



# Cloud Computing: Security, Resource Optimization, and Algorithm Evaluation

## Computación en la Nube: Seguridad, Optimización de Recursos y Evaluación de Algoritmos

Nidia Jael Muñoz Oviedo<sup>1</sup> 

<sup>1</sup> Universidad de Nariño, 520002 Pasto, Colombia.

Submitted: 02-07-2026 | Revised: 07-09-2026 | Accepted: 12-10-2026 | Published: 13-10-2026

### ABSTRACT

Cloud computing is a key component of modern digital infrastructure; however, its adoption faces challenges related to operational efficiency and security. This systematic review analyzes the convergence of data protection, resource optimization, and algorithm evaluation in distributed environments. Methodologically, it examines metrics and approaches used to validate algorithmic performance and ensure efficient service delivery. The findings highlight the effectiveness of metaheuristic and hybrid algorithms for task scheduling, as well as virtual machine consolidation techniques that improve hardware utilization and reduce energy consumption. Persistent risks are also identified, such as DDoS attacks and vulnerabilities in multi-tenant architectures, for which solutions based on blockchain, federated learning, and homomorphic encryption are emerging. This synthesis provides a classification of adaptive strategies to enhance security and efficiency in cloud computing, serving as a reference for the development of more resilient, transparent, and sustainable ecosystems.

Keywords: Cloud Computing, Resource Optimization, Algorithm Evaluation, Cloud Security, System Performance.

### RESUMEN

La computación en la nube es clave en la infraestructura digital actual, pero su adopción enfrenta retos en eficiencia operativa y seguridad. Esta revisión sistemática analiza la convergencia entre protección de datos, optimización de recursos y evaluación de algoritmos en entornos distribuidos. Metodológicamente, examina métricas y enfoques para validar el desempeño algorítmico y garantizar servicios eficientes. Los hallazgos destacan la eficacia de algoritmos metaheurísticos e híbridos para la programación de tareas, así como técnicas de consolidación de máquinas virtuales que mejoran el uso del hardware y reducen el consumo energético. También se identifican riesgos persistentes, como ataques DDoS y vulnerabilidades en arquitecturas multi-inquilino, frente a los cuales surgen soluciones basadas en blockchain, aprendizaje federado y cifrado homomórfico. Esta síntesis aporta una clasificación de estrategias adaptativas para mejorar la seguridad y eficiencia en la nube, sirviendo como referencia para desarrollar ecosistemas más resilientes, transparentes y sostenibles.

Palabras clave: Computación en la Nube, Optimización de Recursos, Evaluación de Algoritmos, Seguridad en la Nube, Rendimiento del Sistema.

## INTRODUCTION

La computación en la nube se define fundamentalmente como un modelo que proporciona acceso bajo demanda a un conjunto compartido de recursos de computación, como aplicaciones, plataformas e infraestructura, los cuales están alojados en centros de datos remotos y pueden ser asignados o liberados dinámicamente por los proveedores para maximizar su disponibilidad. Esta tecnología se describe académicamente como un esquema que permite un acceso fácil y generalizado a un grupo compartido de recursos informáticos personalizables, incluyendo redes, servidores, almacenamiento y servicios, que pueden ser aprovisionados y liberados rápidamente con un esfuerzo de gestión o interacción con el proveedor mínimo[1].

For the development of this systematic literature review, a rigorous search and selection process was conducted across five recognized academic sources: DOAJ, IEEE Xplore, ResearchRabbit, Redalyc, and Scopus. From these databases, a total of 120 scientific articles were collected and subjected to previously defined inclusion and exclusion criteria. The search strategy was structured using keywords related to cloud computing, security, resource optimization, algorithm evaluation, and service performance. Subsequently, filtering was performed based on thematic relevance, methodological quality, and the capacity of the studies to directly answer the six research questions posed, thereby ensuring a solid and representative basis for the analysis.

The research process was developed through an iterative analysis of the selected literature, allowing the identification of patterns, trends, and knowledge gaps around the thematic axes of the study. From this analysis, six research questions emerged that guide the work, related to the evaluation of algorithmic performance, security and privacy strategies, performance optimization, the use of metaheuristic algorithms, virtual machine consolidation, and cloud security challenges. The evidence synthesis was based on criteria of relevance, empirical consistency, and technical applicability, which allowed the integration of results from diverse methodological approaches. As a result, key metrics for performance evaluation, advanced resource allocation models, robust data protection strategies, and a growing use of metaheuristic techniques for the optimization of distributed systems were identified.

This article is organized around the six thematic axes derived from the research questions. First, the evaluation of algorithm performance in cloud environments is addressed, analyzing the factors, metrics, and methodologies employed. Subsequently, the tools and strategies aimed at ensuring data integrity, privacy, and transparency are examined. Next, the strategies and metrics necessary to ensure optimal performance levels in cloud services are studied. Following this, an analysis of the metaheuristic algorithms used in the optimization of task scheduling and allocation is presented. Later sections examine in depth virtual machine consolidation techniques for resource optimization in data centers. Finally, the main security challenges facing cloud infrastructure are discussed, providing a comprehensive view that integrates the technical, operational, and strategic aspects of this domain.

## Methods

This systematic literature review was conducted using a structured methodological approach aimed at identifying, selecting, and analyzing relevant studies in the field of cloud computing. The objective was to consolidate scientific evidence related to security, resource optimization, algorithm evaluation, and service performance in distributed environments.

The process began with the definition of the research questions, which guided the search strategy and thematic delimitation. Subsequently, information was collected from 5 academic databases: DOAJ, IEEE Xplore, ResearchRabbit, Redalyc, and Scopus, yielding a total of 120 articles. These were filtered using inclusion and exclusion criteria based on relevance, methodological quality, and correspondence with the study's axes[2].

Finally, the selected articles were analyzed through qualitative synthesis, enabling the identification of significant trends, approaches, and contributions.

## Research Questions

This study aims to present the results of a systematic review of the scientific literature on cloud computing, with emphasis on security, resource optimization, algorithm evaluation, and service performance. To construct the state of the art, the following research questions were formulated:

**Table 1. Definition of general concepts using PIPOH.**

| Criterion     | Description                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------|
| Population    | Cloud computing systems and environments                                                                                    |
| Intervention  | Algorithm evaluation, resource optimization, security strategies, and cloud management techniques                           |
| Results       | Scientific publications that address performance metrics, security, energy efficiency, and resource allocation in the cloud |
| Professionals | Researchers and professionals in Computer Science and Information Technologies                                              |
| Context       | Academic and technological environments related to cloud computing                                                          |

Source: Own elaboration.

- RQ1: What metrics and approaches make it possible to ensure optimal performance levels in cloud computing services?
- RQ2: What factors and methodologies are used to evaluate algorithm performance in cloud computing environments?
- RQ3: What tools and strategies are used to ensure the integrity, privacy, and transparency of data in the cloud?
- RQ4: What metaheuristic algorithms have been proposed to optimize task scheduling and allocation in cloud environments?
- RQ5: What virtual machine consolidation techniques are used to improve resource utilization in cloud data centers?
- RQ6: What are the main security challenges in cloud computing infrastructure?

These questions were formulated based on a preliminary analysis of the literature and structured under a systematic approach that made it possible to delimit the scope of the study and guide the process of searching, selecting, and analyzing the information.

## Search

The proposed search strategy consisted of exploring general terms in specialized databases. In the selected databases, search terms combined with synonyms were applied to cover a greater number of documents to be evaluated. Table 2 presents the terms with their respective synonyms and additional filters.

The search process was conducted in the databases mentioned in Table 3, using fields such as title, keywords, abstract, and full document. Table 4 presents the resulting search string for the main term, together with its synonyms and corresponding filters.

It should be noted that the search was limited to 2021 onward, since this period concentrates the most recent and relevant academic and scientific contributions on cloud computing, particularly regarding security, resource optimization, and algorithm evaluation in distributed environments, areas that have experienced significant growth in scientific production validated by the international research community.

**Table 2. Term, synonyms, and filters for composing the search string**

| Term            | Synonyms                          | Additional filters                   |
|-----------------|-----------------------------------|--------------------------------------|
| Cloud computing | Cloud computing performance       | Security                             |
|                 | Cloud resource management         |                                      |
|                 | Cloud security strategies         | Algorithm evaluation                 |
|                 | Cloud algorithm evaluation        |                                      |
|                 | Virtual machine consolidation     | Software Year of publication >= 2021 |
|                 | Metaheuristic scheduling in cloud |                                      |

Source: own elaboration.

**Table 3. Main term and database.**

| Term            | Database       |
|-----------------|----------------|
| Cloud computing | DOAJ           |
|                 | IEEE Xplore    |
|                 | ResearchRabbit |
|                 | Redalyc        |
|                 | Scopus         |

Source: own elaboration.

**Table 4. Search string.**

| Term            | Synonyms                                                                                                                                                                                                                                                                                                                                    |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud computing | ("Cloud computing" OR "Cloud computing performance" OR "Cloud resource management" OR "Cloud security strategies" OR "Cloud algorithm evaluation" OR "Virtual machine consolidation" OR "Metaheuristic scheduling in cloud") AND (Security OR "Algorithm evaluation" OR "Resource optimization" OR Software) AND (publication year >= 2021) |

Source: own elaboration.

## Selection

All studies included in this review were analyzed; during their evaluation, the following items were considered: title, keywords, abstract, introduction, background, state of the art, methodology, results, and conclusions. Likewise, inclusion and exclusion criteria were defined to guide the review.

The inclusion criterion defined is: a scientific document related to studies on security, resource optimization, algorithm evaluation, and service performance in cloud computing environments, or their search synonyms. The exclusion criteria defined are: studies that do not have their corresponding bibliographic citation, documents that do not contain the search terms or synonyms, works that do not directly address cloud computing environments, and documents that are not available for full download.

**Table 5. Dates of consultation and file download.**

| Database       | Search date |
|----------------|-------------|
| DOAJ           | 27/02/2026  |
| IEEE Xplore    | 28/02/2026  |
| ResearchRabbit | 01/03/2026  |
| Redalyc        | 01/03/2026  |
| Scopus         | 01/04/2026  |

Source: own elaboration.

## Quality assessment

In the quality assessment process for the selected documents, 7 criteria were considered: provenance of the sources, relevance of the content, impact of the study, objective of the research, context of the study, objectivity of the methodological design, and scientific rigor in data analysis. These 7 criteria correspond to 3 fundamental elements of quality management: planning, organization, and control.

The selection of primary sources was carried out in 5 stages, corresponding to the 5 specialized databases consulted, each with 3 phases: phase 1, elimination of duplicate articles; phase 2, elimination of non-downloadable articles; and phase 3, application of the inclusion and exclusion criteria. Because this systematic review used 5 databases with their respective synonyms and filters—in each of which the 3 aforementioned phases were applied—it was necessary to conduct the searches on different dates, as shown in Table 5.

As a result of the search process in the databases, a total of 120 studies were found; after applying the inclusion and exclusion criteria, a total of 68 relevant documents were obtained, which constitute the corpus of analysis for this systematic literature review.

**Table 6. Quality assessment in search and selection processes.**

| Main term       | Search result | Duplicate files | Excluded files | Relevant files | Database       |
|-----------------|---------------|-----------------|----------------|----------------|----------------|
| Cloud computing | 48            | 11              | 19             | 18             | DOAJ           |
|                 | 27            | 3               | 13             | 11             | IEEE Xplore    |
|                 | 8             | 0               | 1              | 7              | ResearchRabbit |
|                 | 23            | 1               | 8              | 14             | Redalyc        |
|                 | 14            | 0               | 0              | 18             | Scopus         |

Source: own elaboration.

**Table 7. Studies included in the systematic review.**

| Year | Quantity | Referencias                                                                                                               |
|------|----------|---------------------------------------------------------------------------------------------------------------------------|
| 2021 | 7        | [8] [20] [32] [33] [34] [38] [68]                                                                                         |
| 2022 | 6        | [4] [31] [35] [49] [56] [65]                                                                                              |
| 2023 | 5        | [11] [12] [19] [31] [53]                                                                                                  |
| 2024 | 9        | [27] [28] [39] [42] [54] [55] [64] [66] [71]                                                                              |
| 2025 | 27       | [5] [6] [7] [13] [14] [15] [16] [22] [23] [25] [26] [30] [37] [40] [41] [43] [44] [45] [48] [52] [58] [59] [60] [61] [67] |
| 2026 | 14       | [9] [10] [17] [18] [21] [24] [29] [36] [47] [50] [51] [57] [63] [70]                                                      |

Source: own elaboration.

## RESULTS

Strategies and metrics required to ensure that cloud services meet optimal performance levels

The evaluation and selection of cloud services requires identifying critical metrics that encompass technical performance, response time, availability, SLA compliance, and costs, classified by criticality and functional or non-functional nature [4]. Optimal performance is quantified through makespan, throughput, and efficiency in the use of physical resources [5]. Ensuring optimal levels requires evaluating the reliability of algorithms, CPU, RAM, and network usage, as well as response time, following ISO/IEC 25023 [6]. Organizational adoption should be guided by ISO/IEC 25010, considering availability, responsiveness, and reliability [7].

From an operational perspective, for low-latency applications, tail latency is a more accurate metric than the average, making it essential to monitor CPU and interference among virtual machines to identify microarchitectural bottlenecks that compromise SLAs [8]. The implementation of deadline-aware scheduling algorithms minimizes waiting times and ensures balanced load distribution among VMs, thereby reducing SLA violations [9]. Regression models for predicting CPU demand enable more robust VM consolidation that optimizes energy efficiency and maintains performance within contracted limits [10]. The literature identifies VM consolidation as an essential strategy and measures its performance through energy consumption, SLA violations, migrations, and associated degradation [11].

Resource allocation strategies must address demand uncertainty through quantitative models that link accesses to hardware consumption, achieving high utilization rates without compromising stability [12]. Ensuring optimal performance in container clouds requires multi-objective optimization models that balance utilization, load balancing, fragmentation, energy consumption, and SLA compliance [13]. VM placement using hybrid algorithms maximizes CPU, RAM, and storage utilization while reducing energy consumption [14]. Adaptive adjustment strategies (ARAA) in Kubernetes optimize energy performance by tracking CPU, memory, and execution time metrics in real time [15].

Workflow scheduling algorithms must minimize makespan, cost, and energy consumption while simultaneously achieving maximum resource utilization [16].

Babayigit et al.[17] evaluate TLBO, PSO, and GA for resource management, focusing their analysis on the cost-time tradeoff and highlighting scalability and convergence as critical metrics. The DALRS system, a hybrid scheduler combining reinforcement learning and genetic algorithms, proposes comprehensive metrics: resource utilization, makespan, latency, energy consumption, and SLA compliance rate[18].

EDLB algorithms minimize execution times by evaluating makespan, resource utilization, and percentage of balance among nodes [19], whereas hybrid algorithms for heterogeneous environments require continuous monitoring of completion time, energy consumption, and computational cost [20]. FireBat combines Firefly and BAT to optimize task mapping, using DOI, makespan, and load fairness as key indicators [21]. GLOPS employs LSTM and linear regression together with metaheuristics for informed assignments, focusing on turnaround time, waiting time, and response time [22]. For fault tolerance, hybrid frameworks with fuzzy logic prioritize critical tasks by evaluating reliability, energy consumption, makespan, and success rate within deadlines [23]. The HGHHC algorithm establishes makespan and resource utilization as success metrics in heterogeneous environments [24].

The integration of LLMs and deep reinforcement learning optimizes performance by controlling average response time, QoS-based task success rate, and operational cost [25]. Persuasive autoscaling guarantees service quality by optimizing the resource allocation rate and reducing delays and failures [26]. Deep learning models for container scheduling (FoRES) quantify success through the container success rate (CSR), resource efficiency, and reduction in node overloads [27]. Knowledge graphs with convolutional neural networks mitigate operational delay and balance load by using load rate, scheduling speed, and energy consumption [28].

In serverless environments, performance is ensured through cold start latency reduction, container reuse, and instance prewarming [29]. Microservices architectures focus their optimization on containerization and dynamic load balancing, evaluating throughput, latency, recovery time, and CPU and memory usage [30]. Dynamic programming strategies under time constraints are validated by workflow success rate, cost ratio, and makespan [31]. Finally, reliability verification through analytic hierarchy uses QPS and technical CPU and memory performance as fundamental indicators [32].

## **Factors and methodologies for evaluating the performance of algorithms in cloud computing environments**

The performance of cloud algorithms is evaluated through multidimensional analysis that integrates makespan, throughput, resource utilization, energy expenditure, and load distribution balance[5]. The predominant factors span economic dimensions (cost, profit), operational dimensions (waiting time, failure rate, makespan), and environmental dimensions (carbon emissions, energy consumption)[33]. Single-parameter evaluation is ineffective; integrating completion time, energy consumption, resource utilization, and computational simulation cost simultaneously has been proposed[20]. For load balancing, temporal efficiency (total and average makespan), processing speed, and distribution effectiveness are measured[19]. Consolidation evaluation is based on energy consumption, SLA violations, VM migration count, and performance degradation[11].

Performance evaluation is frequently conducted through comparative analyses with state-of-the-art algorithms using QoS parameters, turnaround time, response time, and statistical tests to confirm the significance of the results[34]. For failure-prone environments, simulators such as iFogSim and paired t-tests are used to validate improvements against baselines[23]. The performance improvement rate (PIR) quantitatively compares new proposals with the state of the art, complemented by p-value analysis on NASA, HPC2N, and synthetic datasets[24].

In security, algorithms are evaluated with Silhouette and Davies-Bouldin indices, using bootstrap to derive 95% confidence intervals on precision and macro F1[35]. CloudSim Plus simulates distributed infrastructures by measuring utilization, makespan, average latency, and SLA compliance with multiple runs with random seeds[18]. Predictive model validation uses Google Cluster traces with RMSE, F1, and AUC metrics to ensure reliability in fault detection[36]. Load prediction evaluation combines predictive accuracy (MAE, MSE) with deployment efficiency measured by complexity and inference time[37]. Experimental methodologies compare algorithms against baseline scenarios and optimal theoretical limits, focusing on energy savings, number of VM migrations, and SLA compliance[10].

A rigorous performance evaluation requires profiling tools such as Linux Perf or Intel VTune

to identify microarchitectural bottlenecks, prioritizing queue latency and throughput in cloud environments[8]. Performance is comprehensively evaluated through algorithm reliability, monitoring of CPU, RAM, storage, and network traffic, and measurement of real-time response time[6]. Comprehensive system evaluation requires resource monitoring tools and benchmarks to standardize elasticity, latency, and performance tests[38]. Algorithms in container environments are evaluated with multi-objective analysis considering resource waste, load balancing, fragmentation, energy consumption, and convergence time with SLA compliance[13].

VM placement algorithms are measured by total energy consumption and resource utilization rate integrated into a fitness function (fitness score)[14]. Load balancing performance is quantified through the degree of imbalance (DOI) and Jain's fairness index in simulated infrastructures with heterogeneous capacities[21]. The comparison of TLBO, PSO, and GA evaluates cost-time balance, convergence speed, and scalability under increasing tasks[17].

Privacy-oriented evaluation uses a dual index: model accuracy and encryption cost, along with load latency and aggregation time[39]. Normative frameworks such as ISO/IEC 25010 analyze availability, reliability, and security, in addition to provider responsiveness[7]. Methodologies for rating services identify functional and non-functional KPIs, complemented by the CRITIC method to weight factors and Vikor to establish rankings[4]. For auto-scaling systems, metrics of allocation waiting time, service delay, and provisioning failures are prioritized[26]. Cloud performance analysis is mainly conducted through experiments, surveys, case studies, and literature reviews to ensure empirical validity[40].

### **Tools and strategies to ensure the integrity, privacy, and transparency of data in cloud environments**

A comprehensive strategy in edge-cloud environments involves container hardening through digital signature verification and a SIEM system for real-time monitoring, ensuring that only authorized images process confidential data[41]. Federated learning guarantees privacy by keeping data local and sharing only model parameters through encrypted channels (VPN/TLS) and virtual private clouds (VPC), reducing the attack surface[42]. In serverless computing, integrity and privacy are ensured with encryption at rest and in transit, cryptographic signatures for event authentication, the principle of least privilege in IAM, and strict runtime isolation[29].

Transparency in the face of possible corruption requires combining encryption technologies with robust authentication mechanisms to verify the authorship of information[4]. Blockchain networks provide transparency through one decentralized and immutable ledger, complemented by homomorphic encryption that allows encrypted data to be processed without exposing its original content[43]. SDN architectures facilitate granular security policies with elliptic curve cryptography, hash functions, and digital signatures to detect tampering during transit[44]. Certificateless sign-cryption schemes unify digital signature and encryption, eliminating vulnerabilities of traditional certificates and key escrow risks in high-speed communications[45].

Blockchain technology with Merkle hash trees and smart contracts guarantees integrity and operational transparency; zero-knowledge proofs (ZKP) and secure multi-party computation (SMPC) verify authenticity without compromising confidentiality[46]. In serverless, sandboxing, memory erasure between executions, and encryption at rest and in transit, together with secure key management, enable compliance with GDPR and HIPAA[29]. Models for offloading data to the cloud require bidirectional mutual authentication combining SMS and image verification, together with proxy re-encryption and lightweight homomorphic encryption to efficiently process encrypted information[47]. Advanced security tools incorporate differential privacy and scaled attention layers in their AI models to detect threats without exposing users' identities[48]. Adoption in SMEs must be based on ISO 27005 for risk management and on CASB tools to control access and ensure compliance with privacy policies[7]. ISO 30300 and ISO 30301 standards define principles for secure recording and storage, facilitating the transition to encrypted digital archives with continuous availability[49].

The HFHE-Cloud model integrates federated learning and homomorphic encryption for multi-tenant environments, enabling collaborative training without exposing original data and ensuring traceability through on-chain auditing [39]. Protection in multi-tenant databases is achieved with automated CASE tools, logical isolation, RBAC, and partitioning policies to mitigate unauthorized access[50].

The Extended Zero Trust (EZT) methodology combines AI-based anomaly detection, continuous identity validation, and micro-segmentation to provide adaptive defense against insider threats[51]. DFL-RUL employs decentralized federated learning, transmitting only parameter up-

dates, eliminating centralization of raw data, and complying with international data protection standards[52]. IoT Hub unifies data models and ensures consistency, relying on cloud services with advanced threat mitigation and regulatory compliance for transport and storage[53]. The Tree-based-Signature and CyberGuarder protocols secure virtual environments and are complemented by cryptography in Li-Fi systems to strengthen client privacy[40].

XAI tools with SHAP values enable interpretable perspectives on resource allocation, overcoming the black-box nature of traditional algorithms[54]. Rigorous access controls, identity management, and encryption techniques, together with validation of disaster recovery capabilities, ensure the continuous integrity of digital assets[55]. Redundancy and multiple backups guarantee integrity in distributed environments, while virtualization provides transparency to the end user by abstracting the physical location of processing[32]. Provable data possession techniques verify integrity in the cloud; they are critical in sectors with sensitive data, such as healthcare, and facilitate digital forensic audits[56]. Advanced encryption and automatic backups are the main strategies of the cloud operating framework for guaranteeing information security and privacy[11].

### **Metaheuristic algorithms for optimizing task scheduling and allocation in cloud environments**

Metaheuristic methods are distinguished by their capacity to explore complex solution spaces; recognized approaches include GA, KHA, and CSA, as well as hybrid models such as PSO-SA and F-ACO to minimize makespan, energy consumption, and operating costs[57]. In addition to ACO, GA, and PSO, WOA, LOA, CS, and GWO have been proposed; these outperform traditional techniques in makespan and deadline violation rate[9]. In multi-objective programming, common techniques are ACO, GA, and PSO, while Cat Swarm Optimization has emerged to manage execution time and load in highly complex scenarios[5].

In edge and cloud environments, GA, FA, and PSO are employed as standard options, along with specialized variants such as OHNSGA and hybrid memetic algorithms (MADCP), to improve exploration and accelerate convergence[58]. For sustainable consolidation of VMs, IGA-POP, the Imperialist Competitive Algorithm (ICA), and Advanced Ant Colony Optimization (AACO) are reported, often integrated with machine learning techniques[10]. Sustainable management can be optimized using bio-inspired metaheuristics integrated into game theory frameworks such as GTGWO, PSO-GTA, and KASIA to maximize the use of clean energy[59].

The hybrid algorithm HHO-GWO integrates the global search of Harris Hawks Optimization with the local exploitation of Grey Wolf Optimizer for resource scheduling in containers, outperforming FA and WOA[13]. For scientific workflows, the DSSSO algorithm combines Dolphin Swarm Optimization (DSO) and Sparrow Search Algorithm (SSA), complemented by ACO and IBOA to optimize makespan and energy consumption[16]. GWO-EFO optimizes resource allocation in heterogeneous environments, while CSO and NSGA-III balance load and improve QoS[60]. The hybrid algorithm HCS-BA combines the Lévy flights of Cuckoo Search with the fine-tuning of the Bat Algorithm, while also reviewing Tabu search and FPO to reduce resource waste[14].

Traditional approaches employ the improved Multiverse Optimizer and adaptive PSO (AdPSO), which seek near-optimal solutions through dynamic adjustments to changes in load[25]. Simulated Annealing and genetic algorithms iteratively explore the solution space to avoid overprovisioning[61]. TLBO stands out for its fast convergence and low variance, whereas PSO is more effective in highly adaptable resource environments[17]. FireBat integrates the capabilities of Firefly with BAT, also categorizing PSO, ACO, ABC, and GWO as fundamental tools for reducing makespan[21].

The ICSO algorithm (Improved Chicken Swarm Optimization) documents effective metaheuristics, including algorithms inspired by whales, bats, cats, ant lions, and bee colonies for NP-hard problems[62]. HGHHC hybridizes HGSO and HHO by incorporating comprehensive opposition-based learning (COBL) to avoid local optima and improve makespan and resource usage[24]. GLOPS combines PSO for global exploration and Simulated Annealing for local refinement, achieving a 48.79% reduction in turnaround time compared to traditional approaches[22]. DALRS integrates GA for global refinement of assignments proposed by a reinforcement learning agent, managing more than 10,000 concurrent tasks while optimizing latency, cost, and energy consumption[18].

PSO offers lower costs and faster execution, whereas GA presents advantages in energy efficiency and reduction of operational costs under certain conditions in fog computing[63]. GIGOL integrates GA with GWO for multi-objective assignment problems, balancing response time, load balancing, and availability through population-based search and opposition-based learning[64]. In robust systems, MHHO+ACO balances load with fault awareness, improving the handling of critical tasks without excessive replication costs[23].

The research is divided between individual metaheuristics (bat, whale, cat swarm, ant lion) and hybridization strategies that combine ACO with PSO to maximize resource utilization[62]. PSO and ACO predominate in resource management; other approaches include cuckoo search, penguin optimization, firefly algorithms, and grey wolf optimization to reduce energy consumption and migrations[11]. MVO and CSO gain relevance due to their ability to handle the complexity of task scheduling; the integration of ACO and PSO enables dynamic load distribution adapted to real-time energy metrics[15]. For multi-objective optimization, SPEA, NPGA, and ABC are used, imitating biological behaviors to find optimal solutions in massive load environments[33]. The combination of GA with the Flower Pollination Algorithm (FPA) leverages the convergence of FPA and the crossover and mutation operators of GA to optimize completion time[20]. WOA and CSA overcome the limitations of traditional heuristics by avoiding local optima during task allocation[65].

### **Virtual machine consolidation techniques to optimize resource usage in cloud data centers**

VM consolidation is a fundamental optimization method that groups multiple virtual instances onto a minimum number of physical servers; the most common techniques are Best-Fit Decreasing (BFD) and its modified variant (MBFD), which seek compact and efficient allocation by reducing waste and energy consumption[11]. The most effective techniques include Best Fit and E-MBFD policies integrated with regression models to predict CPU demand, enabling dynamic allocation with safety margins to absorb fluctuations without compromising SLAs[10]. In sustainable computing, game theory frameworks model VMs and hosts as strategic players; the GTGWO algorithm facilitates intelligent migration to data centers with renewable energy[59].

Quantum computing techniques and genetic algorithms solve multi-objective optimization problems, achieving utilization rates of up to 90% through load balancing that minimizes energy waste[5]. Push and Pull migration techniques based on linked lists allow VMs to adjust their load in real time, moving processes from overloaded nodes to those with idle capacity to guarantee optimal utilization and deadline compliance[9]. The hybrid HCS-BA algorithm balances global exploration and local exploitation to avoid resource waste from inactive servers and reduce the energy footprint of data centers[14]. Multiplexing and consolidation of workloads allow more tasks to be executed on the allocated capacity, optimizing physical infrastructure and maximizing benefits with fewer data centers[61].

Persuasive autoscaling (PASM) with deep reinforcement learning facilitates a more adaptable resource distribution by verifying shared instances and executing migrations based on the demand ratio to minimize waiting times and service failures[26]. Intelligent schedulers with GWO-EFO ensure optimal resource mapping, reducing execution times and guaranteeing maximum utilization of available physical and virtual capacity[60]. VM consolidation, combined with methods such as dynamic voltage and frequency scaling (DVFS), balances operational performance with power consumption[18]. Dynamic consolidation reorganizes workloads to optimize the utilization of available resources without degrading agreed service levels[22].

Load balancing and server consolidation are pillars for maximizing system efficiency by enabling an equitable distribution of workload and reducing underutilization through the grouping of virtual instances[21]. Algorithms such as ChicWhale facilitate VM migration, constituting a fundamental enabling component for consolidation processes that improve data management and efficiency in distributed resources[66]. The joint consolidation of VMs and containers enables more flexible and efficient management in green cloud environments, significantly reducing energy consumption[15].

Hybrid techniques that combine K-Means with reinforcement learning make it possible to accurately identify which VMs should be migrated from overloaded servers, guaranteeing optimal load balancing[67]. The skewness metric quantifies the inequality in the use of hardware resources, facilitating the consolidation of heterogeneous workloads to maximize overall utilization and support green computing[54]. Live migration concentrates workloads on fewer active nodes, making it possible to shut down idle servers without degrading the quality of service to the end customer[40].

### **Main security challenges in cloud infrastructure**

The integration of edge-cloud infrastructures faces critical risks derived from its open architecture, including malicious data alteration and compute power hijacking, compromising availability and compliance with performance standards[41]. In serverless computing, shared infrastructure and event-based invocation amplify the challenges: gaps in tenant isolation lead to data leaks, and third-party libraries with permissive configurations facilitate attackers' lateral movement[29].

Virtualization requires new protection approaches, since conventional physical measures do not guarantee workload isolation or the management of legal liability when the user transfers operational control to the provider[44].

Malware poses a critical threat to IaaS infrastructure, exacerbated by users' inexperience; the redundant use of configuration scripts allows a single vulnerability to propagate across all servers[68]. Non-linear and persistent attack patterns—such as remote reconnaissance and privilege escalation—evade traditional monitoring systems during the transmission and distributed storage phases[43]. Dependence on external certificate authorities and the risk that the cloud administrator may access master keys create inherent distrust that demands certificateless cryptographic schemes[45].

Serverless computing introduces side-channel vulnerabilities, data leakage between functions, and exposure of residual states during container reuse after a cold start[29]. Centralized infrastructure creates single points of failure, while multi-tenancy increases the risk of inconsistencies in information management and privacy breaches[46]. Communication channels face DoS attacks, identity theft, malicious code injection (XSS), and spoofing techniques that compromise the integrity of resources delegated to the cloud[47]. IDS systems cannot scale in ultra-high-speed networks, and AI models have difficulty identifying zero-day attacks; moreover, high computational cost and lack of interpretability limit their real-time implementation[48].

Misconfigurations and storage security flaws are frequent vulnerabilities; organizational distrust of external control represents a critical barrier to service integrity and availability[7]. The convergence of AI and cloud introduces global challenges in which complex cyberattacks can incapacitate critical infrastructures, and the use of the cloud to design synthetic biological agents raises unprecedented biosecurity dilemmas[69]. The high dimensionality of traffic, class imbalance in datasets, and the constant evolution of attack patterns hinder effective intrusion detection in distributed and multi-tenant environments[35].

Cloud infrastructure is vulnerable to internal threats such as flooding, port scanning, and DDoS, which compromise the system's confidentiality, integrity, and availability triad[51]. The multi-tenant model presents critical risks of unauthorized cross-access among clients that share physical or logical infrastructures, requiring operational transparency from the provider (CSP)[50]. Challenges vary by service model: in IaaS, virtualization limitations are the fundamental challenge; in PaaS, interoperability and host sensitivity problems arise; and in SaaS, the focus is on authentication, authorization, and data protection[66]. Attacks by malicious insiders are the most destructive, as such insiders possess legitimate access or elevated privileges that allow them to bypass firewalls and conventional detection systems[70]. The multi-tenant architecture and node heterogeneity create risks of information leakage during synchronization of distributed models, requiring new encryption and anonymization strategies[39]. Operational failures can corrupt or destroy data, leading to authentication problems that block access for legitimate users[36].

VM migration in green clouds is vulnerable to the interception of sensitive data and to compromise of the kernel and hardware state[40]. DDoS attacks saturate bandwidth and server resources, preventing legitimate traffic in infrastructures whose dynamic design breaks conventional perimeter security paradigms[56]. The coexistence of multiple instances on a single physical server allows a vulnerability in a VM to be exploited to escalate privileges and gain unauthorized access to other users' data[11]. Compliance with various international laws such as the GDPR, when information is stored on servers outside the organization's direct authority, represents a fundamental barrier to cloud adoption[55]. The public cloud presents greater security and integrity challenges compared with hybrid or private models, which offer greater control over infrastructure[71].

## CONCLUSIONS

The results of this systematic review show that cloud computing continues to establish itself as an essential paradigm for managing digital infrastructures, but its efficiency depends on the interrelation among performance, security, and resource optimization. The analyzed literature shows that metrics such as makespan, latency, throughput, CPU utilization, memory, energy consumption, SLA compliance, and number of virtual machine migrations are fundamental for evaluating the performance of services and algorithms in distributed environments.

Likewise, it is concluded that metaheuristic and hybrid algorithms represent a dominant trend for task scheduling and resource allocation in the cloud. In particular, approaches based on GA, PSO, ACO, GWO, HHO, BAT, cuckoo search, and hybrid combinations have demonstrated the ability to reduce execution times, improve load balancing, decrease energy consumption, and

avoid local optima in highly dynamic scenarios.

Virtual machine consolidation is identified as a key strategy for optimizing data center utilization. Techniques such as BFD, MBFD, live migration, predictive demand models, reinforcement learning, and hybrid approaches make it possible to reduce idle servers, improve energy efficiency, and maintain agreed service levels. These findings reinforce the importance of integrating adaptive mechanisms capable of responding to real-time load variations.

In terms of security, the review confirms that cloud environments face persistent threats associated with multi-tenant architectures, DDoS attacks, misconfigurations, malware, data leaks, side channels, and risks derived from virtualization. To address these challenges, the most relevant solutions include blockchain, federated learning, homomorphic encryption, zero-knowledge proofs, zero-trust architectures, robust identity management, and distributed auditing mechanisms.

Finally, it is concluded that the development of resilient, sustainable, and secure cloud ecosystems requires multidimensional evaluation models that are not limited to technical performance, but rather integrate economic, energy, environmental, regulatory, and privacy criteria. Consequently, future research should be oriented toward hybrid frameworks that combine artificial intelligence, advanced security, and multi-objective optimization, with reproducible experimental validations and rigorous comparisons against the state of the art.

## REFERENCES

1. O. A. Shonubi, "The role of digital B2B platforms with industry 4.0 technological ecosystems(integration of cloud computing, artificial intelligence and internet of things) as a growth lever", *Sustain. Futur.*, vol. 10, p. 101041, dic. 2025, doi: 10.1016/j.sft.2025.101041.
2. S. L. Pfleeger y B. A. Kitchenham, "Evidence-Based Software Engineering Guidelines Revisited", *IEEE Trans. Softw. Eng.*, vol. 51, núm. 3, pp. 814–819, mar. 2025, doi: 10.1109/TSE.2025.3526730.
3. J. A. Jiménez-Toledo, C. Collazos, y O. Revelo-Sánchez, "Consideraciones en los procesos de enseñanza-aprendizaje para un primer curso de programación de computadores: una revisión sistemática de la literatura", *Tecnológicas*, vol. 22, pp. 83–117, dic. 2019, doi: 10.22430/22565337.1520.
4. F. Nadeem, "Evaluating and Ranking Cloud IaaS, PaaS and SaaS Models Based on Functional and Non-Functional Key Performance Indicators", *IEEE Access*, vol. 10, pp. 63245–63257, 2022, doi: 10.1109/ACCESS.2022.3182688.
5. N. M. Alsafri, A. Y. Hamed, A. Mindil, y M. R. Hassan, "Innovative quantum techniques for improving system performance in cloud computing", *Egypt. Inform. J.*, vol. 30, p. 100710, jun. 2025, doi: 10.1016/j.eij.2025.100710.
6. F. Quiñonez-Cuenca et al., "Evaluación de AIoT en modelos computacionales en la nube y en el borde aplicado a la detección de mascarillas", *Ingenius*, núm. 27, dic. 2021, doi: 10.17163/ings.n27.2022.04.
7. V. I. Guevara Arias y S. Domingo Soriano, "La nube en Pymes mediante las normas ISO 27005", *Rev. Ing.*, vol. 6, núm. 15, pp. 169–182, may 2022, doi: 10.33996/revistaingenieria.v6i15.98.
8. L. Pons, S. Petit, y J. Sahuquillo, "Advanced resource management: A hands-on master course in HPC and cloud computing", *J. Parallel Distrib. Comput.*, vol. 202, p. 105091, ago. 2025, doi: 10.1016/j.jpdc.2025.105091.
9. R. Bs, N. M, N. Srikanth, N. V. Halatti, y P. Srinivasan, "A novel push pull optimization algorithm fostered deadline aware task scheduling in virtualized cloud computing", *Frankl. Open*, vol. 14, p. 100499, mar. 2026, doi: 10.1016/j.fraope.2026.100499.
10. E. Cesario, P. Lindia, F. Lobello, A. Vinci, y S. Capalbo, "Enhancing energy efficiency in cloud computing through regression models: A data-driven approach with experimental validation", *Future Gener. Comput. Syst.*, vol. 177, p. 108245, abr. 2026, doi: 10.1016/j.future.2025.108245.
11. J. Singh y N. K. Walia, "A Comprehensive Review of Cloud Computing Virtual Machine Consolidation", *IEEE Access*, vol. 11, pp. 106190–106209, 2023, doi: 10.1109/ACCESS.2023.3314613.
12. L. Zhang, J. Bai, y J. Xu, "Optimal Allocation Strategy of Cloud Resources With Uncertain Supply and Demand for SaaS Providers", *IEEE Access*, vol. 11, pp. 80997–81010, 2023, doi: 10.1109/ACCESS.2023.3300735.
13. D. Zhang, X. Xie, y Y. Song, "A Multi-Objective Optimization-Based Container Cloud Resource Scheduling Method", *Future Internet*, vol. 18, núm. 1, p. 58, ene. 2026, doi: 10.3390/fi18010058.
14. S. Benflis, S.-S. Bendib, S. Maamar, F. Z. Cherhabil, y H. Merouani, "Virtual Machine Placement in Cloud Environments Using a Hybrid Cuckoo Search and Bat Algorithm", *J. Telecommun. Inf. Technol.*, vol. 102, núm. 4, pp. 33–42, dic. 2025, doi: 10.26636/jtit.2025.4.2244.
15. B. M. Beena et al., "Adaptive Energy Optimization in Cloud Computing Through Containerization", *IEEE Access*, vol. 13, pp. 159548–159565, 2025, doi: 10.1109/ACCESS.2025.3606932.
16. S. Subashree, M. Rajakumaran, G. Pushpa, y S. Senthilkumar, "Hybrid dolphin swarm sparrow search optimization based multi-objective cloud workflow scheduling", *J. Cloud Comput.*, vol. 14, núm. 1, p. 80, dic. 2025, doi: 10.1186/s13677-025-00828-8.
17. M. Bishnoi y N. Dutta, "Comparative Analysis of Dynamic Cost-Time Allocation Techniques in Cloud Environments", *ITM Web Conf.*, vol. 81, p. 01002, 2026, doi: 10.1051/itmconf/20268101002.
18. M. M. E. M. M. Salem, "Distributed Machine Learning Optimization for Large-Scale Cloud Resource Scheduling: A Hybrid Deep Learning and Evolutionary Algorithm Approach", 2026, doi: 10.34808/TQ2025/29.2/B.
19. R. Zhanuzak, M. A. Ala'Anzy, M. Othman, y A. Algarni, "Optimizing Cloud Computing Performance With an Enhanced Dynamic Load Balancing Algorithm for Superior Task Allocation", *IEEE Access*, vol. 12, pp. 183117–183132, 2024, doi: 10.1109/ACCESS.2024.3508793.
20. N. K. Walia et al., "An Energy-Efficient Hybrid Scheduling Algorithm for Task Scheduling in the Cloud Computing Environments", *IEEE Access*, vol. 9, pp. 117325–117337, 2021, doi: 10.1109/ACCESS.2021.3105727.
21. N. Pathania, B. Singh, I. Batra, D. Prashar, A. A. Khan, y S. Kadry, "FireBat: a hybrid approach for load balancing in cloud computing", *J. Cloud Comput.*, vol. 15, núm. 1, p. 5, ene. 2026, doi: 10.1186/s13677-025-00805-1.
22. S. A. A. M. Zarif et al., "GLOPS: A Hybrid Approach for Enhanced Scheduling in Cloud Computing Environments via Machine Learning-Based Process Prediction", *IEEE Access*, vol. 13, pp. 134385–134402, 2025, doi: 10.1109/ACCESS.2025.3592211.
23. A. Alwabel y M. Numair, "Fault Tolerance in Fog Computing: Hybrid Approach", *IEEE Access*, vol. 14, pp. 8573–8583, 2026, doi: 10.1109/ACCESS.2026.3653254.
24. N. Omran Alkaam, A. Bakar Md Sultan, M. B. Hussin, y K. Yatim Sharif, "Hybrid Henry Gas-Harris Hawks Comprehensive-Opposition Algorithm for Task Scheduling in Cloud Computing", *IEEE Access*, vol. 13, pp. 12956–12965, 2025, doi: 10.1109/ACCESS.2025.3530860.
25. H. Pei et al., "LLM-based cost-aware task scheduling for cloud computing systems", *J. Cloud Comput.*, vol. 14, núm. 1, p. 81, dic. 2025, doi: 10.1186/s13677-025-00822-0.
26. V. R. Rajasekar y G. Santhi, "Pervasive Auto-Scaling Method for Improving the Quality of Resource Allocation in Cloud Platforms", *Big Data Cogn. Comput.*, vol. 9, núm. 11, p. 294, nov. 2025, doi: 10.3390/bdcc9110294.
27. J. Jeon, S. Park, B. Jeong, y Y.-S. Jeong, "Efficient Container Scheduling With Hybrid Deep Learning Model for Improved Service Reliability in Cloud Computing", *IEEE Access*, vol. 12, pp. 65166–65177, 2024, doi: 10.1109/ACCESS.2024.3396652.

28. H. Sun, L. Gu, C. Dong, X. Ma, Z. Liu, y Z. Li, "Cloud Computing Resource Scheduling Algorithm Based on Unsampld Collaborative Knowledge Graph Network", *IEEE Access*, vol. 12, pp. 186476–186483, 2024, doi: 10.1109/ACCESS.2024.3472212.
29. A. Kumari, R. K. Behera, K. S. Sahoo, B. Sahoo, y A. H. Gandomi, "Emergence of serverless computing in cloud: A state-of-the-art review of challenges and opportunities", *Mach. Learn. Appl.*, vol. 24, p. 100862, jun. 2026, doi: 10.1016/j.mlwa.2026.100862.
30. Z. Abdiramanov, "Design and implementation of a scalable microservice-based cloud computing service for stochastic fluid flow modeling", *Array*, vol. 29, p. 100679, mar. 2026, doi: 10.1016/j.array.2026.100679.
31. S. Manam, K. Moessner, y S. Vural, "Deadline-Constrained Cost Minimisation for Cloud Computing Environments", *IEEE Access*, vol. 11, pp. 38514–38522, 2023, doi: 10.1109/ACCESS.2023.3258682.
32. Y. Zheng y X. Wen, "The Application of Artificial Intelligence Technology in Cloud Computing Environment Resources", *J. Web Eng.*, oct. 2021, doi: 10.13052/jwe1540-9589.2067.
33. B. Kruekaew y W. Kimpan, "Multi-Objective Task Scheduling Optimization for Load Balancing in Cloud Computing Environment Using Hybrid Artificial Bee Colony Algorithm With Reinforcement Learning", *IEEE Access*, vol. 10, pp. 17803–17818, 2022, doi: 10.1109/ACCESS.2022.3149955.
34. F. Ahmad et al., "Levelized Multiple Workflow Allocation Strategy Under Precedence Constraints With Task Merging in IaaS Cloud Environment", *IEEE Access*, vol. 10, pp. 92809–92827, 2022, doi: 10.1109/ACCESS.2022.3202651.
35. S. K. S et al., "An Unsupervised Cloud-Centric Intrusion Diagnosis Framework Using Autoencoder and Density-Based Learning", *Future Internet*, vol. 18, núm. 1, p. 54, ene. 2026, doi: 10.3390/fi18010054.
36. S. Aldomi, H. Suleiman, A. Shatnawi, y L. Alawneh, "A deep learning approach for early prediction of task failures in cloud computing environments", *Syst. Soft Comput.*, vol. 8, p. 200442, jun. 2026, doi: 10.1016/j.sasc.2026.200442.
37. N. F. Siddiqui et al., "SpectraNet: a lightweight hybrid time–frequency deep learning framework for sustainable cloud workload forecasting", *J. Cloud Comput.*, vol. 14, núm. 1, p. 75, dic. 2025, doi: 10.1186/s13677-025-00815-z.
38. X. Su y X. Li, "Elastic Performance Test Method of Web Server in Cloud Computing Environment", *J. Web Eng.*, ago. 2021, doi: 10.13052/jwe1540-9589.20514.
39. J. Wang y Y. Wang, "Privacy Protection Optimization Method for Cloud Platforms Based on Federated Learning and Homomorphic Encryption", *Sensors*, vol. 26, núm. 3, p. 890, ene. 2026, doi: 10.3390/s26030890.
40. A. Ahmad, S. U. Khan, H. U. Khan, G. M. Khan, y M. Ilyas, "Challenges and Practices Identification via a Systematic Literature Review in the Adoption of Green Cloud Computing: Client's Side Approach", *IEEE Access*, vol. 9, pp. 81828–81840, 2021, doi: 10.1109/ACCESS.2021.3085707.
41. Q. Deng, M. Goudarzi, A. Shaghghi, M. Sarvi, y R. Buyya, "A secure framework for containerized IoT applications in integrated edge–cloud computing environments", *Future Gener. Comput. Syst.*, vol. 174, p. 108010, ene. 2026, doi: 10.1016/j.future.2025.108010.
42. M. Montagnese et al., "Cloud computing for equitable, data-driven dementia medicine", *Lancet Digit. Health*, vol. 7, núm. 11, p. 100902, nov. 2025, doi: 10.1016/j.landig.2025.100902.
43. R. Ravi Kanth y T. Prem Jacob, "Evolutionary gravitational neocognitron neural network espoused blockchain-based intrusion detection framework for enhancing cybersecurity in a cloud computing environment", *Ain Shams Eng. J.*, vol. 16, núm. 12, p. 103805, dic. 2025, doi: 10.1016/j.asej.2025.103805.
44. X. Dong y Y. Xie, "Research on cloud computing network security mechanism and optimization in university education management informatization based on OpenFlow", *Syst. Soft Comput.*, vol. 7, p. 200225, dic. 2025, doi: 10.1016/j.sasc.2025.200225.
45. J. Mala, V. J. Arulkarthick, P. Bachanna, y K. Srihari, "Weibull distributed recurrent neural ergodic skewed certificateless signcryption for data protection in cloud computing environment", *Ain Shams Eng. J.*, vol. 17, núm. 3, p. 103991, mar. 2026, doi: 10.1016/j.asej.2026.103991.
46. K. T y K. V, "Blockchain-Enhanced Framework for Ensuring Data Consistency, Transparency and Privacy in Cloud Computing", *J. Appl. Eng. Technol. Sci. JAETS*, vol. 7, núm. 1, pp. 708–729, dic. 2025, doi: 10.37385/jaets.v7i1.8851.
47. A. S. Al-Ahmad, A. Shrestha, O. Ali, y H. Kahtan, "Cross-technology cloud offloading model", *J. Cloud Comput.*, vol. 14, núm. 1, p. 74, dic. 2025, doi: 10.1186/s13677-025-00819-9.
48. C. Rout, S. Sethi, J. C. Badajena, y R. K. Sahoo, "FSEGM: feature selection and ensemble generative model for adaptive cloud security", *J. Cloud Comput.*, vol. 15, núm. 1, p. 6, dic. 2025, doi: 10.1186/s13677-025-00818-w.
49. Y. A. Cerna Romero, J. Y. Delgado Tantaleán, y H. J. Salas Canales, "Cloud Computing y gestión documental en una empresa de servicios BPO, distrito de Magdalena del Mar (Lima-Perú), 2021", *Ind. Data*, vol. 25, núm. 1, pp. 285–298, ago. 2022, doi: 10.15381/idata.v25i1.21960.
50. S. L. Akram, "Ensuring data protection within multi-tenant databases built on cloud infrastructure", *Iraqi J. Comput. Inform.*, vol. 52, núm. 1, pp. 63–89, feb. 2026, doi: 10.25195/ijci.v52i1.660.
51. N. Mathivanan y B. Lanitha, "An integrated methodology for intrusion detection and mitigation to optimize cloud security", *J. Cloud Comput.*, vol. 15, núm. 1, p. 18, feb. 2026, doi: 10.1186/s13677-026-00858-w.
52. J. Pournazari et al., "DFL-RUL: Decentralised Federated Learning for Battery Remaining Useful Life Estimation on Heterogeneous Edge-to-cloud", *Energy AI*, vol. 24, p. 100689, may 2026, doi: 10.1016/j.egyai.2026.100689.
53. Y. Liu, K. Akram Hassan, M. Karlsson, Z. Pang, y S. Gong, "A Data-Centric Internet of Things Framework Based on Azure Cloud", *IEEE Access*, vol. 7, pp. 53839–53858, 2019, doi: 10.1109/ACCESS.2019.2913224.
54. A. S. Slathia et al., "SHERA: SHAP-Enhanced Resource Allocation for VM Scheduling and Efficient Cloud Computing", *IEEE Access*, vol. 13, pp. 92816–92832, 2025, doi: 10.1109/ACCESS.2025.3568917.

55. A. Santos, J. Martins, P. Duarte Pestana, R. Gonçalves, H. São Mamede, y F. Branco, "Factors Affecting Cloud Computing Adoption in the Education Context—Systematic Literature Review", *IEEE Access*, vol. 12, pp. 71641–71674, 2024, doi: 10.1109/ACCESS.2024.3400862.
56. A. A. Alqarni, "Majority Vote-Based Ensemble Approach for Distributed Denial of Service Attack Detection in Cloud Computing", *J. Cyber Secur. Mobil.*, mar. 2022, doi: 10.13052/jcsm2245-1439.1126.
57. A. Saeed, "A genetic algorithm with selective repair method under combined-criteria for deadline-constrained IoT workflow scheduling in Fog–Cloud computing", *Future Gener. Comput. Syst.*, 2026.
58. Z. Wang, "ReinFog: A Deep Reinforcement Learning empowered framework for resource management in edge and cloud computing environments", *J. Netw. Comput. Appl.*, 2025.
59. F. J. Maldonado Carrascosa, S. García Galán, M. Valverde Ibáñez, M. Szczerska, T. Marciniak, y N. Ruiz Reyes, "Fuzzy game-theoretic optimization for sustainable cloud computing", *Eng. Appl. Artif. Intell.*, vol. 162, p. 112725, dic. 2025, doi: 10.1016/j.engappai.2025.112725.
60. S. K. Soni y M. Awasthi, "OPTIMIZED RESOURCE MANAGEMENT IN CLOUD SCHEDULERS USING HYBRID ELECTRIC FISH AND GREY WOLF OPTIMIZATION", *Proc. Eng. Sci.*, vol. 7, núm. 4, pp. 2685–2694, dic. 2025, doi: 10.24874/PES07.04A.029.
61. Subject Matter Expert (SME), Barclays, USA y A. Mahida, "A Comprehensive Review on Ethical Considerations in Cloud Computing-Privacy, Data Sovereignty and Compliance", *J. Artif. Intell. Cloud Comput.*, pp. 1–4, dic. 2022, doi: 10.47363/JAICC/2022(1)231.
62. S. Liu, X. Chen, y F. Cheng, "Research on Task Scheduling for Internet of Things Cloud Computing Based on Improved Chicken Swarm Optimization Algorithm".
63. S.-E. Chafi, Y. Balboul, M. Fattah, S. Mazer, y M. E. Bekkali, "Enhancing resource allocation in edge and fog-cloud computing with genetic algorithm and particle swarm optimization".
64. M. R. Djebbara, "Cloud Replica Management-Based Hybrid Optimization".
65. T. Gao, Q. Tang, J. Li, Y. Zhang, Y. Li, y J. Zhang, "A Particle Swarm Optimization With Lévy Flight for Service Caching and Task Offloading in Edge-Cloud Computing", *IEEE Access*, vol. 10, pp. 76636–76647, 2022, doi: 10.1109/ACCESS.2022.3192846.
66. P. Rana, I. Batra, A. Malik, I.-H. Ra, O.-S. Lee, y A. S. M. Sanwar Hosen, "Efficacious Novel Intrusion Detection System for Cloud Computing Environment", *IEEE Access*, vol. 12, pp. 99223–99239, 2024, doi: 10.1109/ACCESS.2024.3424528.
67. G. F. Shidik, O. Setiono, E. J. Kusuma, L. B. Handoko, P. N. Andono, y M. F. Abdollah, "Novel Unsupervised Cluster Reinforcement Q-Learning in Minimizing Energy Consumption of Federated Edge Cloud", *IEEE Access*, vol. 13, pp. 92577–92595, 2025, doi: 10.1109/ACCESS.2025.3572084.
68. J. C. Kimmel, A. D. Mcdole, M. Abdelsalam, M. Gupta, y R. Sandhu, "Recurrent Neural Networks Based Online Behavioural Malware Detection Techniques for Cloud Infrastructure", *IEEE Access*, vol. 9, pp. 68066–68080, 2021, doi: 10.1109/ACCESS.2021.3077498.
69. P. R. Karmakar, D. Ghosh, J. Chakraborty, S. Bhattacharjee, y R. Saha, "Cloud Computing : Today and Tomorrow", *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, núm. 4, pp. 2716–2720, abr. 2025, doi: 10.22214/ijraset.2025.68374.
70. A. T. Olusesi, I. K. Okakwu, A. A. Okubanjo, A. I. Oyediji, y O. O. Bello, "Intrusion Detection in Cloud Computing Using Support Vector Machine and Fast Firefly Algorithm", *AUIQ Tech. Eng. Sci.*, vol. 3, núm. 1, ene. 2026, doi: 10.70645/3078-3437.1052.
71. H. Eljak et al., "E-Learning-Based Cloud Computing Environment: A Systematic Review, Challenges, and Opportunities", *IEEE Access*, vol. 12, pp. 7329–7355, 2024, doi: 10.1109/ACCESS.2023.3339250.

## **FUNDING**

No financing

## **CONFLICT OF INTEREST**

None

## **AUTHORSHIP CONTRIBUTIONS**

Drafting – original draft: Nidia Jael Muñoz Oviedo.

Writing–review and editing: Nidia Jael Muñoz Oviedo.