Journal of Global Research in Multidisciplinary Studies (JGRMS)
Volume 2 | Issue 8 | August 2026 | Pages 9-17
DOI: https://doi.org/10.67805/jgrms.v2i8.149
e-ISSN: 3049-2963
RESEARCH ARTICLE OPEN ACCESS
Available online: https://saanvipublications.com/journals/index.php/jgrms

Review of Multi-Cloud Resource Allocation Optimization and Security Assurance Techniques Systems

Dr. Amit Jain
Professor
Department of Computer Science and Engineering,
OP Jindal University, Raigarh (C.G)
amit.jain@opju.ac.in
Corresponding Author: *Dr. Amit Jain(amit.jain@opju.ac.in)

Received: 28 July 2026 | **Revised:** 2 August 2026 | **Accepted:** 5 August 2026 |

***Abstract*—Multi-cloud computing is becoming a prominent paradigm to improve scalability, flexibility, reliability and cost-effectiveness by leveraging services from multiple cloud providers. But distributed resource management with strong security is a big challenge in multi-cloud scenarios, which are heterogeneous and dynamic. This review paper provides an all-inclusive overview on various multi-cloud architectures, deployment models, resource allocation techniques, optimization methods, and security assurance mechanisms. It covers the major resource allocation strategies such as provisioning, scheduling, load balancing, resource scaling and intelligent optimization through machine learning and metaheuristic algorithms to optimize resource utilization and Quality of Service (QoS). Additionally, the article delves into significant security methods for protecting decentralized cloud systems, including authentication, authorization, encryption, intrusion detection, trust management, and zero-trust designs. Also, through the comparison of the most recent literature, the current research trends, challenges and limitations for optimizing resources while keeping security in mind are pointed out. According to the review, combining AI-powered optimisation with sophisticated security frameworks has the potential to enhance the performance, resilience and reliability of multi-cloud environments. Last but not least, the paper outlines future research avenues for explainable AI, federated learning, blockchain-based trust management, energy-efficient resource allocation, and autonomous cloud orchestration to enable secure, scalable, and sustainable next-generation multi-cloud computing environments.**

Keywords—Multi-Cloud Computing, Resource Management, Resource Allocation, Security Assurance, Cloud architecture, Resource Scheduling.

I. Introduction

Computing in the cloud, which provides scalable, on-demand, and cost-effective services over the Internet, has changed the way corporations handle data storage, processing, and management [1]. In the fast-paced digital world, big data analytics, AI, IoT, and enterprise applications are driving a surge in the demand for cloud infrastructures that are highly available, flexible, and resilient. Single-cloud deployments may be simple, but they can also have issues like vendor lock-in, limited service availability, performance bottlenecks, and regulatory restrictions [2]. To address these constraints, a multi-cloud solution has been introduced as a viable approach that allows businesses to leverage cloud services from various providers, offering more flexibility in resource access, fault tolerance, scalability, and disaster recovery.

However, the multi-cloud computing approach also has its drawbacks regarding efficient resource utilization and security assurance, as clouds are inherently diverse with different pricing models, fluctuating workloads, and different security policies [3]. The strategies to allocate resources effectively is critical to schedule workloads, balance loads, provision resources and manage costs while ensuring Quality of Service (QoS). Security measures like authentication, access control, encryption, intrusion detection, trust management, and zero-trust architectures are essential for keeping distributed cloud resources and sensitive data safe from ever-changing threats [4][5]. This paper reviews the latest progress in multi-cloud architectures, resource allocation optimization methods, and security assurance approaches, and identifies the current research gaps and possibilities for future research into secure, intelligent, and efficient multi-cloud systems. The following summarization of the paper are:

- Details the design, implementation, and key characteristics of Multi-Cloud environments, as well as the advantages of these setups in terms of scalability, adaptability, and availability.
- Analyzes the approaches to provisioning resources, scheduling workloads, load balancing, scaling resources and optimization methods to enhance resource utilization and QoS.
- Discusses authentication, access control, encryption, intrusion detection, trust management, and zero-trust architectures as crucial security techniques for protecting multi-cloud systems.

DOI: https://doi.org/10.67805/jgrms.v2i8.149

- Includes discussion of new technologies—including AI/XAI, federated learning, blockchain, energy-efficient optimization, and autonomous cloud orchestration—to build secure, intelligent, and sustainable multi-cloud computing systems.

A. *Structure of the Paper:*

This paper consists of six sections. In section II, multi-cloud computing architecture and models are discussed. In Section III, resource allocation strategies and optimization techniques are reviewed. The techniques for security assurance in multi-cloud systems are introduced in Section IV. In Section V, the most recent literature is reviewed, and in Section VI, the most important results and directions for the future are reviewed.

II. Multi-Cloud Computing Architecture and Models

Multi-cloud computing is the strategy of utilizing two or more CSPs to offer applications, storage, networking, and computing. While single cloud architectures are more restrictive, multi-cloud can help organizations access the unique benefits each provider offers, which include increased availability, scalability, cost savings and resilience as well as lower vendor lock-in [6]. A well-designed multi-cloud architecture enables seamless resource management and service interoperability by using standardized interfaces, orchestration mechanisms and security policies to connect heterogeneous cloud platforms [7]. In these environments, efficient allocation of computing resources, storage resources and networks resources is critical as the resources have to be dynamically allocated to meet the requirements of different applications and QoS. Modern multi-cloud solutions use smart resource management frameworks that combine resource provisioning, workload scheduling, and load-balancing to optimize resource utilization, reduce operational costs, and guarantee uninterrupted service availability [8]. Moreover, the recent developments in AI and ML have greatly improved the utilization of resources, using predictive provisioning, adaptive scheduling, and automated decision-making on diverse cloud configurations.

A. *Multi-Cloud Architecture*

In cloud computing, a multi-cloud architecture is a strategy that uses the resources of more than one cloud provider for application and data deployment, management, and operation [9][10][11]. Workloads are spread across several public, private, or hybrid cloud environments to boost scalability, reliability, flexibility, and cost-effectiveness rather than being placed on a single cloud platform. A typical multi-cloud architecture consists of a combination of computing, storage, networking, security, and application services that are integrated and managed via standardized interfaces, orchestrion platforms, and resource management tools [12]. This architecture facilitates workload distribution, HA, DR, and vendor independence, while guaranteeing security and effective resource usage across diverse cloud architectures.

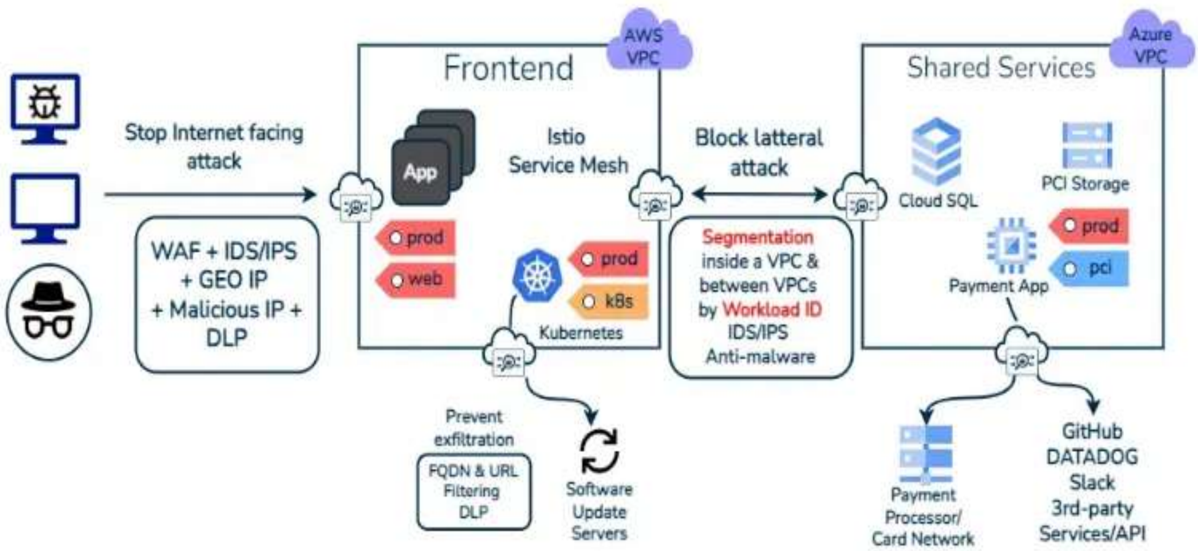

Fig. 1. Multi-Cloud Architecture [13]

The Fig 1. shows a secure multi-cloud reference architecture that provides comprehensive protection from external attacks, lateral movement, data exfiltration, and unauthorized access to cloud-native applications while also securing the communication between front-end applications and shared cloud services. It features multiple layers of security controls, Kubernetes orchestration, VPCs, WAF, IAM, and DevSecOps practices to provide full coverage in distributed cloud environments [14].

1) *User Access Layer*

The user access layer is the point of entry to the multi-cloud environment. It protects incoming Internet traffic with WAF, IDS/IPS, Geo-IP filtering, malicious IP blocking and DLP, to prevent cyberattacks and unauthorized access.

2) *Frontend Cloud Environment*

The front end runs in an AWS VPC and represent the customer-facing applications. It employs Istio Service Mesh for secure service communication, traffic management and authentication and Kubernetes for container orchestration [15][16].

3) *Network Segmentation and Zero-Trust Security*

This layer provides micro-segmentation, internal firewalls, IDS/IPS and anti-malware to secure workloads and block lateral movement by attackers[17]. It is built on Zero-

Trust principles and is continuously verifying access requests within the cloud network [18].

4) Shared Services Environment

The shared services environment runs on an Azure VPC, and contains Cloud SQL databases, payment services, and PCI-compliant storage. Secure communication and resource isolation keeps sensitive business information secure [19].

5) Data Protection

The protection measures that are used for data are encryption, secure access to databases, data loss prevention policies, secure storage, and access control. These methods ensure the security of data confidentiality, integrity, and availability on several cloud platforms.

6) Devsecops and Software Update Infrastructure

This layer takes care of Security aspects in the Software Development lifecycle via secure deployment pipelines, automated software updates and vulnerability patching. Continuous security validation helps to minimise deployment risks [20].

7) Third-Party Integration

The architecture secures interactions with trusted services via authentication, authorization, encrypted communication and API security policies with external payment processors and third-party APIs.

8) Github Repository and CI/CD Pipeline

Source code is kept in GitHub and deployed using automated CI/CD pipeline. The pipeline provides version control, automated testing, security scanning, and continuous deployment to enhance software quality and the speed of secure application delivery.

B. Multi-Cloud Computing Models

Multi-cloud computing models explain the delivery and deployment of cloud services from multiple cloud providers for optimal resource utilization, scalability, and security. The service and deployment models in multi-cloud computing are summarized in Table I. These models guides us to obtain efficient resource allocations, scalability, flexibility, and security in heterogeneous cloud environments [21] [22]. There are three other multi-cloud models:

1) Federated Multi-Cloud

A federated multi-cloud allows multiple cloud providers to cooperate using standardized protocols and interoperability frameworks. This model enables secure sharing of resources, relocating workloads and service interoperability while retaining the independence of participating cloud providers.

2) Community Multi-Cloud

Community multi-cloud is intended for enterprises with identical security, compliance, or operation's needs, like government, healthcare, and research organizations. Infrastructure and services are also shared among participating members, and shared under common governance policies[23].

3) Distributed Multi-Cloud

Distributed multi-cloud spreads resources over different geographic locations to lower latency, increase disaster recovery and service availability. This model enables edge computing and brings applications nearer the end users for better performance [24].

4) Multi-Cloud Software-As-A-Service (Saas) Model

This model involves the use of multiple SaaS applications from various cloud providers to run business operations. Some examples include adding different collaboration tools, CRM systems, and ERP applications, all of which are interoperable and managed from a single location.

TABLE I. SERVICE AND DEPLOYMENT MODELS IN MULTI-CLOUD COMPUTING

Category	Model	Description	Key Features
Service Model	Infrastructure as a Service (IaaS)	Provides virtualized computing resources such as VMs, storage, and networking.	Resource provisioning, VM allocation, scalability
	Platform as a Service (PaaS)	Provides a development and deployment platform without infrastructure management.	Application deployment, platform scalability
	Software as a Service (SaaS)	Delivers fully managed software applications over the Internet.	High availability, load balancing, user accessibility
Deployment Model	Public Cloud	Shared cloud infrastructure managed by third-party providers.	Cost-effective, scalable, on-demand resources
	Private Cloud	Dedicated cloud infrastructure for a single organization.	Enhanced security, privacy, compliance
	Hybrid Cloud	Combines public and private cloud environments.	Workload portability, flexible resource allocation
	Community Cloud	Shared infrastructure for organizations with similar requirements.	Secure collaboration, shared resources
	Multi-Cloud	Uses services from multiple cloud providers.	Vendor independence, resource optimization, reliability, security

III. RESOURCE ALLOCATION IN MULTI-CLOUD ENVIRONMENTS

Resource allocation is one of the basic functions in multi-cloud computing that involves splitting up the computational resources (VMs, containers, storage, bandwidth, processing power, etc.) among multiple cloud service providers. Resource allocation is essential to efficient use of available resources, meet QoS requirements, lower operational cost, lower response time, and increase system reliability [25]. Since multi-cloud environments consist of heterogeneous infrastructures with varying pricing models, SLAs, and resource capacities, intelligent allocation strategies are essential for achieving efficient workload management. VMs and physical resources are two examples of resource allocation mechanisms that cloud computing uses to ensure users have access to limited resources. In the SLA between a cloud provider and a cloud user, the other criteria are just as crucial, as seen in Fig 2.

DOI: https://doi.org/10.67805/jgrms.v2i8.149

Fig. 2. Resource allocation strategy [26]

A possible resource allocation approach is to do the following:

- **Resource Contention:** When several users or applications are sharing a limited resource, delays and performance degradation occur.
- **Resource Scarcity:** Based on the fact that available cloud resources cannot keep up with the need of workloads, and thus resource prioritization must be efficient.
- **Resource Fragmentation:** When resources are distributed unevenly or are divided into small parts, resources are allocated less efficiently than they could be, even if there is capacity to allocate them out.
- **Over-Provisioning:** Provides more resources than needed, resulting in poor resource usage and higher costs.
- **Under-Provisioning:** Provides insufficient resources which leads to bottlenecks, performance degradation or SLA violation.

In multi-cloud settings, there are a number of ways resources can be distributed:

A. Resource Provisioning

Resource provisioning: It is the provisioning of computing resources according to the requirements of an application. It includes the selection of the right cloud provider and the provisioning of virtual machines, containers, storage, and network resources to ensure efficient application deployment without running into resource shortages or overprovisioning [27].

B. Workload Scheduling

Workload scheduling is the process of allocating applications and computational tasks to the available cloud resources. Effective scheduling distributes workloads across various cloud providers for better resource utilization, faster execution, and avoiding performance bottlenecks.

C. Load Balancing

Load balancing is a method of resource management in which multiple computing resources are used to execute a workload to prevent resource congestion and enhance the system's performance. Load balancing is used for efficient use of distributed resources, to improve application availability and reduce response time, to provide fault tolerance and to dynamically route workloads to resources based on resource utilization and network conditions.

D. Resource Scaling

The ability to automatically scale up or down cloud resources in response to demand is known as resource scaling. Vertical scaling optimizes the exploitation of current resources and horizontal scaling adds or eliminates computer instances, allowing for optimal use of resources and cost optimization [28].

E. Task Migration

Task migration transfers applications or workloads from one cloud provider or virtual machine to another when resource congestion, failures, or performance degradation occur. Migration enhances fault tolerance, maintains service availability, and optimizes resource utilization across distributed cloud environments [29].

F. Quality Of Service (Qos)-Aware Resource Allocation

QoS-aware resource allocation ensures that cloud resources satisfy predefined service requirements such as response time, throughput, latency, reliability, and availability. Resource allocation decisions are optimized to maintain SLA compliance while delivering high-quality cloud services.

G. Cost-Aware Resource Allocation

Cost-aware resource allocation is about minimizing the cost of operations while keeping the application performance within acceptable bounds. It takes into account pricing models, resource usage, workload nature, and costs of cloud providers to determine the most cost-effective allocation of resources.

H. Energy-Efficient Resource Allocation

The goal of energy-efficient resource allocation is to lower power usage in cloud data centers, which includes optimizing server use, merging workloads and idle resources. This strategy reduces the cost of operation, and promotes sustainability and green cloud computing [30].

I. Virtual Machine (Vm) Allocation

VM allocation is the process of allocating VM instances to incoming workloads based on resource demand (CPU, memory, storage, bandwidth). Optimal VM allocation can improve system performance, reduce resource waste, and enable dynamic scaling.

J. Container Resource Allocation

Containerized application services are becoming more commonplace in modern multi-cloud platforms and are orchestrated by platforms like Kubernetes. Container resource allocation distributes CPU, memory, and storage resources among containers to achieve efficient application deployment, scalability, and fault tolerance.

1) Resource Allocation Optimization Techniques in Multi-Cloud

The goal of optimizing resource allocation in multi-cloud systems is to make the most efficient use of compute, storage, and network resources. The goal of optimization techniques is to reduce the execution time, operational cost, and energy usage required, while maximizing resource utilization and QoS. The topics covered in this section include static allocation, heuristic and metaheuristic methods, and AI-based optimization.

2) *Static Resource Allocation*

A static resource allocation is when computer resources are given out based on the job that needs to be done and the infrastructure that is available before the application is run. With this method, calculation overhead is minimized because allocation is fixed at run time. Performance is predictable, and it is also straightforward to manage. In a multi-cloud setup with variable workloads and diverse resources, however, static allocation can result in wasted resources, over-allocation, and lack of agility. This makes it less efficient in fulfilling dynamically changing QoS demands and in optimizing the usage of resources provided by different cloud products.

3) *Dynamic Resource Allocation*

Workload demands, system performance, and available resources are the three main factors that determine how resources are distributed in real time through dynamic resource allocation. It differs from static allocation because it uses monitoring, prediction and adaptive decision-making to dynamically allocate or de-allocate resources, thereby enhancing scalability and resource efficiency [31][32]. Cloud orchestration, virtualization, elasticity and composable infrastructure are essential tools supporting dynamic allocation for modern multi-cloud environments. Dynamic allocation adds more complexity to the calculation, but it is essential for efficient use of resources, lower operational expenses, lower latency, and better application performance when workloads change.

4) *Heuristic Optimization*

Heuristic optimization uses problem-specific rules and approximate decision-making strategies to get near-optimal resource allocation solutions without having to execute the optimization for too long. These algorithms are efficient and can be applied in the multi-cloud scenario with large number of clouds where exact optimization techniques are not feasible because of high complexity [33]. The common heuristic method is FCFS, SJF, Min-Min, Max-Min, and Priority-based scheduling. Heuristic methods offer quick decision making on resource allocation, have lower computational costs, but have the potential of converging to local optima and are not suitable for many highly dynamic and heterogeneous multi-cloud workloads.

5) *Metaheuristic Optimization*

Metaheuristic optimization involves population based and nature inspired search methods to search the solution space extensively and find good resource allocation strategies. They can effectively and efficiently solve complex multi-objective optimization problems in multi-cloud setups, due to their ability to balance global exploration with local exploitation [34]. The most common metaheuristic algorithms are GA, PSO, ACO, GWO, and WOA Metaheuristic algorithms are generally more accurate in optimizing and more adaptive than heuristic ones, but require more computational time and parameter tuning.

6) *AI And Machine Learning-Based Optimization*

AI and ML can help to make intelligent decisions regarding resource allocation by forecasting workload demands and automating resource management across multi-cloud environments [35][36]. These technologies optimize how resources are used, can scale with the demand, reduce costs, and enhance QoS using data, making cloud systems more adaptive, reliable, and efficient.

Table II presents a comparison of major resource allocation optimization techniques for multi-cloud environments on their working principles, advantages and disadvantages. It exposes the features of the static, dynamic, heuristic, metaheuristic and artificial intelligence approaches to optimization for efficient resource management.

TABLE II. COMPARISON OF RESOURCE ALLOCATION OPTIMIZATION TECHNIQUES IN MULTI-CLOUD ENVIRONMENTS

Category	Technique	Description	Advantages	Limitations
Resource Allocation	Static Resource Allocation	Resources are allocated before execution based on predefined workload requirements.	Low computational overhead, predictable performance, simple implementation.	Poor adaptability, resource underutilization, unsuitable for dynamic workloads.
	Dynamic Resource Allocation	Resources are allocated and adjusted in real time according to workload demands and resource availability.	High resource utilization, scalability, improved QoS, reduced operational cost.	Higher computational complexity and monitoring overhead.
Optimization Technique	Heuristic Optimization	Uses problem-specific rules to obtain near-optimal solutions with low execution time.	Fast execution, low complexity, suitable for large-scale systems.	May converge to local optimum and provide suboptimal solutions.
	Metaheuristic Optimization	Uses population-based and nature-inspired algorithms such as GA, PSO, ACO, GWO, and WOA to solve complex optimization problems.	High optimization accuracy, global search capability, adaptable to complex problems.	High computational cost, parameter tuning required, longer execution time.
Intelligent Optimization	AI and Machine Learning-Based Optimization	Employs AI and ML algorithms to predict workloads and optimize resource allocation automatically.	Intelligent decision-making, predictive scaling, improved QoS, reduced resource wastage, adaptive resource management.	Requires large training datasets, high computational resources, and increased model complexity.

IV. SECURITY ASSURANCE TECHNIQUES IN MULTI-CLOUD SYSTEMS

In multi-cloud setups, workloads, applications, and sensitive data are spread across a mix of cloud service providers that have distinct infrastructures and security policies, making security assurance crucial. Multi-cloud systems are not just about providing consistent access to data, they also introduce new problems with data security, threat detection, access control, cross-cloud authentication and

DOI: https://doi.org/10.67805/jgrms.v2i8.149

identity management [37] [38]. To solve these challenges, modern security frameworks incorporate IAM, powerful authentication and authorization processes, encryption, IDS, and security-conscious resource allocation to guarantee secure and dependable cloud execution [39]. The combination of these recent developments with AI, ZTA, and automated security orchestration adds an extra layer of security assurance, ensuring continuous monitoring, adaptive access control, anomaly detection, and intelligent resource management in various distributed cloud environments.

Table III demonstrates the comparison of major security assurance technique applied in multi-cloud system, description, benefits and drawbacks of these techniques for secure and efficient cloud resource management.

TABLE III. COMPARISON OF SECURITY ASSURANCE TECHNIQUES IN MULTI-CLOUD SYSTEMS

Category	Technique	Description	Advantages	Limitations
Identity and Access Management (IAM)[40]	Centralized IAM	Manages user identities and access policies across multiple cloud platforms using unified identity governance.	Simplifies identity management, reduces identity sprawl, improves compliance and centralized policy enforcement.	Complex integration across heterogeneous cloud providers and increased management overhead.
Authentication and Authorization[41]	Multi-Factor Authentication (MFA), Single Sign-On (SSO), RBAC, ABAC	Verifies user identities and enforces access permissions based on authentication and predefined authorization policies.	Strengthens access control, prevents unauthorized access, improves user convenience, and supports regulatory compliance.	Additional authentication steps may increase user complexity and administrative effort.
Data Security[42]	Data Protection Mechanisms	Protects data throughout its lifecycle using secure storage, access control, integrity verification, backup, and privacy-preserving techniques.	Ensures confidentiality, integrity, availability, and compliance with security regulations.	Data management becomes more challenging across distributed multi-cloud environments.
Encryption[43]	AES, RSA, ECC, Homomorphic Encryption	Encrypts data during storage and transmission to prevent unauthorized disclosure and secure cross-cloud communication.	Provides strong data confidentiality, secure communication, and protection against data breaches.	Introduces computational overhead and encryption key management complexity.
Intrusion Detection [44]	AI/ML-Based Intrusion Detection Systems (IDS)	Continuously monitors network traffic, user behavior, and system activities to identify malicious attacks and anomalies.	Early threat detection, improved security monitoring, automated incident response, and reduced attack impact.	High computational requirements and potential false-positive alerts.
Security-Aware Resource Allocation[45]	Secure Scheduling and Risk-Aware Resource Provisioning	Allocates computing resources based on workload requirements while considering security policies, trust levels, risk scores, and compliance constraints.	Balances security, performance, resource utilization, and Quality of Service (QoS) in multi-cloud environments.	Increased scheduling complexity and additional decision-making overhead.

V. LITERATURE REVIEW

This section provides a comprehensive overview of the literature on methods for ensuring the security of multi-cloud resource allocation and optimization. Mohammad Swaleh Khan et al. (2026) suggest intelligent resource allocation framework, which uses ML techniques for optimization of cloud resource utilization. The work proposed involves analyzing workload attributes like CPU usage, memory usage, and network traffic to forecast optimal resource designations. Various ML algorithms such as RF, XGBoost, LR, and LSTM are deployed and tested. Experimental results have shown that ensemble and DL models have a great effectiveness in achieving high allocation accuracy and system efficiency [46].

Preethi et al. (2025) The goal of this research is to build a safe system that can withstand attacks from inside. Data submission, encryption, distribution, and decryption are all encompassed in the proposed F-SE method. The proposed methodology also encrypts massive datasets before storing them in many clouds. The simulation study makes advantage of real-time cloud storage systems. Compared to the existing methods, the results showed that the proposed F-SE model was superior [47].

Bo Yuan et al. (2024) introduces a novel approach to allocating resources that maximizes the distribution of AI tasks in environments with many clouds. Data transfer between clouds, decision-based adaptive support learning, multi-dimensional monitoring and profiling, performance measurement and performance prediction, and other advanced ML techniques are all part of the system. The results are a big step up from previous solutions, with average resource use going up by 9.8% and job completion time going down by 21%. The system has remarkable reliability and scalability even when tested with 5,000 virtual machines. During a hypothetical three-year period, a cost-benefit analysis reveals a decrease of 30.6% in Total Cost of Ownership and a decrease of 30.5% in energy and gas usage, which translates to carbon emissions [48].

Ayman Mohamed Mostafa et al. (2023) created a framework for adaptive multi-factor multi-layer authentication that incorporates intrusion detection and access control into its automated method selection process. Several authentication elements, such as the user's geolocation and browser confirmation method, are used to boost the identification verification of cloud users. These factors include the user's length, validity, and value, which helps to improve the authentication process and decrease false alarms. Data is further encrypted using an additional layer of AES-based security to prevent disclosure. Passwords stored in the cloud directory provider are encrypted using the AES algorithm [49].

Kapil N. Vhatkar and Girish P. Bhole (2022) proposes a novel optimization concept and uses it to create an improved model for allocating resources within containers. An innovative hybrid algorithm called Whale Random update assisted Lion Algorithm (WR-LA) was developed to facilitate optimal resource allocation in containers. It combines elements of both WOA and LA. Optimal resource allocation is also achieved by taking into account goals such as Threshold Distance, Balanced Cluster Use, Total Network Distance, and System Failure, in that order. Finally, the suggested model outperforms other traditional models in terms of performance [50].

Vasugi T (2022) proposes a multi-cloud resource management architecture powered by AI to enhance network security, operational efficiency, and environmental dynamicity. It tackles the diverse needs of regulated financial systems by integrating ML–derived workload prediction, automated resource orchestration and policy-based compliance enforcement. Additionally, the model includes data-governance alignment, cost-aware optimization, and cross-cloud interoperability for optimal performance across diverse cloud environments. However, experimental evaluations have shown that the framework can reduce resource wastage, boost system reliability and increase the security resilience in multi-cloud banking systems [51].

A comparative analysis of multi-cloud resource allocation optimization and security assurance techniques is presented in Table IV.

TABLE IV. Comparative Analysis of Multi-Cloud Resource Allocation Optimization and Security Assurance Techniques

Authors & Year	Objective	Techniques/Approach	Multi-Cloud Focus	Key Findings / Contributions
Mohammad Swaleh Khan, Mohammad Taufeeq and Mood Zohaib Khan (2026)	To develop an intelligent framework for optimizing cloud resource utilization using machine learning.	Random Forest, XGBoost, Logistic Regression, LSTM, Workload Prediction	AI-Based Resource Allocation	Developed an ML-driven resource allocation framework that accurately predicts optimal resource configurations, improving allocation accuracy and overall system efficiency.
Preethi et al. (2025)	To develop a secure framework that protects data against insider attacks in multi-cloud environments.	F-SE Framework, Encryption, Secure Data Storage, Multi-Cloud Security	Security Assurance & Data Protection	Proposed the F-SE security model that enhances secure data submission, encryption, storage, and decryption while effectively mitigating insider attacks in real-time cloud environments.
Bo Yuan et al. (2024)	To optimize AI task distribution and resource allocation across multi-cloud environments.	ML, Performance Prediction, Multi-Dimensional Monitoring, Adaptive Decision Support	AI-Driven Multi-Cloud Resource Optimization	Improved average resource utilization by 9.8%, reduced task completion time by 21%, lowered total cost of ownership by 30.6%, and reduced energy consumption by 30.5%.
Ayman Mohamed Mostafa et al. (2023)	To strengthen cloud security using adaptive authentication and access control mechanisms.	Multi-Factor Authentication, Access Control, Intrusion Detection, AES Encryption	Cloud Security Assurance	Proposed a multi-layer authentication framework that improves identity verification, reduces false alarms, and enhances data confidentiality through AES encryption.
Kapil N. Vhatkar and Girish P. Bhole (2022)	To optimize container resource allocation in cloud environments.	WR-LA, WOA, LA	Container Resource Optimization	Introduced a hybrid optimization algorithm that improves container resource allocation by considering balanced clustering, system failures, threshold distance, and network distance.
Vasugi T (2022)	To design an AI-based architecture for efficient and secure multi-cloud resource management.	ML, Workload Prediction, Automated Resource Orchestration, Policy-Based Compliance, Anomaly Detection	AI-Based Multi-Cloud Management & Security	Developed an AI-driven architecture that improves resource utilization, cost optimization, system reliability, security resilience, and cross-cloud interoperability in multi-cloud environments.

VI. Conclusion and Future Work

Multi-cloud computing is now an important strategy for providing scalable, reliable, and cost-effective cloud services by leveraging resources from various cloud providers. But the idea of multi-cloud introduces a lot of challenges when it comes to resource allocation and workload optimization or security assurance. This review included an in-depth description of multi-cloud architecture and deployment, along with resource allocation strategies and optimization techniques that enhance resource utilization, execution time, operational costs, and QoS. The paper also examined several key approaches to security assurance such as authentication, access control, encryption, intrusion detection, trust management, and zero-trust security frameworks that are crucial for securing distributed cloud infrastructures. The literature reviewed reveals that the use of intelligent optimization techniques alongside sophisticated security measures can substantially improve the performance, security and dependability of multi-cloud environments. Future studies are needed to address the challenges of AI- and XAI-based resource allocation, federated learning, trust management using blockchain, energy-aware scheduling, zero-trust security architectures, quantum-resistant cryptography, and autonomous cloud orchestration. They can enhance decision making, secure the system, use resources more efficiently, and enable the creation of secure, scalable and sustainable next-generation multi-cloud environments.

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of interest.

How to cite this article:
A. Jain, "Review of Multi Cloud Resource Allocation Optimization and Security Assurance Techniques Systems," *Journal of Global Research in Multidisciplinary Studies*, vol. 2, no. 8, pp. 9–17, Aug. 2026.Doi. https://doi.org/10.67805/jgrms.v2i8.149

REFERENCES

[1] M. J. B. Mehta, "AI-Driven Test Engineering for Cloud-Native Systems," *Int. J. Data Sci. IoT Manag. Syst.*, vol. 5, no. 1, Jan. 2026, doi: 10.64751/ijdim.2026.v5i1.297.

[2] V. K. Sharma and A. K. S, "Hierarchical Cloud-IoT Architecture for AI-Powered Intelligent Disaster Response," in *2025 7th International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, IEEE, Oct. 2025, pp. 603–610. doi: 10.1109/ICIDCA66325.2025.11280408.

[3] R. K. Kanneganti, "Security and Compliance Issues in Cloud-Based Deployments of Content and Workflow Management Systems," *Eastasouth J. Inf. Syst. Comput. Sci.*, vol. 2, no. 01, pp. 131–138, Aug, 2024, doi: https://doi.org/10.58812/esiscs.v2i01.1122.

[4] D. R. Azmeera and J. Hyatt, "Software Errors, Product Functionality, and Organizational Cascades: Evidence from Developer-Lived Experience," 2026.

[5] S. Tyagi and A. Tyagi, "Evaluating the Performance with Deep Learning Techniques in Cybersecurity for Effective Threat Detection," 2026, pp. 437–452. doi: 10.1007/978-981-96-8687-2_31.

[6] J. B. Mehta, "Ai-Driven Compliance Validation System And Framework For Multi-Cloud Enterprises," 63/919,564, 2025

[7] K. Jangiti, "Design and Validation of a Machine Identity Governance Framework for AI Agents in Multi-Cloud Environments," in *SoutheastCon 2026*, 2026, pp. 1–6. doi: 10.1109/SoutheastCon63549.2026.11476363.

[8] K. R. Kiran, "API Integration Barriers in Case-Based Process Management: A Review of Interoperability and Real-Time Response Constraints Outline," *Qual. Res.*, vol. 25, no. 3, pp. 21–48, 2025, doi: doi.org/10.5281/zenodo.16782616.

[9] A. B. Chatterjee, "A Proposed Hybrid Distributed Ledger Architecture for Cross-Border Payments: Design and Conceptual Framework," *Int. J. EmergingTrends Comput. Sci. Inf. Technol.*, vol. 1, no. 1, pp. 210–217, Feb, 2026, doi: https://doi.org/10.63282/3050-9246.IJETCSIT-V7I1P132.

[10] K. K. Mohammed, "Leadership Practices of Data Engineering for AI and Machine Learning," *Int. J. Sci. Res. Eng. Trends*, vol. 12, no. 1, pp. 1–5, 2026.

[11] K. Jangiti, "Design and Validation of a Machine Identity Governance Framework for AI Agents in Multi-Cloud Environments," in *SoutheastCon 2026*, Huntsville, AL, USA: IEEE, 2026, pp. 1–6, February-March. doi: 10.1109/SoutheastCon63549.2026.11476363.

[12] R. Azmeera, "The Effects of Increased Software Errors on Software Product Functionality," University of the Cumberlands, 2025.

[13] Fluence, "Multi-Cloud Architecture: Proven Strategies for Resilience, Savings, and Growth in 2026," Fluence.

[14] S. Chatterjee, "A Data Governance Framework for Big Data Pipelines: Integrating Privacy, Security, and Quality in Multitenant Cloud Environments," *Tech. Int. J. Eng. Res.*, vol. 10, no. 5, pp. 746–758, May, 2023, doi: https://tijer.org/TIJER/papers/TIJER2305456.pdf.

[15] S. R. Chanthati, "Implementing a Graph Neural Network (GNN) in Amazon Web Services (AWS) involves setting up infrastructure for data processing, training, and deployment," *WCAIAA2025*, 2025, doi: 10.5281/zenodo.20313312.

[16] M. Mittal, "The Metaverse and Web3: A New Era of Decentralized Digital Ecosystems," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 10, no. 06, Jun. 2022, doi: 10.15680/IJIRCCE.2022.1006001.

[17] D. Jain and S. Jain, "Artifact Comparison Analyzer: Evaluating Microservice Build Metrics for Performance and Efficiency Improvements," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA: IEEE, 2026, pp. 1–6, February. doi: 10.1109/ICAIC67076.2026.11395685.

[18] V. Gudur, C. Upadhyay, S. Sudarsan, R. Dandigam, A. Patel, and S. Tiwari, "Trust Deviation Metrics (TDM) for AI-Driven Cloud Orchestration," in *Proceedings of the 2026 9th International Conference on Information and Computer Technologies*, New York, NY, USA, NY, USA: ACM, Mar. 2026, pp. 539–544. doi: 10.1145/3803291.3803293.

[19] H. P. Cyril, N. D. Bhandarwar, S. Kumara, and S. Mathur, "Securing Containerised Applications Using Kubernetes-Based Orchestration in Software Development," in *2026 International Conference on Intelligent Computing, Networks, and Security (IC-ICNS)*, Bhubaneswar, India: IEEE, 2026, pp. 1–6, March. doi: 10.1109/IC-ICNS68863.2026.11537887.

[20] S. K. Madishetty, "Cyber Resilience and DevOps in Operating Rooms: Securing Connected Embedded Medical Devices in High Risk Clinical Environments," *J. Electr. Syst.*, vol. 19, no. 3, pp. 244–253, Jan. 2024, doi: 10.52783/jes.9597.

[21] A. Warrier, "Event-Driven iPaaS Architectures for Real-Time Healthcare Data Synchronization Across Enterprise Systems," *IJLRP-International J. Lead. Res. Publ.*, vol. 3, no. 8, pp. 1–9, August, 2022.

[22] R. Taware, S. K. Anumula, H. R. Chennam, and O. H. Kundurthy, "Exploring AI-Based Self-Configuring Slice Allocation Across Hybrid Access Networks," in *2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON)*, IEEE, Aug. 2025, pp. 1–6. doi: 10.1109/NMITCON65824.2025.11188257.

[23] R. rao Thallada, N. Alapati, and K. Nallabothu, "Explainable AI-Driven Predictive Risk Management Framework for Enterprise GRC Platforms," 2026. doi: https://doi.org/10.21203/rs.3.rs-9328473/v1.

[24] P. C. Shekhar, "Chaos Testing: A Proactive Framework for System Resilience in Distributed Architectures," *Int. J. Sci. Res.*, vol. 13, no. 11, pp. 851–855, 2024.

[25] R. Lingam, *Integrating Trustworthiness Into the AI Lifecycle (Trustworthiness)*. IGI Global Scientific Publishing, 2026. doi: 10.4018/979-8-3373-6935-8.ch008.

[26] T. Alyas, T. M. Ghazal, B. Sulaiman Alfurhood, G. F. Issa, O. Ali Thawabeh, and Q. Abbas, "Optimizing Resource Allocation Framework for Multi-Cloud Environment," *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 4119–4136, 2023, doi: 10.32604/cmc.2023.033916.

[27] Omoniyi Babatunde Johnson, Jeremiah Olamijuwon, Emmanuel Cadet, Olajide Soji Osundare, and Zein Samira, "Designing multi-cloud architecture models for enterprise scalability and cost reduction," *Open Access Res. J. Eng. Technol.*, vol. 7, no. 2, pp. 101–113, Nov. 2024, doi: 10.53022/oarjet.2024.7.2.0061.

[28] P. C. Pradnya H Desai, Parikshit Mahalle, *Intelligent Access Control Schemes for the Internet of Everything: A Survey of Techniques, Challenges, and Future Directions*. Springer Nature Switzerland, 2026.

[29] S. D. Veeravalli, S. B. Venkata, A. Ashirova, R. MS, S. A. D. Poovaiah, and D. Turaev, "Breaking the Swarm Paradigm: Single Candidate Optimization for Cloud Task Allocation," in *2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3)*, Bhubaneswar, India: IEEE, 2025, pp. 1–7, July.

[30] Y. Muni, "A Review of Efficient Routing Architectures Using OSPF, BGP, and MPLS in Multi-Protocol Networks," *Eng. Technol.*, vol. 11, no. 01, pp. 8597–8604, January, 2026, doi: https://doi.org/10.47191/etj/v11i01.21.

[31] M. Ramees, C. Mukkolakkal, and A. C. Overview, "1.5 Million Messages Per Second on 3 Machines : Benchmarking and Latency Optimization of Apache Pulsar at Enterprise Scale," *Arxiv J.*, pp. 8–11, 2026.

[32] R. U. L. A. Yeruva, D. Singh, S. Suddala, and N. Bhatt, "Augmented Data Management: Enhancing Cache Performance and Cybersecurity through AI and Mobile Integration," *J. Comput. Mech. Manag.*, vol. 5, no. 3, pp. 280–293, May, 2026, doi: https://doi.org/10.57159/jcmm.5.3.26691.

[33] M. Kari, "A Comprehensive Performance Study of Hashing Algorithms: MD5, SHA-256, and SHA-512 using Java," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 6, pp. 1–8, 2023.

[34] R. V. S. S. Bharattej, R, H. M. Al-Jawahry, S. Rafikiran, D. Beula, and E. T. V. R. Kanth, "Blood Pressure Monitoring and Hypertension Prediction using Dynamic Opposite Learning Based Prairie Dog Optimization Algorithm," in *2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, Tumkuru, India: IEEE, 2024, pp. 1–7, December. doi: 10.1109/ICMNWC63764.2024.10872294.

[35] S. K. Malaraju and S. K. Madishetty, "AI-Augmented Compiler Optimization for Energyefficient Software Execution on

Embedded Systems," in *2025 14th International Conference on System Modeling & Advancement in Research Trends (SMART)*, Moradabad, Uttar Pradesh, India: IEEE, 2025, pp. 1–6, November. doi: 10.1109/SMART66937.2025.11389313.

[36] M. Mittal, "The Rise of Generative AI: Evaluating Large Language Models for Code and Content Generation," *Int. J. Adv. Sci. Eng. Technol.*, vol. 10, no. 4, pp. 1–7, 2023.

[37] S. Singamsetty, "AI-Enabled Data Stewardship Real-Time Alignment of Privacy and Storage Policies Across Global Systems using Deep CNN-RNN Techniques," in *2025 5th Asian Conference on Innovation in Technology (ASIANCON)*, PIMPRI, India: IEEE, 2025, pp. 1–6, August. doi: 10.1109/ASIANCON66527.2025.11281010.

[38] K. Venkata and R. K. Koppireddy, "Revolutionizing Identity Verification: AI-Driven Digital identity solutions for a secure and seamless future," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 1, pp. 2814–2824, February, 2025, doi: 10.32628/CSEIT251112301.

[39] M. R. C. Mukkolakkal, "Deploy, Calibrate, Monitor, Heal -- No Human Required: An Autonomous AI SRE Agent for Elasticsearch," 2026. doi: https://doi.org/10.48550/arXiv.2604.03933.

[40] N. Adik, "The Rise of Open and Free Networks: A Community-Driven Paradigm for Decentralized Connectivity," in *2025 IEEE First International Conference on Innovations in Engineering and Next-Generation Technologies for Sustainability (ICINVENTS)*, Coimbatore, India: IEEE, 2025, pp. 1–9, November. doi: 10.1109/ICINVENTS64613.2025.11402224.

[41] V. Chaturvedi, "Modern Software Development with Java, Spring Boot, and Python: A Survey of Frameworks and Best Practices," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 188–197, December, 2023, doi: 10.56472/25832646/JETA-V3I8P121.

[42] S. Kumara, "A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395886.

[43] V. K. R. K. Koppireddy, "Passwordless Authentication: A Modern Approach to Secure Access," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 63, 2025.

[44] A. Joon, B. K. R. Janumpally, A. Gogineni, and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, HUBBALI, India: IEEE, 2025, pp. 1–8, September. doi: 10.1109/CONIT65521.2025.11167760.

[45] R. Palwe, "SAFIRE: Secure AI Framework for Institutional Readiness & Enablement," *Int. J. Comput. Artif. Intell.*, vol. 7, no. 4, pp. 136–139, 2026.

[46] M. S. Khan, M. Taufeeq, and M. Z. Khan, "Intelligent Resource Allocation in Cloud Computing Using Machine Learning," *GIS Sci. J.*, vol. 13, no. 04, pp. 226–237, 2026.

[47] Preethi, S. S. Bisht, D. Kundra, H. Kandhari, P. Singh, and H. Kaushik, "Enhancing multi-cloud security: novel method for big data storage," *Int. J. Syst. Assur. Eng. Manag.*, pp. 1–9, Jan. 2025, doi: 10.1007/s13198-024-02689-x.

[48] B. Yuan, G. Cao, J. Sun, and S. Zhou, "Optimising AI Workload Distribution in Multi-Cloud Environments : A Dynamic Resource Allocation Approach," *J. Ind. Eng. Appl. Sci.*, vol. 2, no. 5, pp. 68–79, 2024, doi: 10.5281/zenodo.13863194.

[49] A. M. Mostafa *et al.*, "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication," *Appl. Sci.*, vol. 13, no. 19, 2023, doi: 10.3390/app131910871.

[50] K. N. Vhatkar and G. P. Bhole, "Optimal container resource allocation in cloud architecture: A new hybrid model," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 5, pp. 1906–1918, May 2022, doi: 10.1016/j.jksuci.2019.10.009.

[51] V. T, "AI-Optimized Multi-Cloud Resource Management Architecture for Secure Banking and Network Environments," *Int. J. Res. Appl. Innov.*, vol. 5, no. 4, pp. 7368–7376, 2022, doi: 10.15662/IJRAI.2022.0504003.