011 IEEE International Conference on Cloud Computing Technology and Science* (pp. 472–478). IEEE. https://doi.org/10.1109/CloudCom.2011.73

9. Rimal, B. P., Choi, E., & Lumb, I. (2012). A taxonomy and survey of cloud computing systems. *Journal of Network and Computer Applications*, *36*(1), 1–21. https://doi.org/10.1016/j.jnca.2012.04.002

10. Feng, D., Zhang, M., Zhang, Y., Xu, Z., & Li, H. (2013). An overview of cloud computing. *Proceedings of the 2013 International Conference on Cloud Computing and Big Data*, 26–32. https://doi.org/10.1109/CCBD.2013.57