Engineering: science, technology, and innovation.
Volume 13, 2026. E-ISSN:2313-1926

DOI: https://doi.org/10.26495/23m7xb95
Publishing Fund USS

Impact of AI on cloud infrastructure security management in IT environments: A systematic review

Impacto de la IA en la gestión de seguridad de infraestructuras cloud en entornos TI: Una revisión sistemática

Juan Diego Molina Nanfuñay[1], Leonardo Javier Guimaray Matute[1], Alberto Carlos Mendoza de los Santos[1]

[1]Universidad Nacional de Trujillo, Trujillo, La Libertad

How to cite
J. D. Molina Nanfuñay, L. J. Guimaray Matute, and A. C. Mendoza de los Santos, "Impact of AI on cloud infrastructure security management in IT environments: A systematic review". Ingeniería: ciencia, tecnología e innovación, vol. 13, 2026. https://doi.org/10.26495/23m7xb95

Article information
Received: 09/05/2025
Accepted: 30/12/2025
Published: 13/02/2026

Corresponding author
Juan Diego Molina Nanfuñay
jmolina@unitru.edu.pe

ABSTRACT: This article had the **objective** of analysing the impact of artificial intelligence on the security management of cloud infrastructures in IT environments, identifying its main applications, benefits, and challenges. **Methodology:** A systematic literature review was conducted using the PRISMA methodology, based on scientific papers and relevant studies published between 2021 and 2025 in academic databases such as Scopus and Google Scholar. **Results:** The selected studies show that AI enhances early threat detection, automates critical security processes, and optimises incident response, thereby strengthening cloud-based IT service management. However, they also reveal risks related to data privacy, loss of control, and increasing technological dependency. **Conclusions**: It is concluded that AI is a key resource for improving the protection of cloud infrastructures, provided that its implementation is carefully planned, aligned with best-practice frameworks, and supported by continuous human oversight to mitigate unforeseen vulnerabilities.

Keywords: Cybersecurity, risk management, IT service management, artificial intelligence, cloud security.

RESUMEN: El presente artículo tuvo como **objetivo** analizar el impacto de la inteligencia artificial en la gestión de la seguridad de infraestructuras cloud en entornos de TI, identificando sus principales aplicaciones, beneficios y desafíos. **Metodología**: Se realizó una revisión sistemática de la literatura, siguiendo la metodología PRISMA, a partir de artículos científicos y estudios relevantes publicados entre 2021 y 2025 en bases de datos académicas como Scopus y Google Scholar. **Resultados:** Los estudios seleccionados evidencian que la IA mejora la detección temprana de amenazas, automatiza procesos de seguridad críticos y optimiza la respuesta ante incidentes, contribuyendo al fortalecimiento de la gestión de servicios TI en la nube. Sin embargo, también revelan riesgos asociados a la privacidad de los datos, la pérdida de control y la creciente dependencia tecnológica. **Conclusiones:** Se concluye que la IA constituye un recurso clave para incrementar la protección de las infraestructuras cloud, siempre que su implementación se realice de manera planificada, bajo marcos de buenas prácticas y con una supervisión humana constante que mitigue la aparición de vulnerabilidades no previstas.

Palabras clave: Ciberseguridad, gestión de riesgos, gestión de servicios TI, inteligencia artificial, seguridad en la nube.

1. INTRODUCTION

The cloud approach is gaining acceptance as a fundamental component in the digital transformation process of modern organisations, facilitating the adoption of advanced technologies that respond to the needs of a business environment that is transforming and constantly evolving [1]. In this context, cloud has changed its initial role from a simple technological alternative to an indispensable requirement for the successful adoption of AI tools, as it acts as the basic infrastructure for their operation. Cloud computing, AI and the synergy between the two have revolutionised the way information systems operate, moving from rigid architectures to dynamic and adaptable environments designed to accelerate model training, offer real-time inference and maintain continuous learning systems.

With the expansion of the cloud environment, its security has become a primary concern for organisations around the world. The large amount of information stored and processed in cloud environments makes security an issue that requires constant attention from organisations in order to preserve data integrity [2]. Cloud security also covers a number of areas, including data encryption to ensure confidentiality, network security to prevent access by unauthorised agents, identity management to control who can access which resources, and, finally, regulatory compliance to certify that applicable standards and regulations are being met [3].

AI also stands out as a technological solution that can transform what is known about security management.
Thanks to large-scale data training, AI continuously learns and improves its ability to process information and make predictions based on feedback and comparison [4]. This prior training gives it an advantage over human workers in detecting advanced phishing attacks, malware, ransomware, DDoS attacks, and anomalous behaviour by users interacting with the system [2].

Taking the above into account, this systematic literature review (SLR) poses the following general research question: What are the benefits of integrating AI into cloud infrastructure security management within IT environments?
Based on this general question, the SLR aims to answer the following specific questions:

- What are the main applications of AI in cloud infrastructure security management within IT environments?
- What benefits and challenges arise from the implementation of AI in cloud security management?
- What recommendations can be made to improve the integration of AI into cloud infrastructure security management?

Although several papers on cloud security and artificial intelligence have been published in recent years, many of them focus on specific use cases, domains, or technologies, resulting in a fragmented view of the current state of knowledge [2], [5]. In this regard, a systematic review of the literature is necessary to synthesise the available evidence, organise scattered findings, identify research gaps, and offer a structured perspective that can serve as a basis for decision-making in the management of IT services on AI-supported cloud infrastructures.

The scope of this review focused on specific aspects of security management in cloud infrastructures where AI has a significant impact, including identity and access management, rapid response to security incidents, efficient vulnerability analysis,

security monitoring and logging, as well as regulatory compliance and risk management.

Security in cloud infrastructures has emerged as a relevant field of research, along with studies addressing the challenges of this environment, which include both internal and external threats, personal data protection, and compliance with various regulatory requirements [2]. Previous research has explored the progressive application of AI in the cybersecurity environment, highlighting its ability to integrate data from multiple cloud services and provide a holistic view of existing risks and vulnerabilities [5]. On the other hand, ITIL v4, a framework of IT best practices, explicitly recognises IT security management as an essential practice within the IT service management model, which must be considered in all planning activities and integrated across all practices and services offered by the organisation.

2. METHODS AND COMPUTATIONAL METHODOLOGY

This research conducted a systematic literature review focused on the impact of artificial intelligence technologies for security management in cloud infrastructures within IT environments. The study adopted a qualitative documentary approach, with a systematic review design, based on the PRISMA guidelines. The population consisted of scientific articles and papers indexed in the Scopus and Google Scholar databases, published between 2021 and 2025. From this population, a final sample of nine studies was obtained, selected using explicit inclusion and exclusion criteria. The categories of analysis were grouped into four dimensions: automation of incident detection and response, optimisation of cloud protection, improvement of risk and privacy management, and challenges and opportunities in cloud security.

2.1 Methodological foundations

A systematic review allows the explicit and orderly organisation of available evidence on a specific topic, facilitating the formulation of more precise research questions based on a structured and transparent process [6]. This study followed the recommendations of the PRISMA guideline, which guides the identification, selection, critical evaluation, and synthesis of studies, contributing to improving the methodological quality of systematic reviews [7].

2.2 Search strategy

The search for information was conducted in two academic databases with broad coverage:

Scopus and Google Scholar. Publications between 2021 and 2025 were considered in order to collect the most recent contributions on the use of AI in cloud security management. The search was performed in the title, abstract and keyword fields, prioritising studies related to cybersecurity, cloud services, artificial intelligence and IT service management.

2.3 Search terms

To construct the search strategy, English keywords related to artificial intelligence, cloud computing, machine learning, cloud security and information technology were combined. These words were linked using logical operators (AND) in order to define the intersection between AI and security in cloud infrastructures.

2.4 Database search formulas

Scopus: (TITLE-ABS-KEY ("artificial intelligence" AND "cloud services") AND TITLE-ABS-KEY (network AND security) AND TITLE-ABS-KEY (machine AND learning) AND TITLE-ABS-KEY (cloud AND security))

Google Scholar: "artificial intelligence" AND "cloud services" AND "network security" AND "machine learning" AND "cloud security" AND "information technologies"

2.5 Inclusion and exclusion parameters

Inclusion parameters

Articles published between 2021 and 2025 related to the fields of computer science, engineering, decision-making, and business studies were included. The studies had to explicitly address topics related to artificial intelligence, machine learning, cloud computing, cloud services, cloud security, cybersecurity, data protection, or information security. Furthermore, only articles from scientific journals and papers presented at academic conferences were considered.

Exclusion parameters

Duplicate documents and those that did not directly address the relationship between cloud services, artificial intelligence, machine learning, and cloud security were excluded. Non-academic sources (technical reports, blog posts, informational material), papers without full access, and publications outside the established time frame (prior to 2021 or after 2025) were also discarded.

2.6 Study selection process

Initially, 303 articles were identified by searching the two databases mentioned above. The inclusion and exclusion criteria were then applied sequentially:

Identification

In the identification phase, 303 records were retrieved: 64 from Scopus and 239 from Google Scholar. After removing duplicates and conducting an initial review of titles and abstracts, studies that did not meet the inclusion criteria were discarded, leaving 33 studies for more detailed evaluation.

Screening

In the screening phase, abstracts and keywords were critically read, allowing 25 articles with greater thematic relevance to be selected. Subsequently, in the eligibility stage, the full text of these 25 documents was obtained and the inclusion and exclusion criteria were applied again. In this phase, 10 articles were excluded because they focused on technological contexts that did not directly involve cloud infrastructures, because they dealt with AI without linking it to security, or because they did not provide sufficient information on cloud security management.

Text evaluation

Full access was obtained to 25 articles, 10 of which were excluded for not meeting the specific criteria of cloud services and security and artificial intelligence.

Final selection

As a result of this process, a final sample of 9 articles was obtained that adequately addressed the research questions and the objective of the systematic review. This procedure is summarised in the PRISMA flow diagram presented in Figure 1, which details the phases of identification, screening, eligibility, and final selection of studies, as well as a summary of the records identified in Table 1.

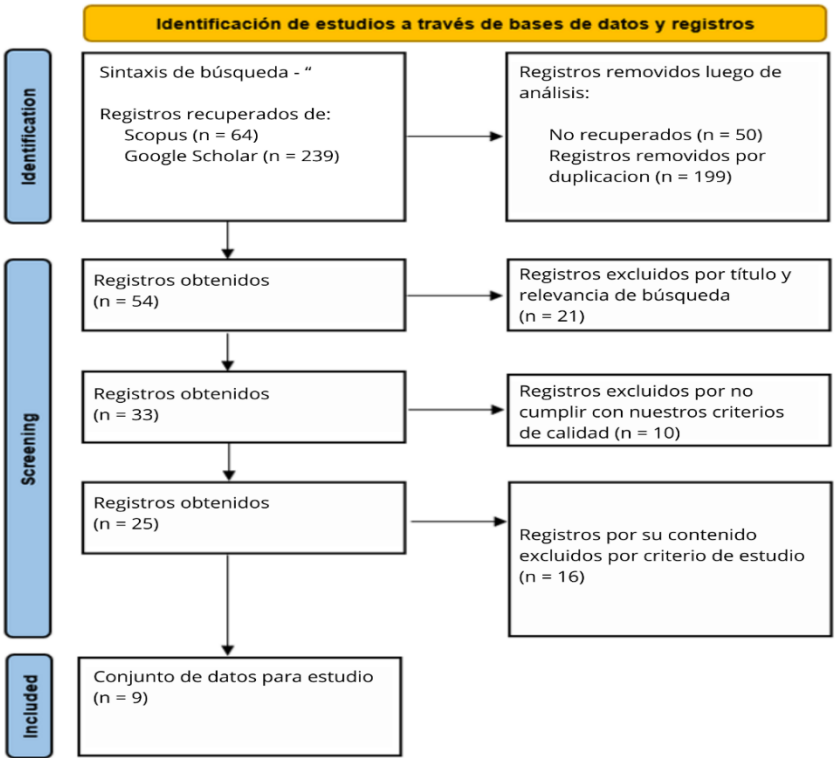

Figure 1. Four-level PRISMA flow diagram.
Source: own elaboration.

Table 1. Number of records identified through database searches.
Source: own elaboration.

Database	Number of articles
Scopus	64
Google Scholar	239
Total	303

Source: own elaboration.

3. RESULTS

This section presents the findings obtained from the systematic review of the literature, after applying the inclusion and exclusion criteria described in the methodology section. From a total of 303 records identified in Scopus and Google Scholar, a sample of nine articles was finally selected that address the relationship between artificial intelligence and security management in cloud infrastructures from different application contexts (general cybersecurity, cloud services, health, communications platforms, and incident management).

As shown in Table 2, the studies analysed are distributed between 2021 and 2025 and include proposals focused on attack detection, cloud service protection, preservation of sensitive data privacy, and incident management efficiency. Based on the content analysis of these studies, the findings were organised into four dimensions directly related to the research questions posed: automation of incident detection and response, optimisation of cloud protection, improvement in risk and privacy management, and challenges and opportunities in cloud security

Table 2. Selected articles. Source: own elaboration.

No.	Year	Author(s)	Database	Title
1	2023	Mehmood, M., Amin, R., Muslam, M. M. A., Xie, J., Aldabbas, H.	Scopus	Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning
2	2024	Dutta, J., Puthal, D.	Scopus	Advancing eHealth in Society 5.0: A Fuzzy Logic and Blockchain-Enhanced Framework for Integrating IoMT, Edge, and Cloud With AI
3	2024	Altowaijri, S. M., El Touati, Y.	Scopus	Securing Cloud Computing Services with an Intelligent Preventive Approach
4	2023	Azamuddin, W. M. H., Aman, A. H. M., Sallehuddin, H., Abualsaud, K., Mansor, N.	Scopus	The Emerging of Named Data Networking: Architecture, Application, and Technology
5	2021	Dinh, P. T., Park, M.	Scopus	R-EDoS: Robust Economic Denial of Sustainability Detection in an SDN-Based Cloud through Stochastic Recurrent Neural Network
6	2021	Mershad, K., Dahrouj, H., Sarieddeen, H., Shihada, B., Al-Naffouri, T., Alouini, M.-S.	Scopus	Cloud-Enabled High-Altitude Platform Systems: Challenges and Opportunities
7	2021	Seh, A. H., Al-Amri, J. F., Subahi, A. F., Agrawal, A., Kumar, R., Khan, R. A.	Scopus	Machine learning based framework for maintaining privacy of healthcare data
8	2022	Vegas-Capristan, N., Soto-Alarcón, A.	Google Scholar	La eficiencia de la gestión de incidencias en Cloud Services
9	2025	Eneque Suarez, V. G.	Google Scholar	Análisis comparativo de servicios y funcionalidades de AWS, Azure y Elastic Cloud en el entorno de Cloud Computing

Overall, the results show that AI provides advanced capabilities for continuous monitoring of the cloud environment, early identification of complex threats and reduced response times, but it also introduces new vulnerabilities due to its dependence on large volumes of data and more complex technical architectures.

3.1 Automation of incident detection and response

In relation to the first research question, linked to the main applications of AI in cloud infrastructure security management, studies agree that its most immediate contribution lies in the automation of incident detection and response.

In [8], the authors propose a scheme for detecting privilege escalation in cloud environments based on supervised learning algorithms (Random Forest, AdaBoost, LightGBM), capable of processing large volumes of records and differentiating more

effectively between legitimate and malicious activities. Their results show a substantial improvement over traditional approaches based on static rules, both in reducing false positives and in the reaction time to suspicious events.

Complementarily, [9]-[11] address Economic Denial of Sustainability (EDoS) attacks in SDN-supported clouds, proposing a recurrent neural network model that analyses traffic and distinguishes between legitimate increases and malicious patterns of resource consumption. This approach demonstrates how AI can anticipate attacks that seek to exhaust the economic capacity of cloud services, beyond mere technical saturation.

Studies focused on incident management in cloud services [12], [13] also highlights the usefulness of AI for automatically classifying, prioritising and routing incidents, reducing the operational burden on IT staff and enabling responses that are more aligned with the actual impact on services. Overall, this evidence shows that AI not only speeds up the identification of threats, but also helps to structure response flows that are more consistent with the criticality of each incident.

However, while AI speeds up the identification of threats at speeds unattainable by the human eye, it also runs the risk of becoming anchored to predefined patterns that may overlook the unexpected. On the one hand, models increase accuracy in known scenarios; on the other, they can become fragile in the face of novel attacks or drastic changes in user behaviour, requiring continuous model updates and ongoing expert supervision.

3.2 Cloud protection optimisation

In terms of the benefits of AI for the protection and availability of cloud services, the studies reviewed show that its integration strengthens the resilience of distributed and complex infrastructures.

In [10], cloud-enabled high-altitude platform systems (HAPS) are analysed, where AI is used to anticipate communication failures, manage network resources and optimise service continuity in remote or hard-to-reach contexts. The use of learning algorithms allows for dynamic adjustment of resource allocation and mitigation of interruptions before they result in outages visible to the end user.

From another perspective, [11] show that deep learning can reinforce the economic sustainability of cloud services by identifying anomalous usage patterns that compromise availability. Their proposal not only protects the infrastructure, but also helps to preserve service quality and control the operating costs associated with persistent attacks.

For their part, [14], [15] propose a framework for eHealth in Society 5.0 that integrates IoMT, edge and cloud with AI, emphasising the need for protection and service continuity mechanisms to accompany the growth in the volume of clinical data and the number of connected devices. In this scenario, AI acts as an orchestrating layer that decides what information is processed at the edge, what is sent to the cloud, and how security resources are prioritised to maintain system availability and integrity.

In short, the evidence suggests that AI strengthens the availability of cloud services when traditional networks succumb to the pressure of volumetric attacks or extreme operating conditions, although it introduces complexity into already dense architectures and demands additional computing capabilities that must be carefully planned.

3.3 Improvements in risk management and privacy

Regarding risk management and privacy, which are closely linked to the second research question on the benefits and challenges of AI, studies emphasise a permanent tension between the need for data and the protection of sensitive information.

In [12], the authors propose a machine learning-based framework for maintaining the privacy of health data, in which models detect unusual access and atypical behaviour in

electronic health records. AI can distinguish between legitimate use and potential abuse with a level of accuracy that is difficult to achieve through manual inspection, thereby strengthening the protection of highly sensitive data. However, this improvement relies on access to large volumes of clinical information, which increases the potential impact of a security breach if controls fail.

The contributions of [13] show that the efficiency of incident management in cloud services also depends on how incidents are documented, classified and fed back. The incorporation of advanced analytics and AI into these processes makes it possible to identify recurring risk patterns and adjust security and business continuity policies, contributing to more mature operational risk management.

Overall, the findings indicate that AI strengthens the protection of sensitive data when conventional defences falter, but in doing so it requires a flow of information that threatens confidentiality itself and forces a rethinking of data governance strategies, service level agreements and regulatory compliance mechanisms.

3.4 Challenges and opportunities in cloud security

Finally, in relation to the third research question, aimed at identifying recommendations and opportunities for integrating AI into cloud infrastructure security management, the studies reviewed reveal an ambivalent scenario: AI is simultaneously presented as a protection tool and a source of new vulnerabilities.

[14] analyse the Named Data Networking (NDN) paradigm and highlight its potential to improve privacy and efficient content distribution through caching. However, they warn that data fragmentation and replication can multiply attack surfaces if not accompanied by rigorous authentication, authorisation and encryption policies, especially when combined with AI algorithms for traffic routing and optimisation.

In the context of eHealth, [15] emphasise that the integration of AI, edge and cloud opens up opportunities to strengthen security — for example, by detecting anomalous behaviour in real time — but at the same time raises the demands for governance, algorithmic transparency and accountability in the processing of clinical data.

Finally, comparative studies of large-scale cloud provider services and functionalities show that leading platforms are increasingly incorporating AI-based security services, but with significant differences in monitoring, automation, and management capabilities. These differences condition the possibilities for organisations to implement AI-based security strategies consistently in multi-cloud environments.

The promise of AI to shield cloud environments therefore coexists with the threat of new vulnerabilities arising from its intensive use, reinforcing the need for reference frameworks such as ITIL v4 and constant human supervision to maintain the balance between automation, control and responsibility.

4. DISCUSSION

The results of this systematic review show that the integration of AI into cloud infrastructure security management is not an isolated phenomenon, but a cross-cutting trend that spans different domains (business services, healthcare, communications platforms, incident management). Organising the findings into four dimensions allowed us to respond to the research questions in a coherent manner, showing that AI applications focus on automating incident detection and response, optimising service protection and availability, strengthening risk management, and opening up new opportunities, but also challenges, for cloud security.

Compared to previous studies, the findings of [8] and [11] corroborate the idea, already suggested in the technical literature on cybersecurity, that rule-based approaches are

insufficient in dynamic cloud environments and must be complemented with machine learning models capable of adapting to changing attack patterns. However, this review adds value by showing that solutions originally designed for specific problems (privilege escalation, EDoS) converge on the same axis: the need for detection and response systems capable of operating in near real time and integrating with IT service management processes.

Likewise, the study made by [10] on HAPS platforms and the eHealth framework proposed by [15] broaden the traditional discussion of cloud security, normally focused on data centres and business services, to scenarios where service continuity has critical impacts on communication and people's health. When comparing these studies with approaches focused on healthcare data privacy [12] and incident management in cloud services [13], it can be seen that, beyond differences in context, there is a consensus around AI as a support for rapid decision-making in high-risk situations, but also an explicit recognition of the increased technical complexity and risk in the event of failures.

From a practical perspective, the results suggest several implications for organisations that manage cloud infrastructures. Firstly, the adoption of AI solutions for security should not be limited to incorporating isolated tools, but should be integrated into an IT service management model, such as that proposed by ITIL v4, which allows for the articulation of automated detection, incident response, change management and continuous improvement. Secondly, there is a clear need to strengthen data governance: AI requires large volumes of information to train and improve its models, but this must be balanced with clear policies on data minimisation, access segmentation and regulatory compliance.

Thirdly, the findings reinforce the importance of maintaining human oversight of the most critical processes. Although AI models can surpass the human eye in speed and analytical capacity, final decisions in high-impact incidents, such as unauthorised access to clinical data [12] or loss of availability in essential services [10], [11], must continue to be made by specialised teams that assess the context, weigh the risks, and avoid disproportionate automatic responses.

The review also highlights several limitations. Firstly, the number of studies that meet the inclusion criteria is small (9 articles), which prevents the results from being generalised to all organisational realities and sectors. Secondly, the review was restricted to two databases (Scopus and Google Scholar) and a limited time frame (2021–2025), so it is possible that relevant research exists in other repositories or outside this time frame. Thirdly, the heterogeneity of the designs, contexts, and metrics used in the selected studies did not allow for a quantitative meta-analysis, so the results are presented in the form of a narrative synthesis.

These limitations open up clear avenues for future research: expanding the search to other databases specialising in security and cloud computing, incorporating literature in other languages, delving deeper into case studies that detail the concrete implementation of AI solutions in real organisations, and moving towards comparative analyses that evaluate the performance of different AI approaches under similar conditions.

In summary, the debate among the studies reviewed shows that AI is consolidating its position as a driver of transformation in cloud infrastructure security management, but its contribution is neither neutral nor automatic. The benefits in terms of automation, proactive detection, and resilience must be balanced with careful management of privacy, data governance, and technological dependency. In this scenario, the contribution of this review lies in offering a structured overview of the applications, benefits, challenges and opportunities of AI in cloud security, which serves as input both for decision-making in IT service management and for the design of new research in the field.

5. CONCLUSIONS

The systematic review allowed the analysis of the impact of artificial intelligence on cloud infrastructure security management in IT environments, based on nine studies that address this phenomenon from different application contexts. Overall, the evidence reviewed shows that AI has become a key component in strengthening cloud security by providing advanced capabilities for continuous monitoring, early threat detection, and incident response automation, which contributes to improving the operational efficiency and resilience of services on cloud infrastructures.

The findings confirm that the most relevant AI applications focus on the proactive identification of complex attacks, the mitigation of incidents that compromise the availability and economic sustainability of services, and the reinforcement of sensitive data protection in critical sectors such as healthcare. The combination of machine learning algorithms, neural networks, and advanced analytical approaches makes it possible to distinguish more accurately between legitimate and malicious behaviour, reduce false positives, and prioritise security events according to their impact on IT services. In this way, AI provides significant support for cloud security management from a comprehensive service management perspective.

However, the integration of AI also introduces significant challenges that cannot be ignored. The intensive use of data to train and adjust models increases the risks associated with privacy and confidentiality of information, while also increasing the technical complexity of cloud architectures and dependence on specialised solutions. If not managed properly, these factors can lead to new attack surfaces, greater exposure to configuration failures, or automated decisions that do not sufficiently consider the business context. In this sense, AI is not an isolated solution, but an element that must be articulated with robust data governance policies, best practice frameworks such as ITIL v4, and clear mechanisms of responsibility for information processing.

Based on the above, it can be concluded that the effective integration of AI into cloud infrastructure security management requires a balance between automation and human control. Organisations need to combine intelligent monitoring, detection and response tools with specialised teams capable of supervising models, interpreting their results, adjusting risk thresholds and making informed decisions in high-impact incidents. It is also essential to strengthen the ongoing training of IT staff in cybersecurity, data governance and the ethical use of AI, as well as to carefully evaluate the capabilities of cloud providers when operating multi-cloud or hybrid environments.

Finally, although the results of our review offer a structured view of the applications, benefits, challenges and opportunities of AI in cloud security, they also highlight the need for further research. Future research could expand the number of databases consulted, incorporate case studies in organisations from different sectors, compare the performance of different AI approaches under similar conditions, and delve deeper into aspects such as model explainability, algorithmic risk management, and the impact of AI on decision-making within IT service management. These efforts will consolidate and refine the conclusions presented here, contributing to a more mature and responsible adoption of AI in cloud infrastructure protection.

6. ABOUT THE ARTICLE

Funding: This study did not receive external funding and was developed entirely in the academic sphere.

Acknowledgements: The authors would like to thank the *Gestión de Servicios de TIC* [ICT Service Management course], Alberto Carlos Mendoza de los Santos of the National University of Trujillo for the academic framework that enabled the development of this study, as well as the guidance provided by the course instructor.

Author contributions:

Juan D. Molina: Research, conceptualisation of the study, drafting of the original manuscript, preparation of tables, and review of the consistency of the manuscript.

Leonardo J. Guimaray: Research, drafting of the original manuscript, figure creation, table formatting, and final document formatting.

Alberto C. Mendoza: Project supervision, critical review of the manuscript, and validation of the final version of the content. All authors have read and agree with the published version of the manuscript.

Conflicts of Interest: The authors declare that they have no financial, academic, or personal conflicts of interest that could have influenced the development or results of this manuscript.

REFERENCES

[1] L. F. Mero-Terán, and E. J. Macías-Arias, "Technological models of cloud computing in the digital transformation of higher education: A systematic literature review," *593 Digital Publisher CEIT*, vol. 10, no. 1, pp. 29–53, Jul. 2025. https://doi.org/10.33386/593DP.2025.1.2704

[2] imedia,"Cómo la IA puede mejorar la seguridad en Internet de las cosas," imediacomunicacion.com. Accessed: Jul. 1, 2023. [Online]. Available: https://www.imediacomunicacion.com/como-la-ia-puede-ayudar-a-mejorar-la-seguridad-en-internet-de-las-cosas-iot-2/

[3] S. Fernández, and L. Campo, "Inteligencia artificial al servicio de la seguridad en la nube," keepler.io. Accessed: Jul. 1, 2023. [Online]. Available: https://keepler.io/es/2021/06/02/inteligencia-artificial-al-servicio-de-la-seguridad-en-la-nube/

[4] NUTANIX, "¿Qué es la inteligencia artificial?," nutanix.com. Accessed: Jul. 1, 2023. [Online]. Available: https://www.nutanix.com/es/info/artificial-intelligence

[5] Microsoft "¿Qué es la inteligencia artificial para la ciberseguridad?," microsoft.com. Accessed: Jul. 1, 2023. [Online]. Available: https://www.microsoft.com/es-es/security/business/security-101/what-is-ai-for-cybersecurity

[6] M. Petticrew, and H. Roberts, *Systematic reviews in the social sciences: A practical guide*, Chichester, England: Wiley-Blackwell, 2005. https://onlinelibrary.wiley.com/doi/book/10.1002/9780470754887

[7] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, Jan. 2021. https://doi.org/10.1136/bmj.n71

[8] M. Mehmood, R. Amin, M. M. Ali Muslam, J. Xie, and H. Aldabbas, "Privilege escalation attack detection and mitigation in cloud using machine learning," *IEEE Access*, vol. 11, pp. 46561–46576, May. 2023. https://doi.org/10.1109/ACCESS.2023.3273895

[9] S. M. Altowaijri, and Y. El Touati, "Securing cloud computing services with an intelligent preventive approach," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 3, pp. 13998–14005, Jun. 2024. https://doi.org/10.48084/ETASR.7268

[10] K. Mershad, H. Dahrouj, H. Sarieddeen, B. Shihada, T. Al-Naffouri, and M.-S. Alouini, "Cloud-enabled high-altitude platform systems: Challenges and opportunities," *Front. Comms. Net.*, vol. 2, p. 716265, Jul. 2021. https://doi.org/10.1109/ACCESS.2021.3061601

[11] P. T. Dinh, and M. Park, "R-EDoS: Robust economic denial of sustainability detection in an SDN-based cloud through stochastic recurrent neural network," *IEEE Access*, vol. 9, pp. 35057–35074, Feb. 2021. https://ieeexplore.ieee.org/document/9360795

[12] A. Hussain Seh, J. F. Al-Amri, A. F. Subahi, A. Agrawal, R. Kumar, and R. Ahmad Khan, "Machine learning based framework for maintaining privacy of healthcare data," *Intell. Autom. Soft Comput.*, vol. 29, no. 3, pp. 697–712, Jul. 2021. https://www.techscience.com/iasc/v29n3/43042

[13] N. Vegas-Capristan, and A. Soto-Alarcón, "Eficiencia de la gestión de incidencias en cloud services: una revisión sistemática," *Revista Campus,* vol. 27, no. 34, pp. 197–208, Nov. 2022. https://doi.org/10.24265/campus.2022.v27n34.03

[14] W. M. Hazwan Azamuddin, A. H. Mohd Aman, H. Sallehuddin, K. Abualsaud, and N. Mansor, "The emerging of named data networking: Architecture, application, and technology," *IEEE Access*, vol. 11, pp. 23620–23633, Feb. 2023. https://ieeexplore.ieee.org/document/10038676

[15] J. Dutta, and D. Puthal, "Advancing eHealth in Society 5.0: A Fuzzy Logic and Blockchain-Enhanced Framework for Integrating IoMT, Edge, and Cloud With AI," *IEEE Access*, vol. 12, pp. 195710-195730, Dec. 2024. https://ieeexplore.ieee.org/document/10810439