Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2026,
Volumen 10, Número 2.

https://doi.org/10.37811/cl_rcm.v10i2

APLICACIONES DEL MACHINE LEARNING PARA LA DETECCIÓN DE ANOMALÍAS EN ENTORNOS CLOUD.

APPLICATIONS OF MACHINE LEARNING FOR ANOMALY DETECTION IN CLOUD ENVIRONMENTS

Maria Teodolinda Ortega Ovalle
Universidad de Panamá

DOI: https://doi.org/10.37811/cl_rcm.v10i2.23655

Aplicaciones del machine learning para la detección de anomalías en entornos cloud.

Maria Teodolinda Ortega Ovalle[1]

maria.ortegao@up.ac.pa

https://orcid.org/0009-0000-3629-9751

Universidad de Panamá

Panamá

RESUMEN

La detección de anomalías en entornos cloud constituye un desafío fundamental para garantizar la seguridad, disponibilidad y confiabilidad de los servicios digitales. El objetivo de este trabajo es analizar las aplicaciones del machine learning en la identificación de comportamientos inusuales dentro de infraestructuras de computación en la nube. Se implementó una metodología de revisión documental con enfoque cualitativo, explorando estudios recientes sobre algoritmos supervisados, no supervisados y de deep learning aplicados a la detección de anomalías. Los principales hallazgos evidencian que los modelos basados en clustering y redes neuronales profundas ofrecen mayor precisión en la identificación de patrones anómalos, mientras que los enfoques híbridos permiten reducir falsos positivos. Se concluye que el machine learning representa una herramienta clave para fortalecer la seguridad en entornos cloud, aunque persisten retos relacionados con la escalabilidad, la interpretabilidad de los modelos y la integración con sistemas de monitoreo en tiempo real.

***Palabras clave**:* Machine learning, detección de anomalías, cloud computing, seguridad informática, inteligencia artificial.

[1] Autor principal
Correspondencia: maria.ortegao@up.ac.pa

Applications of Machine Learning for Anomaly Detection in Cloud Environments

ABSTRACT

Anomaly detection in cloud environments is a fundamental challenge to ensure the security, availability, and reliability of digital services. This work aims to analyze the applications of machine learning in identifying unusual behaviors within cloud computing infrastructures. A qualitative documentary review methodology was implemented, exploring recent studies on supervised, unsupervised, and deep learning algorithms applied to anomaly detection. The main findings show that clustering-based models and deep neural networks provide higher accuracy in identifying anomalous patterns, while hybrid approaches help reduce false positives. It is concluded that machine learning is a key tool to strengthen security in cloud environments, although challenges remain regarding scalability, model interpretability, and integration with real-time monitoring systems.

Keywords: Machine learning, anomaly detection, cloud computing, cybersecurity, artificial intelligence.

Artículo recibido 02 abril 2026
Aceptado para publicación: 30 abril 2026

INTRODUCCIÓN

La computación en la nube ha revolucionado la manera en que las organizaciones gestionan sus recursos tecnológicos, ofreciendo escalabilidad, flexibilidad y reducción de costos. Sin embargo, esta transformación también ha incrementado la complejidad de los sistemas y, con ello, los riesgos asociados a la seguridad y confiabilidad de los servicios. El problema de investigación que se aborda en este artículo es la necesidad de contar con mecanismos eficaces para la detección temprana de anomalías en entornos cloud, considerando que los métodos tradicionales basados en reglas estáticas resultan insuficientes frente a la dinámica y volumen de datos actuales.

La relevancia de este estudio radica en que la detección de anomalías es esencial para prevenir ataques cibernéticos, fallos de configuración y pérdidas de información, aspectos que impactan directamente en la continuidad del negocio y la confianza de los usuarios. Teóricamente, el trabajo se sustenta en los postulados del aprendizaje automático, particularmente en algoritmos de clasificación, clustering y redes neuronales, que permiten identificar patrones inusuales en grandes volúmenes de datos.

Diversos estudios previos han demostrado la eficacia del machine learning en la detección de intrusiones y anomalías en sistemas distribuidos (Chandola, Banerjee, & Kumar, 2009; Ahmed, Mahmood, & Hu, 2016). Sin embargo, aún existen vacíos relacionados con la escalabilidad de los modelos y su capacidad de adaptación a entornos cloud heterogéneos. Este artículo aporta una revisión crítica de las aplicaciones más recientes, destacando las ventajas y limitaciones de cada enfoque.

El contexto de la investigación se enmarca en la creciente adopción de servicios cloud por parte de empresas de todos los sectores, lo que ha generado un aumento en la superficie de ataque y en la necesidad de mecanismos de seguridad avanzados. El objetivo general del trabajo es analizar las aplicaciones del machine learning para la detección de anomalías en entornos cloud, identificando los principales enfoques metodológicos y sus resultados.

METODOLOGÍA

El presente estudio se desarrolló bajo un enfoque cualitativo de tipo exploratorio-descriptivo, sustentado en una revisión documental sistemática de literatura científica publicada entre 2009 y 2024. La elección de este enfoque responde a la necesidad de comprender las aplicaciones del *machine learning* en la detección de anomalías en entornos cloud desde una perspectiva amplia, considerando tanto avances

teóricos como implementaciones prácticas. Según Kitchenham y Charters (2007), la revisión sistemática permite identificar, evaluar e interpretar toda la investigación relevante disponible sobre un tema específico, garantizando rigor metodológico y replicabilidad.

El diseño de investigación fue no experimental y transversal, dado que se trabajó con fuentes secundarias sin manipulación de variables y se analizaron estudios disponibles en un periodo determinado. La población de estudio estuvo conformada por artículos científicos indexados en bases de datos como IEEE Xplore, ACM Digital Library, ScienceDirect y SpringerLink. Se aplicó un muestreo intencional, seleccionando cuarenta documentos relevantes según criterios de inclusión y exclusión. Los criterios de inclusión consideraron publicaciones en inglés o español que abordaran detección de anomalías en entornos cloud mediante técnicas de *machine learning*, siempre que fueran artículos con acceso completo y publicados en revistas arbitradas. Por otro lado, se excluyeron documentos sin revisión por pares y estudios centrados exclusivamente en detección de anomalías en redes tradicionales sin relación con cloud computing.

Las técnicas de recolección de datos consistieron en la revisión documental y el análisis comparativo de enfoques metodológicos descritos en los artículos seleccionados. Se empleó una matriz de análisis para organizar la información, clasificando los estudios según tipo de algoritmo (supervisado, no supervisado, híbrido, *deep learning*) y resultados obtenidos. Este procedimiento se fundamenta en trabajos previos como el de Chandola, Banerjee y Kumar (2009), quienes realizaron un análisis exhaustivo de técnicas de detección de anomalías, y el de Ahmed, Mahmood y Hu (2016), que revisaron métodos aplicados específicamente en el ámbito de la seguridad de redes.

En cuanto a las consideraciones éticas, se respetaron los principios de integridad académica, citando adecuadamente todas las fuentes consultadas conforme a las normas APA 7. No se trabajó con datos sensibles ni con participantes humanos, por lo que no fue necesario un consentimiento informado. Finalmente, se reconocen como limitaciones la dependencia de fuentes secundarias y la posible falta de uniformidad en los criterios de evaluación de resultados entre los estudios revisados. Sin embargo, esta metodología permite ofrecer una visión crítica y actualizada sobre el estado del arte en la aplicación del *machine learning* para la detección de anomalías en entornos cloud.

Tabla 1 Criterios de inclusión y exclusión de estudios revisados

CRITERIO	DESCRIPCIÓN
INCLUSIÓN	Artículos en inglés o español, publicados en revistas arbitradas, con acceso completo, relacionados con detección de anomalías en cloud mediante ML
EXCLUSIÓN	Documentos sin revisión por pares, estudios centrados en redes tradicionales sin relación con cloud

MARCO TEÓRICO

La detección de anomalías es un campo de investigación que ha evolucionado significativamente en las últimas dos décadas, especialmente con la incorporación de técnicas de *machine learning*. Chandola, Banerjee y Kumar (2009) definen la anomalía como cualquier patrón en los datos que no se ajusta al comportamiento esperado, y señalan que su identificación es crucial en áreas como la seguridad informática, el monitoreo de sistemas y la detección de fraudes. En el contexto de la computación en la nube, la detección de anomalías adquiere mayor relevancia debido a la naturaleza distribuida y dinámica de los entornos cloud, donde los datos se generan en tiempo real y en volúmenes masivos.

El *cloud computing* se caracteriza por ofrecer servicios bajo demanda, escalabilidad y flexibilidad, pero también introduce riesgos relacionados con la seguridad y la confiabilidad de los sistemas. Según Mell y Grance (2011), la nube se fundamenta en modelos de servicio como IaaS, PaaS y SaaS, cada uno con vulnerabilidades específicas que requieren mecanismos de monitoreo avanzados. En este sentido, el *machine learning* se presenta como una alternativa a los métodos tradicionales basados en reglas, ya que permite identificar patrones ocultos y adaptarse a cambios en los datos.

Los algoritmos supervisados, como las máquinas de soporte vectorial y los árboles de decisión, han demostrado eficacia en la clasificación de comportamientos normales y anómalos, siempre que se disponga de conjuntos de datos etiquetados (Zhang et al., 2019). Sin embargo, en entornos cloud, la disponibilidad de datos etiquetados es limitada, lo que ha impulsado el uso de enfoques no supervisados como el clustering y la detección basada en densidad. Ahmed, Mahmood y Hu (2016) destacan que los métodos no supervisados son especialmente útiles para identificar anomalías desconocidas, aunque presentan el reto de generar un mayor número de falsos positivos.

El *deep learning* ha emergido como una tendencia clave en la detección de anomalías en la nube. Modelos como las redes neuronales convolucionales y las redes recurrentes permiten analizar secuencias de datos y detectar patrones complejos asociados a ataques o fallos de configuración (Xu et al., 2018). No obstante, la interpretabilidad de estos modelos sigue siendo un desafío, lo que limita su adopción en entornos donde la transparencia es un requisito.

Asimismo, se han desarrollado enfoques híbridos que combinan técnicas supervisadas y no supervisadas, buscando aprovechar las ventajas de ambos paradigmas. Según Ribeiro et al. (2020), los sistemas híbridos permiten reducir la tasa de falsos positivos y mejorar la precisión en la detección de anomalías, aunque requieren mayor capacidad computacional y un diseño más complejo.

En síntesis, el marco teórico evidencia que la detección de anomalías en entornos cloud mediante *machine learning* se sustenta en tres grandes enfoques: supervisado, no supervisado y profundo, cada uno con fortalezas y limitaciones. La literatura revisada muestra que la tendencia actual se orienta hacia modelos híbridos y soluciones basadas en *deep learning*, capaces de adaptarse a la dinámica de los entornos cloud y de ofrecer mayor precisión en la identificación de comportamientos anómalos.

RESULTADOS Y DISCUSIÓN

La revisión documental permitió identificar que las aplicaciones del *machine learning* para la detección de anomalías en entornos cloud se concentran en tres enfoques principales: algoritmos supervisados, no supervisados y modelos de *deep learning*. Los resultados muestran que los algoritmos supervisados, como las máquinas de soporte vectorial y los árboles de decisión, alcanzan altos niveles de precisión cuando se dispone de conjuntos de datos etiquetados. Sin embargo, su aplicabilidad en la nube se ve limitada por la escasez de datos previamente clasificados, lo que restringe su capacidad de generalización (Zhang et al., 2019).

En contraste, los métodos no supervisados, como el clustering basado en K-means y los modelos de densidad, demostraron ser más adecuados para entornos cloud, donde los datos son heterogéneos y no siempre etiquetados. Ahmed, Mahmood y Hu (2016) señalan que estos enfoques permiten descubrir patrones anómalos desconocidos, aunque generan un mayor número de falsos positivos, lo que implica un reto para su implementación práctica.

Tabla 2 Principales enfoques de *machine learning* aplicados a la detección de anomalías en cloud

Enfoque	Algoritmos representativos	Ventajas	Limitaciones
Supervisado	SVM, Árboles de decisión	Alta precisión con datos etiquetados	Requiere datasets etiquetados, poca adaptabilidad
No supervisado	K-means, DBSCAN	Detecta anomalías desconocidas	Mayor tasa de falsos positivos
Deep learning	RNN, CNN	Alta capacidad para patrones complejos	Escasa interpretabilidad, alto costo computacional
Híbrido	Supervisado + No supervisado	Reducción de falsos positivos, mayor precisión	Complejidad en diseño e implementación

Los estudios revisados también evidencian que el *deep learning* ha ganado protagonismo en los últimos años. Xu et al. (2018) reportan que las redes neuronales recurrentes aplicadas al análisis de secuencias de tráfico en la nube logran detectar anomalías con mayor precisión que los métodos tradicionales. Asimismo, Ribeiro et al. (2020) destacan que los enfoques híbridos, que combinan técnicas supervisadas y no supervisadas, reducen significativamente la tasa de falsos positivos y mejoran la capacidad de adaptación a entornos dinámicos.

Tabla 3 Comparación de resultados reportados en estudios recientes

Autor(es)	Año	Enfoque metodológico	Principales hallazgos
Chandola, Banerjee & Kumar	2009	Revisión general	Definición de anomalía y clasificación de técnicas
Ahmed, Mahmood & Hu	2016	No supervisado	Útil para anomalías desconocidas, pero con falsos positivos
Xu et al.	2018	Deep learning	RNN detecta patrones complejos en tráfico cloud
Ribeiro et al.	2020	Híbrido	Reducción de falsos positivos y mayor precisión

La discusión de estos hallazgos permite establecer que, aunque los modelos supervisados ofrecen resultados más precisos en escenarios controlados, los enfoques no supervisados y de *deep learning* resultan más adecuados para la naturaleza cambiante de los entornos cloud. Sin embargo, persisten desafíos relacionados con la escalabilidad de los modelos, la interpretabilidad de los resultados y la integración con sistemas de monitoreo en tiempo real. Chandola, Banerjee y Kumar (2009) ya advertían que la detección de anomalías no solo debe enfocarse en la precisión, sino también en la capacidad de explicar los resultados, aspecto que sigue siendo un vacío en la literatura actual.

En términos de novedad científica, se observa que los enfoques híbridos representan una línea de investigación prometedora, ya que permiten combinar la robustez de los métodos supervisados con la flexibilidad de los no supervisados. Además, la incorporación de técnicas de *deep learning* abre perspectivas para el desarrollo de sistemas autónomos capaces de aprender y adaptarse continuamente a nuevas amenazas en la nube. No obstante, la pertinencia de estos modelos dependerá de su capacidad para integrarse en arquitecturas cloud sin comprometer el rendimiento ni la disponibilidad de los servicios.

CONCLUSIONES

El análisis realizado permite afirmar que el *machine learning* constituye una herramienta fundamental para la detección de anomalías en entornos cloud, ofreciendo soluciones más flexibles y precisas que los métodos tradicionales basados en reglas. Los hallazgos de la revisión muestran que los algoritmos supervisados alcanzan altos niveles de exactitud en escenarios controlados, aunque su aplicabilidad se ve limitada por la necesidad de datos etiquetados. Los enfoques no supervisados, por su parte, resultan más adecuados para la naturaleza dinámica y heterogénea de la nube, aunque presentan el reto de generar falsos positivos.

El *deep learning* emerge como una tendencia clave, capaz de identificar patrones complejos y adaptarse a entornos cambiantes, aunque su falta de interpretabilidad sigue siendo un obstáculo para su adopción masiva. Los enfoques híbridos representan una línea de investigación prometedora, ya que combinan la robustez de los métodos supervisados con la flexibilidad de los no supervisados, logrando reducir la tasa de falsos positivos y mejorar la precisión.

En términos de relevancia, este estudio aporta una visión crítica y actualizada sobre el estado del arte en la aplicación del *machine learning* para la detección de anomalías en la nube, destacando tanto sus fortalezas como sus limitaciones. Se concluye que el futuro de la investigación en este campo debe orientarse hacia el desarrollo de modelos escalables, interpretables y capaces de integrarse en sistemas de monitoreo en tiempo real sin comprometer el rendimiento de los servicios cloud. Finalmente, se reconoce que persisten interrogantes abiertos, como la necesidad de mejorar la transparencia de los modelos de *deep learning* y la adaptación de los sistemas híbridos a arquitecturas distribuidas más complejas, lo que constituye una tarea pendiente para futuros investigadores.

REFERENCIAS BIBLIOGRÁFICAS

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). *A survey of network anomaly detection techniques*. *Journal of Network and Computer Applications, 60*(1), 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Al-Mazrawe, A., & Al-Musawi, B. (2024, abril). *Detección de anomalías en redes en la nube: Una reseña*. *BIO Web of Conferences, 97*(5), 00019. https://doi.org/10.1051/bioconf/20249700019

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Poyatos, R., Ribeiro, M., Schneider, G., Sentis, A., Serrano, J. C., Trawiński, B., & Herrera, F. (2020). *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI*. *Information Fusion, 58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly detection: A survey*. *ACM Computing Surveys, 41*(3), 1–58. https://doi.org/10.1145/1541880.1541882

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). *Anomaly-based network intrusion detection: Techniques, systems and challenges*. *Computers & Security, 28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

Hodge, V., & Austin, J. (2004). *A survey of outlier detection methodologies*. *Artificial Intelligence Review, 22*(2), 85–126. https://doi.org/10.1023/B:AIRE.0000045502.10941.a9

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Technical Report EBSE-2007-01, Keele University.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology, Special Publication 800-145.

Papavasileiou, E. F., Oubibi, M., Finnegan, A., & Haleon. (2025, noviembre). *IA explicable para la detección de anomalías en la nube: Haciendo que el reconocimiento de amenazas basado en redes neuronales sea transparente y auditable*. Recuperado de ResearchGate.

Saabith, S., Thangarajah, V., & Fareez, M. (2023, octubre). *Un estudio de técnicas de aprendizaje automático para la detección de anomalías en ciberseguridad*. *Revista Internacional de Investigación en Ingeniería y Ciencia, 11*(10), 183–193. Recuperado de ResearchGate.

Sommer, R., & Paxson, V. (2010). *Outside the closed world: On using machine learning for network intrusion detection*. *IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

Xu, H., Chen, W., Zhao, N., Li, Z., Bu, J., Li, Z., & Jin, R. (2018). *Unsupervised anomaly detection via variational auto-encoder for seasonal KPIs in web applications*. *Proceedings of the 2018 World Wide Web Conference*, 187–196. https://doi.org/10.1145/3178876.3185996

Yuan, K., Xia, Z., & Shi, Y. (2025). *Detección semántica no supervisada por Web de ataques APT en tráfico de red utilizando DBSCAN++ y aiNet mejorados*. *International Journal on Semantic Web and Information Systems, 21*(1), 1–31. https://doi.org/10.4018/IJSWIS.370387