IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

Survey of Resource Optimization and Security Techniques in Multi Cloud Computing Environments

Dr. Nilesh Jain
Associate Professor, Department of Computer Sciences and Applications
Mandsaur University, Mandsaur
nileshjainmca@gmail.com

Abstract: *Multi-cloud computing has evolved into a sophisticated model that enables organizations to leverage services from multiple cloud providers to enhance scalability, flexibility, reliability, and continuity. While the technology offers many benefits, there are numerous challenges related to resource optimization and security in heterogeneous cloud infrastructure, given its dynamic nature, diverse service models, varied pricing schemes, and increasing cyberattacks. A comprehensive overview of the resource optimization and security approaches in multi-cloud computing. First, it provides a brief discussion of the basics of multi-cloud computing and its architecture and deployment models. Then, it analyzes some of the most popular resource optimization approaches, which include resource allocation, workload scheduling, load balancing, dynamic resource provisioning, auto-scaling, virtual machine and container optimization, cost-aware optimization, energy-aware resource management, AI-driven optimization, and metaheuristic approaches. Moreover, it provides an overview of the popular security techniques, namely identity and access management, encryption, Zero Trust Architecture, intrusion detection and prevention systems, secure data replication, network security, blockchain-based security, and continuous monitoring. The study of recent literature on the topic brings out the issues, both pros and cons, involved in the area of resource optimization and security. The survey finds that the need of the hour is to incorporate resource optimization along with security measures into next-generation multi-cloud computing environments.*

Keywords: Multi-Cloud Computing, Resource Optimization, Cloud Security, Identity and Access Management, Zero Trust Architecture, Intrusion Detection System (IDS), Blockchain Security.

I. INTRODUCTION

Cloud computing is a technological innovation that provides configurable and on-demand computing resources through outsourced services. It enables organizations to access scalable, flexible, reliable, and cost-effective computing infrastructure with faster service deployment. Cloud service providers such as Microsoft Azure, Amazon Web Services (AWS), IBM Cloud, and Google Cloud Platform offer diverse computing, storage, and networking services to meet different organizational requirements[1][2]. The evolution of cloud computing has led to the adoption of multi-cloud computing, where organizations utilize services from multiple independent cloud providers to improve performance, reliability, cost efficiency, and business continuity. Different cloud platforms can be selected for specific applications, including data storage, document sharing, and data analytics, according to organizational needs[3].

Resource management in multi-cloud computing has traditionally relied on static allocation, heuristic-based, and rule-based approaches. Although these methods provide basic resource allocation, they often result in resource wastage, insufficient capacity during workload fluctuations, and limited adaptability to dynamic environments[4][5]. Cloud computing has seen an increase in the delivery of computing resources as a utility to meet cloud consumers' dynamically changing needs. Essentially, the purpose is to transfer responsibility for resource management and allocation to cloud providers, to create demand for computing resources, to reduce service launch time, and to eliminate the costs of establishing the infrastructure. Examples of cloud providers include Microsoft Windows Azure, IBM Cloud, Amazon Web Services and Google Apps. Indeed, the key characteristics that cloud computing systems exhibit include scalability, reliability, and flexibility [6][7].

The multi-cloud idea provides a creative way to integrate all their requirements into a single platform. Networks, servers, storage, apps, and services are just a few of the IT resources that can be conveniently shared under this paradigm. In multi-cloud computing, particular data is used to communicate across clouds[8]. Security concerns are the primary elements that regulate the expansion of the cloud computing service paradigm. Customers must be more cautious in recognizing the dangers of data breaches in this cloud environment since third-party management of sensitive data is dangerous [9][10]. As organizations increasingly adopt multi-cloud architectures to achieve greater scalability, reliability, and business continuity, the need for advanced resource optimization and security techniques has become more important than ever[11]. This survey reviews recent approaches for resource optimization and security in multi-cloud computing environments, highlighting current challenges, existing solutions, and future research directions.

1.1. Structure of the paper

The remainder of this paper is organized as follows: Section II presents the fundamentals of multi-cloud computing. Section III discusses resource optimization techniques, while Section IV describes security techniques. Section V reviews recent literature, and Section VI concludes the paper with future research directions.

II. Fundamentals of Multi-Cloud Computing

This computing concept involves the use of cloud computing services from two or more separate cloud service providers for deploying and managing applications. Multi-cloud computing facilitates organizations in utilizing the benefits offered by each of the clouds without being bound to any particular one and also helps achieve better availability of services. Multi-cloud computing enhances scalability, flexibility, and fault tolerance by allocating workloads across different clouds on the basis of performance, cost, and compliance criteria[12]. These types of systems typically use technologies like virtualization, containerization, Kubernetes, and cloud orchestration software to achieve better interoperability and resource management[13].

A. Multi-Cloud Architecture

Rather than depending on just one vendor, workloads are deployed across several public, private, or hybrid cloud infrastructures depending on the applications' needs, cost considerations, compliance factors, and performance goals. These clouds have been incorporated into the architecture using standard application programming interfaces (APIs), cloud orchestration solutions, containers, and management mechanisms for effective communication [14]. Key Components of Multi-Cloud Architecture:

- Cloud Service Providers (CSPs): Several CSPs (for instance, AWS, Azure, Google Cloud) provide computing, storage, networking, and platform services[15].
- Application Layer: Cloud-native applications, microservices, or enterprise workloads running in different clouds.
- Orchestration and Containerization: Technologies like Docker and Kubernetes allow workload portability and automation of deployments.
- Cloud Management Platform (CMP): This is used to monitor, provision, govern, and manage resources in the cloud.
- Networking Layer: Connectivity that is secure through use of virtual private network (VPNs), Software Defined Wide Area Network (SD-WAN), application programming interfaces (APIs), and inter-cloud networking.

- Data Management Layer: Responsible for data synchronization, replication, backup, migration, and consistency among various cloud platforms.
- Identity Management and Security: Consistent identity management and security through policies on authentication, authorization, encryption, and compliance.
- Monitoring and Automation: Monitoring and automation through observability, logging, infrastructure-as-code (IaC), and DevOps pipeline processes [16].

B. Types of Multi-Cloud Deployment Models

These models illustrate how organizations deploy applications, services, and data to multiple cloud providers in order to achieve particular business objectives, performance goals, security goals, and compliance goals. Choosing a suitable multi-cloud deployment model would be contingent upon parameters like the type of workload, availability, cost-effectiveness, and others [17]. The most popular multi-cloud deployment models are:

Public multi-cloud:

The services are availed from various cloud providers such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform[18]. Different applications are spread across these cloud providers to enhance performance, efficiency, and minimize vendor lock-in.

- Hybrid multi-cloud: A private cloud infrastructure combined with different public clouds. The applications that are considered confidential or critical are run on private clouds whereas other applications are deployed on public clouds.
- Distributed multi-cloud: The services and applications are distributed over different cloud providers at any one time. Applications are allocated to different providers based on considerations such as latency, resource availability, geographical location, and operational costs.
- Federated multi-cloud: This is a multi-cloud approach whereby the different cloud providers collaborate with each other via standard interfaces for interconnectivity purposes.
- Cloud-Native Multi-Cloud: Cloud-native multi-cloud uses cloud computing techniques including containers, microservices, Kubernetes, and DevOps methodologies to create applications capable of being launched and managed uniformly on more than one cloud provider. This technique increases portability, scalability, automation, and resilience of applications.
- Disaster Recovery Multi-Cloud: This type of cloud deployment ensures that critical applications and data are duplicated among more than one cloud provider to provide business continuity in case of an outage, cyberattack, or any other infrastructure failure.

III. RESOURCE OPTIMIZATION IN MULTI-CLOUD

Optimization in multi-cloud computing involves effective utilization, management, and deployment of computing resources, including VMs, containers, storage, networking, and processing power, among others, across various cloud providers[19]. Resource optimization aims to improve resource utilization while keeping operational expenses, energy use, and latency low, without affecting performance or quality of service (QoS) [20]. Unlike single-cloud computing, where resource optimization may not be needed, resource optimization in multi-cloud computing is necessitated by the heterogeneity of cloud platforms [13], differences in pricing, services provided by cloud providers, and the geographical locations of cloud providers' data centers, among other factors [21]. Techniques for resource optimization include workload scheduling, dynamic resource allocation, auto-scaling, virtualization, container orchestration, and AI-driven decision-making, among others. Major Resource Optimization Techniques as shown in Table I:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, July 2026 Impact Factor: 8.2

Table I: Summary of Resource Optimization Techniques in Multi Cloud Computing

Technique	Primary Objective	Technologies/Methods	Advantages	Limitations
Resource Allocation	Allocate computing resources according to workload demands	Virtual Machines (VMs), Containers, Resource Allocation Algorithms	Improves resource utilization and reduces wastage	Complex allocation in heterogeneous cloud environments
Workload Scheduling	Schedule tasks efficiently across multiple cloud providers	Task Scheduling Algorithms, Workflow Scheduling	Reduces execution time and improves throughput	Scheduling overhead increases with dynamic workloads
Load Balancing	Distribute workloads evenly among cloud resources	Dynamic Load Balancers, Traffic Distribution	Prevents resource overload and improves availability	May introduce communication latency
Dynamic Resource Provisioning	Allocate and release resources based on workload changes	Elastic Provisioning, Resource Monitoring	Improves scalability and avoids over/under-provisioning	Requires continuous monitoring and accurate demand prediction
Auto-Scaling	Automatically scale resources according to performance metrics	Horizontal Scaling, Vertical Scaling, Kubernetes Autoscaler	Maintains application performance while reducing costs	Incorrect scaling policies may waste resources
VM and Container Optimization	Optimize placement and migration of VMs and containers	Virtualization, Docker, Kubernetes	Enhances portability, scalability, and resource efficiency	Migration overhead and orchestration complexity

Advantages of Resource Optimization Techniques

- Overall efficiency of resource utilization in several cloud vendors[22].
- Cost savings for both infrastructural and operational purposes.
- Increased performance of applications and reduced response time.
- Dynamic load balancing and auto-scaling capabilities.
- Scalability and flexibility of the cloud services.
- Better Quality of Service (QoS) and SLA.
- Energy savings and lesser impact on environment.
- Fault tolerance and increased availability of services.
- Effective management of heterogeneous clouds.
- Intelligent decisions based on AI optimization.

IV. SECURITY TECHNIQUES IN MULTI-CLOUD COMPUTING

The security methods used in multi-cloud computing aim to protect applications, data, and services across multiple cloud service providers against cyberattacks, unauthorized access, and data breaches. This is because multi-cloud computing incorporates different infrastructures, various security policies, and shared responsibility among other factors. Therefore, ensuring security for the entire cloud service platform is quite challenging. The security methods emphasize protecting data confidentiality, integrity, and availability, while ensuring compliance with regulatory requirements and SLAs. Multi-cloud computing today uses several security methods, including encryption, identity and access management, zero trust architecture, artificial intelligence, and continuous monitoring [23]. Major Security Techniques in Multi-Cloud:

1) Identity and Access Management (IAM)

It manages user authentication and authorization from multiple cloud providers. This is done through:

- RBAC (Role-Based Access Control) - Grants users' access based on their assigned roles within an organization. It simplifies permission management and prevents unauthorized access to cloud resources.
- ABAC (Attribute-Based Access Control) – Provides access based on user, resource, and environmental attributes such as department, location, or time. It offers fine-grained and flexible access control in multi-cloud environments[24].

- MFA (Multi-Factor Authentication) – It enhances security by requiring users to verify their identity using two or more authentication factors, such as a password, biometric verification, or a one-time password (OTP). It significantly reduces the risk of unauthorized access.

It is used to ensure that all users, applications, and services accessing cloud resources have appropriate permissions.

2) Data Encryption

Data encryption is the process of transforming data into an unreadable form during storage and transfer to ensure confidentiality. Some of the data encryption technologies include:

- End-to-End Encryption (E2EE) – It protects data from the sender to the intended recipient, ensuring that only authorized parties can access the information during transmission.
- Attribute-Based Encryption (ABE) – It encrypts data based on user attributes or access policies, allowing only users with matching attributes to decrypt the data.
- Homomorphic Encryption (HME) – It enables computations to be performed directly on encrypted data without decrypting it, preserving data privacy during cloud processing.
- Key management - The secure generation, storage, distribution, rotation, and revocation of cryptographic keys to ensure the confidentiality and integrity of encrypted data across multi-cloud environments.

3) Zero Trust Security

Zero Trust Architecture (ZTA) uses the "Never Trust, Always Verify" policy. In ZTA, each user, application[25], and device will always be authenticated and authorized no matter their locations, either in the cloud environment or out of the cloud. This method helps in reducing insider threats and lateral movement[26].

4) Intrusion Detection and Prevention System (IDPS)

IDPS monitors cloud environments to detect cyberattacks[27], security violations, and suspicious behaviors. The IDPS uses some technologies including:

- Signature-based - Detects attacks by comparing network traffic with known attack signatures or patterns. It is highly effective against previously identified threats but cannot detect unknown attacks.
- Anomaly-based - Identifies intrusions by detecting deviations from normal system or network behavior. It can detect unknown and zero-day attacks but may generate false positives[28].
- AI/ML Based - Artificial intelligence and machine learning algorithms to analyze traffic patterns, identify anomalies, and detect cyber threats with higher accuracy and faster response times.

5) Secure Cloud-to-Cloud Data Replication and Backup

In case of important information, cloud providers replicate such data among themselves via secured means. This ensures the availability of the data, protection from ransomware attacks, hardware failures, etc.

6) Network Security

Network security is essential for providing safe communication between cloud platforms using firewalls, Virtual Private Networks (VPN), Software Defined Networking (SDN), API security and network segregation techniques [29][30].

7) Security Monitoring and Auditing

Organizations will be able to identify vulnerabilities and security incidents and act accordingly with the help of security monitoring and auditing. Security Information and Event Management (SIEM) solutions can provide visibility into various cloud environments.

8) Compliance and Governance

Compliance methodologies enable organizations to meet legal and regulatory compliance standards like GDPR, HIPAA, ISO/IEC 27001, and PCI DSS. Governance principles allow standardization of security measures, risk management, and auditing across several cloud providers[31].

9) Security Using Blockchain Technology

Blockchain technology provides trust and transparency and improves data integrity through immutable transaction records of cloud resources[32]. The smart contract enables automated access control, auditing, and secure sharing of information between various cloud providers.

4.1 Multi -Cloud Benefits

Resource optimization and security techniques significantly improve the efficiency, reliability, and protection of multi-cloud environments. These techniques enable organizations to maximize cloud resource utilization while maintaining strong security and regulatory compliance. Benefits are:

• Resource optimization ensures efficient utilization of computing, storage, and networking resources.
• Provisioning and auto-scaling help the applications manage variable loads effectively[33].
• Smartly distributing the loads helps minimize the response time and boost application performance.
• The multi-cloud environment helps minimize downtime due to redundancy and failover.
• Ensures continuous availability of services even during any failure.
• Encrypting, IAM, Zero Trust, and intrusion detection help protect from cyber-attacks.
• Minimizes the chances of unauthorized access and breach[34].
• Security measures and governance help organizations adhere to regulatory compliance.
• Improves trust and accountability in cloud operations[35].
• Artificial intelligence automates processes such as resource management, threat detection, and performance optimization.
• Improves efficiency and minimizes human intervention.
• Multiple clouds allow firms to allocate their resources among different cloud vendors. Minimizes dependency on one cloud vendor.[36]

4.2 Multi -Cloud Challenges

Resource optimization and security in multi-cloud environments face several technical and operational challenges due to the heterogeneous nature of cloud platforms, diverse service models, and distributed infrastructures. Efficient resource management and consistent security implementation require coordination across multiple cloud providers while maintaining performance, compliance, and cost efficiency. Challenges are:

• The heterogeneous architecture, API, and management systems used by various cloud service providers make interoperability complicated.
• Non-standardized environment makes resource allocation and security management complicated.
• Dynamic resource allocation across several clouds becomes difficult because of varying workloads and capabilities of providers.[37]
• Ineffective resource allocation may result in either under or over-allocation of resources.
• Various pricing structures at different cloud service providers make it hard for cost optimization.
• Poor workload allocation may lead to higher cost of operation[38].
• The security and privacy of the data stored in the cloud become complicated as it is stored in several cloud environments.
• An organization needs to be compliant with regulatory requirement like GDPR, HIPAA, and ISO/IEC 27001 across different cloud environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

- There can be communication latencies for cloud infrastructure that is geographically dispersed.
- Balancing workload optimization along with keeping latency low is hard.
- Security and performance monitoring for different cloud providers need constant monitoring.
- Real-time threat response is hard in a geographically dispersed environment.

V. LITERATURE REVIEW

The literature review summarizes recent advancements in multi-cloud resource optimization and security, while Table II compares the focus areas, techniques, key findings, limitations, and future research directions of existing studies. The analysis identifies current challenges and highlights the need for intelligent, scalable, and secure multi-cloud frameworks.

Gupta and Shelat, (2026), AI performing critical operations without human supervision and automated deployments introduce significant security challenges. Emerging AI-induced threats, such as model poisoning and AI-enhanced phishing attacks, further intensify cloud vulnerabilities. This review presents common cloud security threats, AI-induced threats, and various security techniques for cloud infrastructure. It also highlights recent research efforts to mitigate these threats and identifies future research directions for developing robust AI-aware cloud security frameworks[39].

Alqarni and Fei, (2026), presents a novel approach to secure data deletion by proposing a shredding-based approach, which breaks apart a file into two non-disclosing disjoint pieces, neither of which contains enough information to reveal the content of the original file. Each piece is stored in a different storage site in the multi-cloud environment. Unlike prior shredding approaches, this method allows for preserving the original file size to make it space-efficient. Evaluations show that the processing overhead is comparable to the original shredding method, while the storage overhead is almost cut to half [40].

Aydi, Nouri and Driss, (2025), proposes a novel approach that integrates the hill climbing algorithm which is a well-known Local Search technique in the Non dominated Sorting Genetic Algorithm II, called LS- NSGA-II to address these issues. In fact, the LS-NSGA- II is used to optimize task assignments across nodes, aiming to minimize execution time while maximizing task priority. Simultaneously, ensures an immutable, transparent, and auditable record of all scheduling decisions, validating each task assignment against resource constraints to enhance system reliability and security [41].

Alajroush, Latif and Saba, (2023), primary contribution is an examination of contemporary, serious trust challenges that arise in a multi-cloud context. And to conduct a survey comparing trust management frameworks for a multi-cloud environment to address the identified challenges. The suggested solution is to have a more robust and secure trust framework based on data compliance. By providing the flexibility, stability, and scalability that many organizations need from cloud computing, this reduces the need to set up a private cloud and deploy separate hardware resources. However, multi-cloud settings present several security and trust issues [42].

Zhao and Jiang, (2023), proposed algorithm optimizes these four parameters for each mobile device to allocate computing resources more rationally, minimize the total energy consumption, and ensure security during scheduling. When modeling computing resources, constraints on maximum energy consumption, computation cycles, storage, bandwidth, and delay are also considered. Compared to the other algorithms in the container cloud, the proposed particle swarm optimization algorithm optimized by hierarchical learning can get the optimal solution of resource scheduling satisfying the constraints faster, with lower energy consumption and higher security [43].

Wang et al., (2022), proposes an efficient, secure, and new data consistency verification scheme using blockchain technology. In order to reduce the computation and communication overhead in the verification process, the scheme uses encrypted tags to build a Merkle hash tree to generate unique and lightweight verification proofs and does not use third-party auditors [44].

Table II: Summary of Related Work in Multi-Cloud Resource Optimization and Security

Authors	Focus Area	Technologies/Techniques	Key Findings	Limitations	Future Work
Gupta and Shelat (2026)	AI-aware cloud security	AI threat analysis, cloud security frameworks	Identified AI-induced threats and reviewed mitigation techniques for cloud environments.	Lacks unified AI-driven security architecture with real-time threat response.	Develop adaptive AI-aware cloud security frameworks with automated defense mechanisms.
Alqarni and Fei (2026)	Secure data deletion	Shredding-based secure storage in multi-cloud	Proposed space-efficient secure data deletion by splitting files across multiple clouds.	Does not address dynamic cloud environments and large-scale deployments.	Improve scalability and integrate intelligent key management for secure storage.
Aydi, Nouri and Driss (2025)	Resource scheduling and security	LS-NSGA-II, Hill Climbing, Blockchain	Optimized task scheduling while ensuring transparency, reliability, and security.	Higher computational complexity and limited validation in heterogeneous environments.	Design lightweight optimization methods for large-scale multi-cloud systems.
Alajroush, Latif and Saba (2023)	Trust management	Trust management frameworks, compliance-based security	Reviewed trust challenges and proposed secure trust frameworks for multi-cloud environments.	Limited implementation and absence of dynamic trust evaluation mechanisms.	Develop intelligent and adaptive trust management models for evolving cloud infrastructures.
Zhao and Jiang (2023)	Resource optimization	Hierarchical Learning-based Particle Swarm Optimization (PSO)	Improved resource scheduling with reduced energy consumption and enhanced security.	Focused mainly on optimization without comprehensive security integration.	Integrate AI-driven security mechanisms with energy-efficient resource allocation.
Wang et al. (2022)	Data integrity verification	Blockchain, Merkle Hash Tree, encrypted tags	Proposed lightweight blockchain-based verification without third-party auditors.	Scalability and latency issues remain in large distributed cloud systems.	Develop scalable blockchain verification schemes with reduced communication overhead.

VI. CONCLUSION AND FUTURE WORK

Multi-cloud computing has emerged as an effective solution for delivering scalable, reliable, flexible, and cost-efficient computing services while reducing vendor dependency and improving business continuity. However, the increasing complexity of distributed cloud environments has made efficient resource optimization and robust security mechanisms essential for maintaining system performance and protecting sensitive information. This survey reviewed the fundamental concepts of multi-cloud computing, resource optimization techniques, and advanced security approaches adopted in heterogeneous cloud environments. The literature analysis demonstrated that intelligent optimization algorithms, AI-driven techniques, blockchain, Zero Trust Architecture, and modern identity management mechanisms substantially improve resource utilization, operational efficiency, cyber resilience, and regulatory compliance. Despite these advancements, challenges related to interoperability, workload management, latency, trust, and consistent security enforcement continue to exist. Overall, integrating intelligent resource optimization with comprehensive security strategies is fundamental to building efficient, scalable, resilient, and sustainable multi-cloud computing environments.

Future research should emphasize intelligent and autonomous multi-cloud management frameworks that integrate AI-driven resource optimization with adaptive security mechanisms. Further investigation into lightweight blockchain solutions, explainable AI, energy-efficient scheduling, Zero Trust architectures, intelligent orchestration, and real-time threat detection can improve scalability, interoperability, resilience, and secure multi-cloud operations.

REFERENCES

[1] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," J. Comput. Inf. Syst., vol. 66, no. 1, pp. 123–150, Jan. 2026, doi: 10.1080/08874417.2024.2329985.

[2] 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.

[3] K. Alang, "AI-Powered Multi-cloud and Hybrid Cloud Strategies," in Revolutionizing the Cloud: Generative AI, Security, and Sustainability, Springer, 2026, pp. 107–125.

[4] A. Paul, "Optimizing Resource Management in Multi-Cloud Computing Environments Using Reinforcement Learning Approaches," 2025.

[5] J. E. Kofi, "Data-Driven Cloud Workload Optimization Using Machine Learning Modeling for Proactive Resource Management," Int. J. Artif. Intell. Data Sci. Mach. Learn., vol. 6, no. 4, 2025, doi: 10.63282/3050-922X.IJERET-V6I4P104.

[6] B. Aldawsari, T. Baker, M. Asim, Z. Maamar, D. Al-Jumeily Obe, and M. Alkhafajiy, "A Survey of Resource Management Challenges in Multi-cloud Environment: Taxonomy and Empirical Analysis," Azerbaijan J. High Perform. Comput., vol. 1, pp. 51–65, 2018, doi: 10.32010/26166127.2018.1.1.51.65.

[7] C. A. Raju Dandigam, "Comparative Study of Machine Learning Algorithms for Predictive Analytics in Web Applications," in 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), Cairo, Egypt: IEEE, 2026, pp. 1–6, April. doi: 10.1109/ICAISET66439.2026.11542167.

[8] S. Singh, "Advancing Wireless Communications with Open Radio Access Network," in 2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI), Tirunelveli, India: IEEE, Jul. 2025, pp. 682–687. doi: 10.1109/ICDICI66477.2025.11135206.

[9] R. Bishukarma, "Optimising Cloud Security in Multi-Cloud Environments : A Study of Best Practices," Int. Res. J., vol. 11, no. 11, pp. 590–598, 2024.

[10] H. N. Dholariya, "Human-in-the-Loop AI for Cloud Data Engineering: The Collaborative Intelligence Architecture (CIRA) for Regulated Industries," J. Inf. Syst. Eng. Manag., vol. 11, no. 1s, pp. 883–898, Jan, 2026.

[11] S. Ali et al., "Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions," Comput. Secur., vol. 157, p. 104599, Oct. 2025, doi: 10.1016/j.cose.2025.104599.

[12] J. Alonso et al., "Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review," J. Cloud Comput., vol. 12, 2023, doi: 10.1186/s13677-022-00367-6.

[13] P. Naayini and S. Kamatala, "Automating Infrastructure Platforms with Cloud, Kubernetes, and Site Reliability Engineering," Int. J. Comput. Tech., vol. 8, no. 6, pp. 1–9, November, 2021.

[14] S. Arora and J. Hastings, "Microsegmented Cloud Network Architecture Using Open-Source Tools for a Zero Trust Foundation," in 2024 17th International Conference on Security of Information and Networks (SIN), IEEE, Dec. 2024, pp. 1–8. doi: 10.1109/SIN63213.2024.10871361.

[15] T. Shah, "Cloud-Based Data Warehousing for Marketing Agility: Lessons from FinTech Migrations to Snowflake and AWS," Int. J. Adv. Res. Sci. Commun. Technol., vol. 4, no. 4, March, pp. 642–652, 2024, doi: 10.48175/IJARSCT-16000B.

[16] N. M. Hamdan, N. Admodisastro, H. Bin Osman, and M. S. Bin Muhammad, "Semantic Interoperability in Multi-Cloud Platforms: A Reference Architecture Utilizing an Ontology-Based Approach," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 14, no. 6, pp. 1967–1975, Dec. 2024, doi: 10.18517/ijaseit.14.6.19861.

[17] D. Gallagher and R. G. Lennon, "Architecting Multi-Cloud Applications for High Availability using DevOps," in 2022 IEEE International Conference on e-Business Engineering (ICEBE), IEEE, Oct. 2022, pp. 112–118. doi: 10.1109/ICEBE55470.2022.00028.

[18] L. Savu, "Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges," in 2011 International Conference on Computer and Management (CAMAN), IEEE, May 2011, pp. 1–4. doi: 10.1109/CAMAN.2011.5778816.
[19] J. B. Mehta, "Autonomous Workload Right-Sizing for Multi-Cloud Cost Optimization," in 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), Cairo, Egypt: IEEE, 2026, pp. 1–11, June. doi: 10.1109/ICAISET66439.2026.11541899.
[20] M. Habibi and N. Jafari, "Multi-Objective Task Scheduling in Cloud Computing Using an Imperialist Competitive Algorithm," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 5, 2016, doi: 10.14569/IJACSA.2016.070540.
[21] S. S. Sefati, M. Keymasi, R. Craciunescu, S. Maiduc, M. Bayram, and B. Arasteh, "Adaptive Resource Scheduling in Multi-Cloud Computing Using Recurrent Neural Forecasting and Memory-Based Metaheuristic Optimization," J. Grid Comput., vol. 23, no. 4, p. 26, Dec. 2025, doi: 10.1007/s10723-025-09812-7.
[22] Y. Wang and X. Yang, "Intelligent Resource Allocation Optimization for Cloud Computing via Machine Learning," 2025. doi: 10.13140/RG.2.2.26564.74886.
[23] R. Dilworth, "Advancements and Challenges in Cloud Computing: Multi-Cloud Management, Security, and AI-Driven Threat Mitigation," in Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference, New York, NY, USA: ACM, Dec. 2024, pp. 639–645. doi: 10.1145/3719384.3719476.
[24] 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.
[25] O. Bonnet, "SCALABLE ZERO-TRUST DEPLOYMENT STRATEGIES FOR HETEROGENEOUS CLOUD ECOSYSTEMS," 2023.
[26] V. Sharma, "Zero Trust Architecture for 5G Networks," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 12, no. 6, Nov. 2024, doi: 10.37082/IJIRMPS.v12.i6.232707.
[27] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in 2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Mohali, Punjab, India: IEEE, 2025, pp. 1–6, December. doi: https://doi.org/10.1109/ISAECT68904.2025.11318752.
[28] J. B. Mehta, "AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS," Int. J. Appl. Math., vol. 38, no. 4s, pp. 1270–1285, August, 2025, doi: https://doi.org/10.12732/ijam.v38i4s.685.
[29] H. Patel, "Cloud Security Reinforcement: AI-Based DSPM and Machine Learning Anomaly Detection," 2021. doi: 10.13140/RG.2.2.10779.17446.
[30] H. P. C. Shiva Kumara, "Deep Learning-Based Intrusion Detection and Cybersecurity Framework for Connected Vehicle CAN Bus Communication Networks," in 2026 14th International Symposium on Digital Forensics and Security (ISDFS), Boston, MA, USA: IEEE, 2026, pp. 1–6, March. doi: 10.1109/ISDFS69419.2026.11459074.
[31] J. W. S. Narendra Kumar Reddy Choppa, "Towards Human-in-the-Loop Orchestration of Agentic SAP Ecosystems : Governance , Cognitive Impact , and Control Tower Design," J. Inf. Syst. Eng. Manag., vol. 10, no. 59, pp. 274-286,Augest, 2025.
[32] H. Rehan, "Zero-Trust Architecture for Securing Multi-Cloud Environments," vol. 2, pp. 236–273, 2022.
[33] F. S. Prity, M. H. Gazi, and K. M. A. Uddin, "A review of task scheduling in cloud computing based on nature-inspired optimization algorithm," Cluster Comput., vol. 26, no. 5, pp. 3037–3067, Oct. 2023, doi: 10.1007/s10586-023-04090-y.
[34] S. Iqbal and A. Heng, "AI-Driven Resource Management in Cloud Computing: Leveraging Machine Learning, IoT Devices, and Edge-to-Cloud Intelligence," 2023. doi: 10.13140/RG.2.2.28383.27049.
[35] J. E. Kofi, "Monitoring Cloud Performance Metrics Utilizing AI to Estimate the Efficiency of Cloud Operations," in 2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), IEEE,

2025, pp. 1–6, December. [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=uTB60gEAAAAJ&citation_for_view=uTB60gEAAAAJ:Y0pCki6q_DkC

[36] D. C. Diningrat, Suhardi, and B. Rahardjo, "Security Issues in Multi-Cloud: A Systematic Literature Review," IEEE Access, vol. 13, pp. 70006–70017, 2025, doi: 10.1109/ACCESS.2025.3561352.

[37] N. M. Hamdan and N. Admodisastro, "Towards a Reference Architecture for Semantic Interoperability in Multi-Cloud Platforms," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 12, 2023, doi: 10.14569/IJACSA.2023.0141254.

[38] J. A. Mahatme and M. R. Satpute, "A Comprehensive Review on Cloud Computing: Challenges, Architectures, and Future Directions," IARJSET, vol. 12, no. 7, Jul. 2025, doi: 10.17148/IARJSET.2025.12736.

[39] K. Gupta and S. Shelat, "AI-Driven Security Challenges in Cloud Computing: A Review of Emerging Threats and Security Solutions," in 2026 3rd International Conference on Advancements and Key Challenges in Green Energy and Computing (AKGEC), IEEE, Feb. 2026, pp. 1–7. doi: 10.1109/AKGEC68790.2026.11485800.

[40] A. K. Alqarni and Z. Fei, "A Space-Efficient Shredding-Based Method for Secure Data Deletion in Multi-Cloud Environments," in 2026 International Conference on Computing, Networking and Communications (ICNC), IEEE, Feb. 2026, pp. 655–659. doi: 10.1109/ICNC68183.2026.11416886.

[41] M. Aydi, H. E. Nouri, and O. B. Driss, "Multi-Objective Task Scheduling in Fog-Cloud Environments: LS-NSGA-II Optimization and Blockchain Integration for Enhanced Security and Efficiency," in 2025 13th International Symposium on Digital Forensics and Security (ISDFS), IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ISDFS65363.2025.11012016.

[42] A. Alajroush, R. Latif, and T. Saba, "Trust Management Frameworks In Multi-Cloud Environment: A Review," in 2023 Sixth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), IEEE, Mar. 2023, pp. 117–120. doi: 10.1109/WiDS-PSU57071.2023.00034.

[43] Y. Zhao and T. Jiang, "Edge Computing Power Optimization Method in Container Cloud Environment," in 2023 3rd International Conference on Electronic Information Engineering and Computer Science (EIECS), IEEE, Sep. 2023, pp. 372–377. doi: 10.1109/EIECS59936.2023.10435532.

[44] F. Wang, J. Zhou, H. Wang, and X. Guo, "A Blockchain-Based Multi-Cloud Storage Data Consistency Verification Scheme," in 2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), IEEE, Dec. 2022, pp. 371–377. doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00054.