www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 14 Issue 07 July 2025, Page No. 27572-27578
ISSN: 2319-7242 DOI: 10.18535/ijecs/v14i07.5193

Comparative Analysis of Cloud Deployment Models: Public, Private, Hybrid, and Multi-Cloud

Erik Ghazaryan

Senior Software Developer, Nagarro
Vienna, Austria

Abstract
This article presents a comprehensive examination of cloud deployment models. The topic is timely because enterprises must navigate an increasingly complex cloud landscape to achieve competitive advantage. The study compares public, private, hybrid, and multi-cloud deployment models on the basis of current scholarly literature and industry data published between 2021 and 2025, with emphasis on their characteristics, benefits, limitations, and use cases. The research novelty lies in the systematic consolidation and analysis of recent studies on cloud-computing deployment, highlighting emerging trends and challenges in multi-cloud environments and their implications for strategic decision-making. The findings are relevant to IT executives, cloud-solution architects, information-technology researchers, and decision-makers engaged in digital transformation. They are also valuable to chief digital officers and chief financial officers who must assess risk and budgetary considerations when migrating infrastructure to the cloud. The principal conclusion is that no single deployment model is universally optimal; selection depends on an organization's specific requirements for security, regulatory compliance, performance, cost, and control. A sustained shift toward hybrid and multi-cloud strategies is observed as organizations seek a balanced approach.

Keywords: cloud computing, public cloud, private cloud, hybrid cloud, multi-cloud, cloud-deployment models, comparative analysis, cloud strategy.

Introduction

The contemporary digital economy is characterised by unprecedented rates of technological change, with cloud computing serving as a foundational enabler of innovation and business-process transformation [1]. The capability of cloud technologies to provide on-demand computing resources, ensure scalability, and optimise costs has made them an indispensable component of the IT strategies adopted by organisations worldwide [2]. Migrating to cloud-based solutions allows enterprises to enhance agility, accelerate time-to-market, and concentrate on core competencies by delegating infrastructure management to specialised providers or to internal IT departments employing new operational approaches [3, 4]. Industry reports indicate sustained growth: according to Gartner, end-user spending on public cloud services is projected to increase by 20.4 % to USD 675.4 billion in 2024, compared with USD 561 billion in 2023; this expansion is driven by generative artificial intelligence (GenAI) and application modernisation [5].

The purpose of this article is to conduct an extensive comparative analysis of public, private, hybrid, and multi-cloud deployment models, drawing on up-to-date scholarly literature and industry data.

The study's novelty derives from the systematic consolidation and examination of recent research on cloud-computing deployment models, identifying emerging trends and challenges within multi-cloud environments and assessing their influence on strategic choices.

The working hypothesis posits that, although public-cloud models continue to dominate general-purpose computing and scalability requirements, hybrid and multi-cloud strategies are increasingly adopted to balance cost, security, compliance, and vendor independence, despite their inherent management complexity.

Materials and Methods

A structured review and analysis of scholarly literature and industry reports were undertaken to achieve the stated objective and to test the working hypothesis. Source retrieval was conducted in leading scientometric databases—Google Scholar, IEEE Xplore, ACM Digital Library, and Scopus—as well as on the websites of authoritative analytic agencies such as Gartner, IDC, and Flexera.

Pal S., Le D. N., and Pattnaik P. K. [3] outline the evolution of cloud models, service layers, and selection criteria for public versus private deployment. Vendors refine these boundaries and characteristics: Amazon Web Services regards the cloud as a collection of remote resources and services managed over the internet [26]; Microsoft Azure emphasises ownership scenarios and network architectures across public, private, and hybrid clouds [27]; Google Cloud defines multi-cloud as orchestrating resources from multiple providers under unified governance [28]; VMware highlights workload elasticity and portability in multi-cloud environments [29]; and IBM describes established deployment models together with sector-specific practices and integration guidance [30].

Comparative studies and market reports complement this classification with practical assessments. Patel H. and Kansara N. [1] construct an evaluation matrix for public, private, and hybrid clouds based on cost, scalability, and risk management. Jawed M. S. and Sajid M. [6] survey architectures, tools, and open challenges across all deployment types, underscoring the need for resource-management automation. Gartner projects end-user spending on public cloud to exceed USD 675 billion in 2024 [5]; the Flexera report records rising adoption of hybrid and multi-cloud strategies among large enterprises [17]; and Statista data confirm sustained revenue growth from public cloud services between 2017 and 2025 [19].

Security and privacy are examined within the context of different models. Möller D. P. F. [7] analyses alignment with the NIST Cybersecurity Framework and MITRE criteria for hybrid settings. Parast F. K. et al. [11] systematise vulnerabilities across IaaS, PaaS, and SaaS layers. Al Ahmad A. S. et al. [12] identify mobile-access risks and propose authentication and encryption methods. Abdulsalam Y. S. and Hedabou M. [14] provide a technical review of data-protection mechanisms in public and private clouds. Yanamala A. K. Y. [20] catalogues emerging security challenges and research directions in identity management.

Architectures of hybrid and multi-cloud systems are considered from the perspectives of integration, orchestration, and management tooling. Seifert M., Kuehnel S., and Sackmann S. [16] investigate SaaS-based hybrid clouds, detailing the difficulties of integration and load balancing between private and public resources. Alonso J. et al. [10] analyse patterns for multi-cloud-native applications and microservice orchestration. Merseedi K. J. and Zeebaree S. R. M. [23] summarise approaches to distributed and federated multi-cloud environments. Firdaus W. and Sukmaaji A. [18] discuss network security and cost control when implementing hybrid and multi-clouds. Putri A. [22] develops management strategies for big-data and AI applications in multi-cloud settings. Madupati B. [25] considers Kubernetes for orchestration, scalability, and security across hybrid and multi-cloud environments. Shafiei H., Khonsari A., and Mousavi P. [24] explore serverless computing as a form in which infrastructure management is abstracted.

Applied domains and findings reveal trends and research gaps. Mishra G. [8] analyses smart healthcare, where hybrid clouds balance patient-data confidentiality with analytics scalability. Maqueira Marín J. M. et al. [15] study the impact of clouds on human-resource management processes. Gill S. S. et al. [9] regard multi-cloud strategies as a means to enhance the resilience and flexibility of AI solutions. Al-Ghaili A. M. et al. [21] describe metaverse architectures that rely on distributed multi-cloud infrastructure. Kim D., Lee S., and Kim S. [2] demonstrate how integrating cloud services can improve the resilience of campus projects and university–community engagement. IDC reports that heightened demand for AR/VR headsets in late 2023 spurred additional cloud-computing capacity for content rendering and streaming [4]. Heidari A. and Jafari Navimipour N. [13] showcase diverse service-discovery mechanisms, ranging from DNS-based solutions to peer-to-peer protocols.

Questions of standardised metrics for comparing performance and security in heterogeneous multi-cloud settings remain insufficiently explored. Most studies focus on individual aspects without proposing comprehensive frameworks for assessing the long-term aggregate effectiveness of multi-cloud strategies.

Results and Discussion

Public cloud denotes a model in which IT resources (for example, servers, data storage, applications) are owned and managed by a third-party cloud provider and offered to multiple customers over the Internet [7, 12]. Private cloud refers to infrastructure reserved exclusively for a single organisation, which may encompass several consumers (for instance, business units) [25, 27]. Ownership, management, and operation of a private cloud can reside with the organisation itself, a third party, or a combination thereof, and its physical location may be on-premises or off-site [14, 22]. Hybrid cloud combines two or more distinct cloud infrastructures (private, public) that remain separate entities but are linked via standardised or proprietary technologies to ensure portability of data and applications [8, 16, 19]. A multi-cloud strategy involves the use of multiple public cloud services from different providers. It is important to distinguish multi-cloud from hybrid cloud: hybrid deployments always include a private component, whereas multi-cloud may consist solely of multiple public clouds [9, 11].

The optimal deployment model depends on numerous factors specific to each organisation. Table 1 summarises the comparison of these models across key criteria.

Table 1. Comparative characteristics of cloud computing deployment models [6, 10, 13, 14, 26].

Criterion	Public Cloud	Private Cloud	Hybrid Cloud	Multi-Cloud
Cost	Low up-front investment; pay-as-you-go	High up-front investment; predictable operating costs	Mixed; potential for optimisation	Mixed; complex cost control
Security	Shared responsibility; inherent risks	High; full control	Complex; integration-dependent	Highly complex; requires unified policies
Scalability	High; virtually unlimited	Limited by available resources; more challenging	High (enabled by public component)	High (leveraging multiple providers)
Control	Limited	Full	Partial; depends on component	Distributed; complex
Performance	Variable (“noisy neighbour” effect)	Predictable	Dependent on configuration and networking	Dependent on providers and integration
Management	Relatively simple (provider-managed)	Complex (in-house)	Highly complex (integration of environments)	Extremely complex (multiple providers)
Vendor lock-in	High risk	Low risk (if fully in-house)	Medium risk (depends on public provider)	Low risk (diversification)
Compliance	Potentially challenging	Simplified	Complex; requires detailed planning	Very complex; requires auditing each provider
Flexibility	High within provider	Low (changes require time)	Very high	Very high (choice of services)

Criterion	Public Cloud	Private Cloud	Hybrid Cloud	Multi-Cloud
	offerings			

Statistical data confirm the growing popularity of hybrid and multi-cloud approaches. The Flexera "2023 State of the Cloud Report," based on survey responses, illustrates the public cloud services used by organisations (Fig. 1) [17].

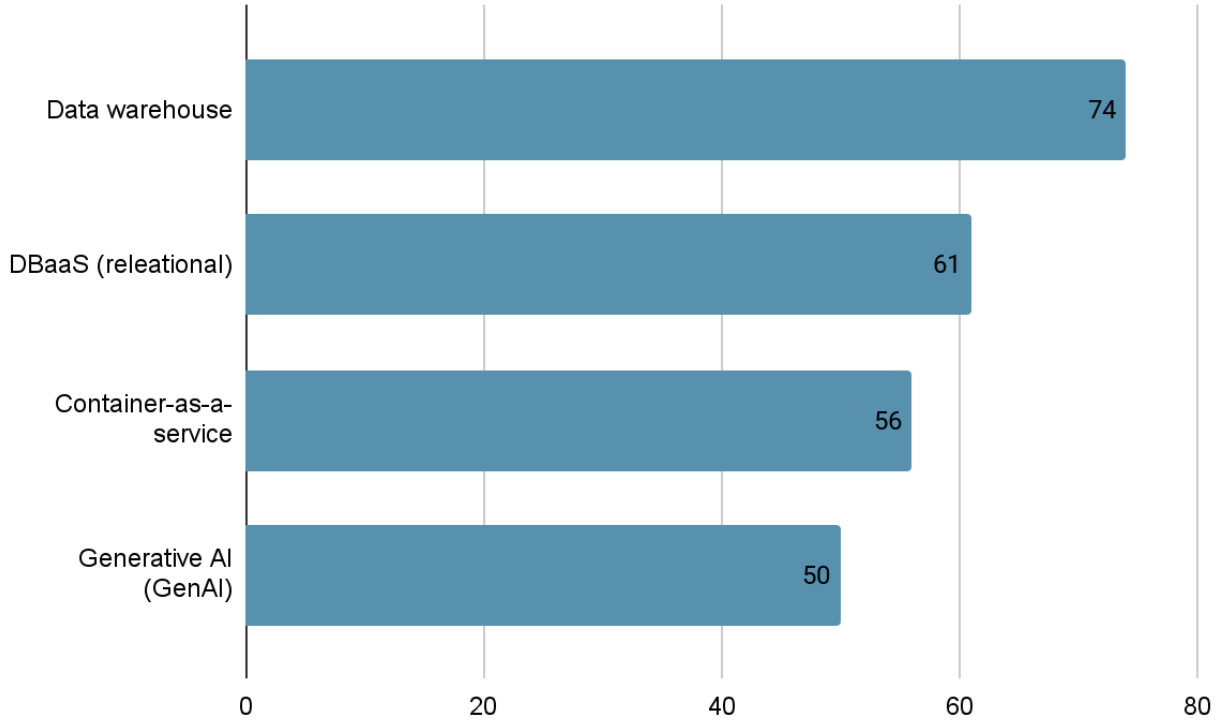

Fig.1. Public cloud services used by organizations [17].

These results indicate that companies strive to combine the advantages of different models. Figure 2 presents the forecast of global user spending on public clouds.

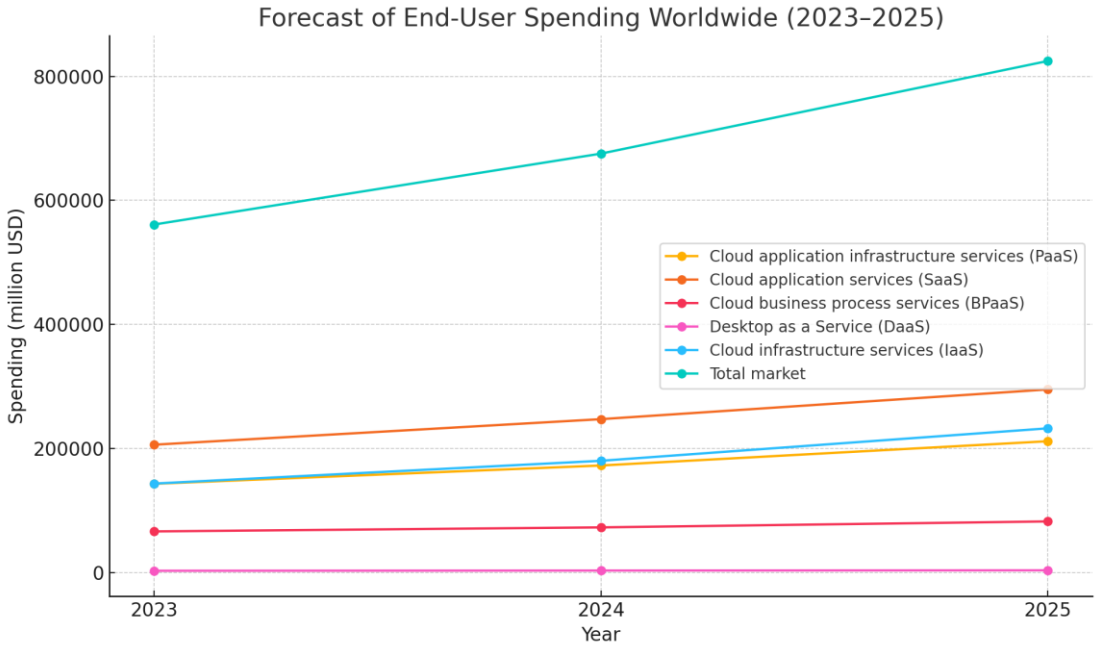

Fig.2. Forecast of user spending worldwide on public clouds [5].

The principal challenges encountered during cloud adoption also vary by model. In public clouds, security remains the foremost concern (reported by approximately 80 % of respondents), followed by cost management and a lack of expertise. Private clouds primarily face issues with cost control and scalability. In hybrid and multi-cloud environments, complexity of management, integration, security enforcement, and compliance in heterogeneous settings emerge as the key challenges [17, 18, 30]. Figure 3 depicts the interrelation among cloud deployment models.

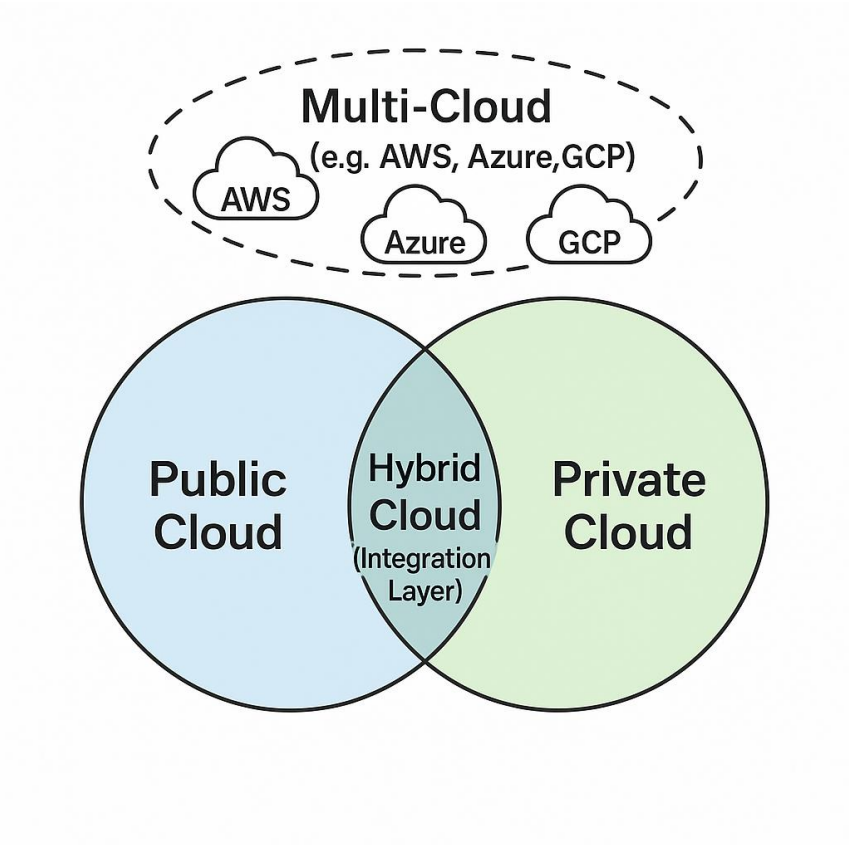

Fig.3. Interrelation of cloud deployment models [15, 20, 28, 29].

When discussing the results, it is important to recognise that deployment-model selection is not static. As businesses evolve, market conditions shift, and new technologies emerge, organisations may revisit their cloud strategies [20, 23]. The move toward hybrid and multi-cloud environments reflects a pursuit of flexibility and optimisation, yet it compels organisations to cultivate new capabilities in managing complexity, ensuring security, and controlling costs [21, 24]. In modern cloud engineering, containerisation and serverless computing act as catalysts for paradigm shifts in application design, deployment, and management: container technologies (Docker, CRI-O) combined with Kubernetes-level orchestrators establish standardised, isolated environments with guaranteed reproducibility and automatic scaling, while serverless platforms (AWS Lambda, Azure Functions, Google Cloud Functions) relieve developers of runtime-management overhead by provisioning resources on-demand in response to events, thereby minimising response times and “warm-up” costs. Their integration—containers for stateful services plus FaaS/BaaS for event-driven components—yields modular, fault-tolerant microservice ecosystems with a high level of infrastructure abstraction, simplifying portability across public, private, and hybrid clouds, as well as compliance with security policies and regulatory requirements.

Conclusion

The analysis of contemporary cloud deployment paradigms—public, private, hybrid, and multi-cloud—based on an extensive review of scholarly publications and industry reports has enabled the systematic

organisation of their functional characteristics, operational benefits, and limitations, as well as the identification of typical application scenarios in both corporate and public domains.

First, public clouds exhibit unparalleled elasticity and cost efficiency when scaling resources for peak demand and short-term initiatives. A high degree of management automation and a broad catalogue of ready-to-use services accelerate time-to-market. However, inherent risks persist: limited control over physical infrastructure, potential vulnerabilities in safeguarding sensitive data, and vendor lock-in, which can hinder long-term digital-transformation strategies.

Second, private cloud environments deployed within corporate or leased data centres provide the highest level of control and regulatory compliance. The absence of reliance on external providers reduces the likelihood of data-breach incidents but increases operational expenses and complicates rapid scalability, particularly during unforeseen demand surges.

The third notable trend is the proliferation of hybrid architectures, which unite the "best of both worlds"—the reliability and security of private clouds with the flexibility and expansive ecosystem of public clouds. Furthermore, a multi-cloud approach allows organisations to diversify risk by selecting services from multiple providers according to workload requirements: mission-critical business applications are hosted in isolated zones, while ancillary services reside in the public cloud. Simultaneously, the growing number of integration points and the need for unified security-policy management introduce additional challenges in orchestration, monitoring, and end-to-end visibility.

In summary, choosing the optimal deployment model is inherently multidimensional and must rest on a thorough evaluation of information-security requirements, regulatory constraints, time-to-market goals, budgetary frameworks, desired control levels, and the organisation's strategic objectives.

The contribution of this study lies in organising existing knowledge and developing a clear methodological framework for comparing cloud solutions. Future research should focus on the creation of unified tools for security and resource management in hybrid multi-cloud ecosystems, as well as on evaluating the impact of emerging technologies—artificial intelligence, machine learning, quantum computing, and edge computing—on the architectural evolution of cloud platforms and the long-term economic consequences of various deployment strategies.

References

1. Patel H., Kansara N. Cloud computing deployment models: A comparative study //International Journal of Innovative Research in Computer Science & Technology (IJIRCST). – 2021. – Vol. 9. - pp. 45-50.
2. Kim D., Lee S., Kim S. Study of campustown projects for the sustainable win-win growth of universities and communities //Sustainability. – 2023. – Vol. 15 (13). DOI: 10.3390/su151310062.
3. Pal S., Le D. N., Pattnaik P. K. Introduction to Cloud Computing //Cloud Computing Solutions: Architecture, Data Storage, Implementation and Security. – 2022. – pp. 21-38. DOI: 10.1002/9781119682318.ch2
4. AR/VR Headsets Surged During the Holiday Season 2023, According to IDC . [Electronic resource] Access mode: https://www.idc.com/getdoc.jsp?containerId=prUS51935924 (date of request: 04/14/2025)
5. Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024 . [Electronic resource] Access mode: https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024 (date of request: 04/16/2025)
6. Jawed M. S., Sajid M. A comprehensive survey on cloud computing: architecture, tools, technologies, and open issues //International Journal of Cloud Applications and Computing (IJCAC). – 2022. – Vol. 12 (1). – pp. 1-33.
7. Möller D. P. F. NIST cybersecurity framework and MITRE cybersecurity criteria //Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. – Cham : Springer Nature Switzerland. - 2023. – pp. 231-271.
8. Mishra G. A Comprehensive Review of Smart Healthcare Systems: Architecture, Applications, Challenges, and Future Directions //International Journal of Innovative Research in Technology and Science. – 2024. – Vol. 12 (2). – pp. 210-218.

9. Gill S. S. et al. AI for next generation computing: Emerging trends and future directions //Internet of Things. – 2022. – Vol. 19. DOI: 10.1016/j.iot.2022.100514.
10. Alonso J. et al. Understanding the challenges and novel architectural models of multi-cloud native applications–a systematic literature review //Journal of Cloud Computing. – 2023. – Vol. 12 (1). – pp. 6.
11. Parast F. K. et al. Cloud computing security: A survey of service-based models //Computers & Security. – 2022. – Vol. 114. DOI: 10.1016/j.cose.2021.102580.
12. AlAhmad A. S. et al. Mobile cloud computing models security issues: A systematic review //Journal of Network and Computer Applications. – 2021. – Vol. 190. DOI: 10.1016/j.jnca.2021.103152.
13. Heidari A., Jafari Navimipour N. Service discovery mechanisms in cloud computing: a comprehensive and systematic literature review //Kybernetes. – 2022. – Vol. 51 (3). – pp. 952-981.DOI:10.1108/K-12-2020-0909.
14. Abdulsalam Y. S., Hedabou M. Security and privacy in cloud computing: technical review //Future Internet. – 2021. – Vol. 14 (1). DOI: 10.3390/fi14010011.
15. Maqueira Marín J. M. et al. Cloud computing and human resource management: systematic literature review and future research agenda //Kybernetes. – 2022. – Vol. 51 (6). – pp. 2172-2191. DOI: 10.1108/K-05-2021-0420.
16. Seifert M., Kuehnel S., Sackmann S. Hybrid clouds arising from software as a service adoption: challenges, solutions, and future research directions //ACM Computing Surveys. – 2023. – Vol. 55 (11). – pp. 1-35. DOI:10.1145/3570156.
17. State of the Cloud Report. [Electronic resource] Access mode: https://info.flexera.com/CM-REPORT-State-of-the-Cloud (date of request: 05/23/2025)
18. Firdaus W., Sukmaaji A. Exploring Opportunities and Challenges in Multi-Cloud and Hybrid Cloud Implementation //Information Technology International Journal. – 2024. – Vol. 2 (2). DOI: 10.33005/itij.v2i2.30.
19. Public cloud services end-user spending worldwide from 2017 to 2025. [Electronic resource] Access mode: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/ (date of request: 04/20/2025)
20. Yanamala A. K. Y. Emerging challenges in cloud computing security: A comprehensive review //International Journal of Advanced Engineering Technologies and Innovations. – 2024. – Vol. 1 (4). – pp. 448-479.
21. Al-Ghaili A. M. et al. A review of metaverse's definitions, architecture, applications, challenges, issues, solutions, and future trends //Ieee Access. – 2022. – Vol. 10. – pp. 125835-125866.
22. Putri A. Multi-Cloud Strategies for Managing Big Data Workflows and AI Applications in Decentralized Government Systems //Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks. – 2025. – Vol. 9 (1). – pp. 1-11. DOI: 10.20535/2411-2976.22024.4-12.
23. Merseedi K. J., Zeebaree S. R. M. The cloud architectures for distributed multi-cloud computing: a review of hybrid and federated cloud environment //The Indonesian Journal of Computer Science. – 2024. – Vol. 13 (2). DOI: 10.33022/ijcs.v13i2.3811.
24. Shafiei H., Khonsari A., Mousavi P. Serverless computing: a survey of opportunities, challenges, and applications //ACM Computing Surveys. – 2022. – Vol. 54 (11). – pp. 1-32. DOI: 10.1145/3510611.
25. Madupati B. Kubernetes for Multi-Cloud and Hybrid Cloud: Orchestration, Scaling, and Security Challenges //Scaling, and Security Challenges (June 30, 2023). – 2023. DOI: 10.2139/ssrn.5076649
26. Amazon Web Services. What is Cloud Computing? [Electronic resource] Access mode: https://aws.amazon.com/what-is-cloud-computing/ (date of request: 05/23/2025)
27. What are public, private, and hybrid clouds? . [Electronic resource] Access mode: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-public-private-hybrid-clouds (date of request: 05/23/2025)
28. What is multicloud? [Electronic resource] Access mode:https://cloud.google.com/learn/what-is-multicloud (date of request: 05/20/2025)
29. What is Multi-Cloud? . [Electronic resource] Access mode: https://www.vmware.com/topics/multi-cloud (date of request: 04/126/2025)

30. The Established Cloud Deployment Models. [Electronic resource] Access mode: https://www.ibm.com/training/course/the-established-cloud-deployment-models-DL52847G (date of request: 05/10/2025)