

Critical analysis of cybersecurity strategies for data protection in the cloud: systematic review

Rivas Rojas, Orlando Leone¹ ; Ráez Martínez, Haymin Teresa² 

^{1,2}Universidad Tecnológica del Perú, Perú, u21318315@utp.edu.pe, c19240@utp.edu.pe

Resumen— *The widespread adoption of cloud computing has increased critical cyber threats, making it urgent to evaluate the effectiveness of conventional defense mechanisms. The objective of this research was to comparatively analyze modern cybersecurity strategies versus traditional methods in cloud environments. A systematic review was conducted under the PRISMA protocol, analyzing 65 articles from the Scopus database published between 2021 and 2025. The results reveal a technological transition where, although cryptography remains the predominant strategy in 49% of the studies, there is an accelerated growth of 38% in the adoption of Artificial Intelligence for proactive detection. It was also identified that unauthorized access and denial-of-service attacks continue to be the main threats. It is concluded that there is a methodological bias in the literature, which prioritizes efficiency metrics in simulations over real security validation; therefore, it is recommended to migrate to hybrid architectures validated in real operational scenarios to ensure information integrity.*

Keywords— *Cloud security, Cybersecurity Strategies, Data protection, Cryptography, AI-based Detection*

Análisis crítico de estrategias de ciberseguridad para protección de datos en la nube: revisión sistemática

Rivas Rojas, Orlando Leone¹ ; Ráez Martínez, Haymin Teresa² 

^{1,2}Universidad Tecnológica del Perú, Perú, u21318315@utp.edu.pe, c19240@utp.edu.pe

Resumen— La adopción masiva de la computación en la nube ha incrementado a ciberamenazas críticas, lo cual hace urgente evaluar la eficacia de los mecanismos de defensa convencionales. El objetivo de esta investigación fue analizar comparativamente las estrategias de ciberseguridad modernas frente a los métodos tradicionales en entornos cloud. Se realizó una revisión sistemática bajo el protocolo PRISMA, analizando 65 artículos de la base de datos Scopus publicados entre 2021 y 2025. Los resultados evidencian una transición tecnológica donde la criptografía se mantiene como la estrategia predominante en el 49% de los estudios, existe un crecimiento acelerado del 38% en la adopción de Inteligencia Artificial para la detección proactiva. Asimismo, se identificó que el acceso no autorizado y los ataques de denegación de servicio continúan siendo las principales amenazas. Se concluye que existe un sesgo metodológico en la literatura, la cual prioriza métricas de eficiencia en simulaciones sobre la validación de seguridad real; por tanto, se recomienda migrar hacia arquitecturas híbridas validadas en escenarios operativos reales para garantizar la integridad de la información.

Palabras clave— Seguridad en la nube, Estrategias de ciberseguridad, Protección de datos, Criptografía, Detección basada en IA

I. INTRODUCCIÓN

La computación en la nube se ha consolidado como un componente esencial de la infraestructura digital actual. Su adopción ha permitido que organizaciones de distintos sectores modernicen sus procesos gracias a capacidades más flexibles y escalables para almacenar, procesar y gestionar información, con el valor añadido de reducir costos operativos [1], [2]. Sin embargo, esta misma dependencia ha ampliado la superficie de exposición frente a incidentes que comprometen la seguridad de datos y servicios críticos [3], [4].

Entre los riesgos más frecuentes se encuentran los accesos no autorizados, los ataques de denegación de servicio, las filtraciones masivas y las vulnerabilidades que acompañan la expansión del Internet de las Cosas [5], [8]. Si bien el cifrado [6][11], la autenticación y el monitoreo conforman la base de la protección en este tipo de infraestructura, su aplicación práctica aún presenta limitaciones operativas y técnicas que permanecen sin resolver. Todavía existen dificultades para integrar soluciones entre plataformas distintas, escalar mecanismos de defensa en arquitecturas complejas o adaptarse a entornos híbridos que cambian con rapidez [7]. Todo ello evidencia la necesidad de examinar con mayor profundidad cómo se están aplicando estas estrategias y hasta qué punto logran responder a las amenazas actuales. A pesar de los avances recientes, la literatura científica continúa mostrando resultados heterogéneos

respecto a la efectividad de los mecanismos de protección en la nube. Algunos trabajos [2] indican que, pese al crecimiento de propuestas tecnológicas, las brechas de seguridad siguen siendo habituales y complejas de contener. Esta situación se agrava con el aumento de ataques distribuidos de denegación de servicio basados en botnets, los cuales afectan directamente la disponibilidad de servicios esenciales en infraestructuras virtualizadas [5]. Asimismo, se advierte que los ataques orientados a hipervisores pueden comprometer no solo los datos, sino también la estabilidad de la infraestructura que los soporta [9]. Aun con herramientas especializadas como los sistemas SIEM, muchos incidentes pasan desapercibidos o se identifican con retraso, lo que reduce el margen de maniobra para responder oportunamente [10], [10]. Algo parecido ocurre con las organizaciones que ya operan en la nube: distintos reportes señalan que continúan registrando accesos indebidos y pérdidas de información confidencial, incluso después de invertir en controles y servicios de seguridad [12]. La incorporación de técnicas basadas en inteligencia artificial tampoco ha resuelto del todo el problema, ya que algunas amenazas evolucionan con rapidez y burlan los mecanismos de detección [14], [15]. Por otro lado, propuestas recientes basadas en blockchain y criptografía cuántica intentan mitigar estas brechas [13]. A esto se suma que los ataques internos siguen siendo especialmente complejos de anticipar y gestionar [15]. Considerando este escenario, se hace evidente que no existe aún una línea de actuación unificada. La variedad de soluciones y prácticas que se han desarrollado en los últimos años refleja avances importantes, pero también deja ver que no hay claridad respecto a cuáles de ellas funcionan mejor según el tipo de organización. Esta falta de claridad complica tanto la evaluación técnica de las propuestas existentes como la toma de decisiones en contextos donde la seguridad es prioritaria.

Por ello, el presente estudio tiene como objetivo realizar una revisión sistemática para analizar de manera detallada lo que se ha investigado hasta ahora sobre protección de datos en la nube, evaluando su efectividad comparada frente a métodos tradicionales e identificando sus limitaciones actuales.

El documento se estructura de la siguiente manera. La Sección II, Metodología, describe el método utilizado para realizar la RSL. Se presentan la utilización de los criterios PICO y el método PRISMA en la búsqueda Scopus. La Sección III, Resultados, clasifica y presenta los hallazgos obtenidos de los artículos incluidos, haciendo énfasis en las amenazas y las estrategias de protección en la nube. Los hallazgos en la Sección

IV, Discusión, serán analizados en relación con sus antecedentes académicos para buscar pruebas de su efectividad. Finalmente, en la Sección V, Conclusiones, se presentan un resumen de los principales hallazgos obtenidos, el aporte de la revisión sistematica y recomendaciones.

II. METODOLOGÍA

Para la elaboración de la RSL, se ejecutó una búsqueda exhaustiva de artículos científicos utilizando la base de datos Scopus. La metodología PICO se llevó a cabo para plantear preguntas estratégicas que contribuyen a la organización de la información pertinente al problema y su posible solución. Sumado a ello, el método PRISMA sirvió como referencia para la elección e identificación de los estudios que se consideraron para inclusión.

A. Formulario de PICO

Se orientó la estrategia PICO, para sistematizar con coherencia las interrogantes de estudio, considerando cuatro elementos fundamentales: Población, intervención, comparación y resultados

1) Identificación de elementos PICO

A partir de la identificación de los componentes del método PICO, se formuló la pregunta de investigación principal para esta revisión:

¿Qué estrategias de ciberseguridad se han aplicado para la protección de datos en la nube, y qué tan efectivas son en comparación con métodos tradicionales para garantizar la confidencialidad, integridad y disponibilidad de la información?

Para analizar las publicaciones, la pregunta principal se dividió en subpreguntas específicas, cada una asociada a un componente PICO. Posteriormente, se determinaron las palabras clave, asegurando que fueran coherentes con el enfoque del estudio. Finalmente, se agregaron los operadores booleanos AND y OR para combinar las palabras clave, además de comillas para los términos compuestos. Esto dio lugar a la ecuación de búsqueda utilizada en la base de datos Scopus.

1) Sintaxis de la formula PICO

Finalmente, se integraron las palabras clave derivadas de cada subpregunta mediante el operador AND. Para refinar y delimitar la búsqueda de documentación relevante para esta revisión, se aplicó una combinación de los operadores OR y AND, lo que resultó en una ecuación de búsqueda más precisa.

TABLA I
ECUACIÓN DE BÚSQUEDA PICO CON PALABRAS CLAVES

Ecuación de búsqueda sin considerar criterios de inclusión y exclusión
("cloud computing" OR "cloud services" OR "cloud environment" OR "cloud platforms" OR "public cloud" OR "private cloud" OR "cloud security" OR "cloud infrastructure") AND ("encryption" OR "authentication" OR "access control" OR "monitoring" OR "blockchain" OR "artificial intelligence" OR "AI" OR "SIEM" OR "firewall") AND ("cybersecurity" OR "cyber threats" OR "security vulnerabilities" OR "data breaches" OR "unauthorized access" OR "DDoS" OR "cyber attack" OR "security risk" OR "data leakage") AND ("security approaches" OR "security methods" OR "security frameworks" OR "traditional security" OR "data protection" OR "information security" OR "confidentiality" OR "integrity" OR "effectiveness" OR "performance")

Ecuación de búsqueda sin considerar criterios de inclusión y exclusión
("cloud computing" OR "cloud services" OR "cloud environment" OR "cloud platforms" OR "public cloud" OR "private cloud" OR "cloud security" OR "cloud infrastructure") AND ("encryption" OR "authentication" OR "access control" OR "monitoring" OR "blockchain" OR "artificial intelligence" OR "AI" OR "SIEM" OR "firewall") AND ("cybersecurity" OR "cyber threats" OR "security vulnerabilities" OR "data breaches" OR "unauthorized access" OR "DDoS" OR "cyber attack" OR "security risk" OR "data leakage") AND ("security approaches" OR "security methods" OR "security frameworks" OR "traditional security" OR "data protection" OR "information security" OR "confidentiality" OR "integrity" OR "effectiveness" OR "performance")

TABLA II
PALABRAS CLAVE DE LAS SUBPREGUNTAS PICO

P	Population	¿Qué amenazas y vulnerabilidades afectan la protección de datos en la nube?	"computación en la nube", "servicios en la nube", "entorno de la nube", "plataformas en la nube", "seguridad en la nube", "nube pública", "nube privada", "infraestructura en la nube"	"cloud computing", "cloud services", "cloud environment", "cloud platforms", "cloud security", "public cloud", "private cloud", "cloud infrastructure"
I	Intervention	¿Qué estrategias de ciberseguridad se han implementado para mitigar esas amenazas?	"cifrado", "autenticación", "control de acceso", "monitoreo", "blockchain", "inteligencia artificial", "IA", "SIEM", "firewall", "estrategias de ciberseguridad"	"encryption", "authentication", "access control", "monitoring", "blockchain", "artificial intelligence", "AI", "SIEM", "firewall", "cybersecurity strategies"
C	Comparison	¿Cómo se comparan estas estrategias de ciberseguridad con los métodos tradicionales de seguridad en la nube?	"ciberseguridad", "ciberamenazas", "vulnerabilidades de seguridad", "brechas de datos", "acceso no autorizado", "ataques DDoS", "ciberataque", "riesgo de seguridad", "filtración de datos"	"cybersecurity", "cyber threats", "security vulnerabilities", "data breaches", "unauthorized access", "DDoS", "cyber attack", "security risk", "data leakage"
O	Outcome	¿Qué resultados reporta la literatura en cuanto a eficacia, beneficios, limitaciones y tendencias emergentes de estas estrategias de ciberseguridad?	"enfoques de seguridad", "métodos de seguridad", "marcos de seguridad", "seguridad tradicional", "protección de datos", "seguridad de la información", "confidencialidad", "integridad", "efectividad", "rendimiento"	"security approaches", "security methods", "security frameworks", "traditional security", "data protection", "information security", "confidentiality", "integrity", "effectiveness", "performance"

2) Criterios de búsqueda empleados

a) CRITERIOS DE INCLUSIÓN

Estudios que analicen o propongan estrategias de ciberseguridad aplicadas a la protección de datos en la nube, artículos que evalúen medidas como cifrado, autenticación, monitoreo, blockchain, inteligencia artificial, SIEM o esteganografía en contextos cloud, documentos publicados entre 2021 y 2025, documentos en inglés, artículos que presenten resultados empíricos, evaluaciones comparativas o propuestas metodológicas aplicables a la seguridad en la nube.

b) CRITERIOS DE EXCLUSIÓN

Documentos no arbitrarios o de literatura gris, investigaciones que no presenten relación con la protección de datos sensibles ni aporten evidencia sobre su efectividad, estudios cuya

temática principal no sea la protección de datos sensibles en entornos cloud, estudios sin acceso al texto completo.

B. Prisma

Para el proceso de selección de estudios se empleó la metodología PRISMA.

1)Proceso de reconocimiento

Se realizó la búsqueda de la literatura en la base de datos Scopus, elegida por su confiabilidad, fines académicos y por la gran cobertura de publicaciones científicas que ofrece. De esta manera se garantizó que los artículos recuperados fueran confiables y relevantes.

1)Eliminación de artículos duplicados

En esta etapa no se eliminaron artículos duplicados.

2)Proceso de elegibilidad

A partir de los 2,157 registros iniciales, se aplicaron filtros automáticos (año de publicación, idioma y tipo de documento), lo que redujo el número a 322. Posteriormente, se llevó a cabo una revisión de títulos y resúmenes para descartar aquellos que no cumplieran con los criterios de inclusión establecidos en el PICO. También se excluyeron los estudios que no eran de acceso abierto y los que estaban fuera de tema.

3)Proceso de elección

Tras la lectura de texto completo, 65 artículos cumplieron con los criterios establecidos.

El procedimiento completo se ilustra en el siguiente flujograma PRISMA, donde se detalla la cantidad de registros identificados, excluidos y finalmente incorporados en la revisión.

A continuación, se representa el flujograma PRISMA.

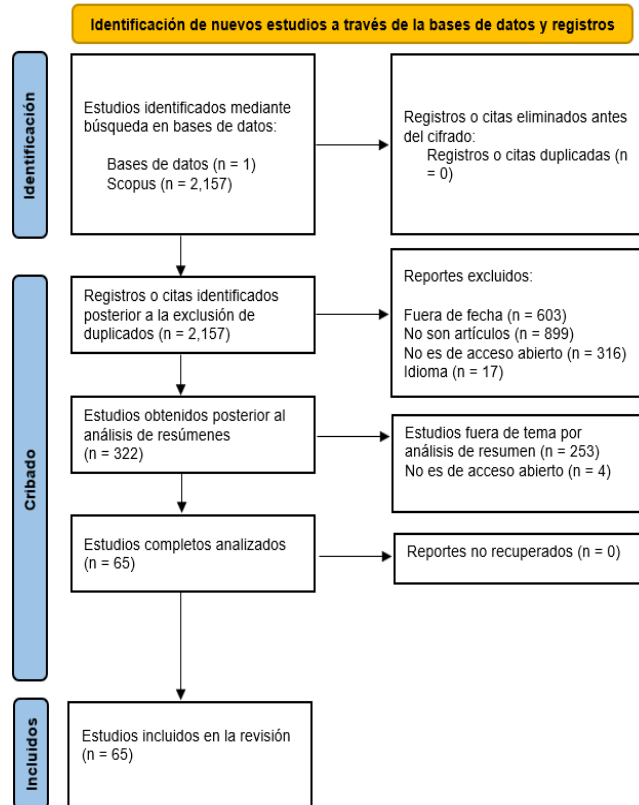


Fig. 1 DIAGRAMA PRISMA

III. RESULTADOS

En el presente apartado, y luego de la recopilación de información de los 65 estudios revisados sistemáticamente, se cumplió con el objetivo de la RSL, el cual es evidenciar las estrategias de ciberseguridad implementadas para proteger los datos en entornos cloud y su efectividad frente a los métodos tradicionales. A continuación, se muestra un resumen de la información obtenida a partir de los estudios revisados durante todo el proceso sistemático.

Los datos se presentan en tablas y gráficos que organizan los principales hallazgos: las amenazas identificadas, las estrategias aplicadas, su comparación con los métodos tradicionales, la efectividad de las métricas utilizadas, además de la clasificación de los entornos en la nube y las limitaciones reportadas.

El propósito de esta sección es mostrar las tendencias, los patrones metodológicos y los vacíos de investigación más relevantes en la literatura sobre ciberseguridad en la nube. Con ello se busca ofrecer una visión completa sobre cómo se están implementando las estrategias modernas y qué implicaciones tienen en la protección de la información en distintos tipo de entornos cloud. Toda la información expuesta se basa en el análisis de los 65 artículos revisados.

A. Información preliminar de la extracción de datos

1. Distribución de los estudios según el año de publicación

Aunque el rango de inclusión contempló investigaciones desde el 2021, los estudios correspondieron a dicho año no fueron considerados por no cumplir los criterios de selección establecidos, concentrándose la evidencia a partir de 2022.

Durante este periodo, se observa que el 6% de los estudios fueron publicados en 2022 [16], [17], [18], [19], el 11% en 2023 [20], [21], [22], [23], [24], [25], [26], el 30% en 2024 [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46] y el 52% en 2025 [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], consolidando un crecimiento progresivo en la generación de conocimiento sobre estrategias de ciberseguridad para la protección de datos en la nube, lo que refleja un interés académico en expansión, particularmente notorio a partir de 2024, año en el que la investigación sobre protección de datos y amenazas en la nube experimentó un impulso significativo.

CATEGORÍA: Año de publicación

FIG. 2 AÑO DE PUBLICACIÓN



2. Distribución de los estudios según el país

En cuanto a la procedencia geográfica de las investigaciones, el análisis evidencia una marcada concentración en el continente asiático. India [18], [20], [23], [24], [28], [30], [31], [32], [34],

[37], [41], [47], [49], [50], [52], [53], [56], [57], [58], [59], [62], [65], [67], [68], [73], [74], [75] destaca como el país con mayor producción científica, representando el 41.5% del total de los estudios incluidos. Le sigue china [16], [21], [33], [45], [60], [63], [70], [72], [78], [80] con 15.4% y un grupo diverso de naciones entre ellas Australia, Egipto, España, Estados Unidos, Israel, Perú, Irak y Turquía [17], [19], [22], [25], [26], [27], [29], [35], [36], [38], [39], [40], [42], [43], [44], [46], [48], [51], [54], [55], [62], [64], [66], [69], [71], [76], [77], [79] se agruparon bajo la categoría “otros países”, aportando en conjunto el 35.4% de la evidencia analizada. Finalmente, Arabia Saudita muestra una participación del 7.7%.

De esto podemos concluir que la mayor parte de investigaciones en esta materia proviene de regiones emergentes de Asia, en las cuales el avance tecnológico e investigación en soluciones de ciberseguridad alojadas en nube para la protección de datos ha generado un mayor interés académico.

TABLA III

DISTRIBUCIÓN DE LOS ESTUDIOS POR PAÍS DE PROCEDENCIA

Países	Nº de País	% de País
India	27	41.5%
China	10	15.4%
Arabia Saudita	5	7.7%
Otros Países	23	35.4%

3. Distribución del enfoque metodológico

Respecto al enfoque metodológico de los estudios analizados, se aprecia que la mayoría opta por un diseño de investigación de tipo mixtocon un 48% mientras que las investigaciones de estudios cualitativos [55] apenas alcanzan el 2%. Esta distribución muestra que existe una clara intención de combinar distintos métodos al analizar las estrategias de ciberseguridad. Se busca unir la información obtenida en la práctica con las ideas teóricas, de modo que el estudio ofrezca una comprensión más completa sobre cómo proteger los datos en entornos de computación en la nube.



FIG. 4 DISTRIBUCIÓN DEL ENFOQUE METODOLÓGICO

4. Método de validación

En relación con los métodos de validación utilizados, la mayoría de los estudios optó por la validación de prototipo [16], [18], [19], [21], [22], [23], [24], [26], [27], [28], [29], [30], [31], [33], [35], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [67], [68], [69], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], representando el 84.6% del total de la muestra. Le siguen los estudios basados en simulación [17], [20], [25], [32], [34], [36], [37], [54], [66] con un 13.8%, y en menor proporción, los estudios de caso [70] con un 1.5%. Esta distribución evidencia una clara preferencia por comprobar la eficacia de las estrategias de ciberseguridad en entornos controlados o experimentales, lo que demuestra el interés de la comunidad científica por evaluar la aplicabilidad real de los modelos y mecanismos propuestos para la protección de datos en la nube.

CATEGORÍA: Métodos de validación utilizados.

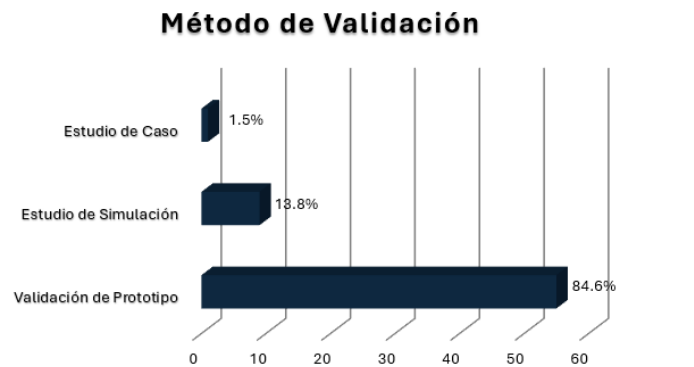


FIG. 5 MÉTODO DE VALIDACIÓN

B. Ítems para la extracción de datos

1) RQ1: ¿Qué amenazas y vulnerabilidades afectan la protección de datos en la nube?

Respecto a las amenazas y vulnerabilidades que afectan la protección de datos en la nube, el análisis revela que el acceso no autorizado [18], [21], [22], [23], [24], [25], [26], [27], [28], [29], [32], [35], [40], [43], [47], [49], [52], [53], [56], [58], [59], [60], [65], [68], [73], [80] constituye la categoría más recurrente, con una presencia del 40% de los estudios revisados. Le siguen los ataques distribuidos de denegación de servicio (DDoS) [19], [20], [31], [38], [44], [45], [46], [54], [57], [61], [67], [71], [72], [75], [79] con un 23% y el compromiso de la integridad de los datos [16], [33], [36], [41], [48], [50], [55], [62], [74], [77] con un 15%. En menor proporción se identifican la fuga de datos [39], [42], [51], [69], [70], [78], que alcanza el 9%, las amenazas cuantitativas [17], [30], [37], [66], [76] con el 8% y la presencia de malware con un 5%. La gráfica muestra que la mayor preocupación dentro de la literatura es el acceso no autorizado, así como asegurar la disponibilidad de los servicios, que son elementos indispensables para resguardar la confidencialidad, integridad y resiliencia en la nube.

CATEGORÍA: Priorización de amenazas estudiadas

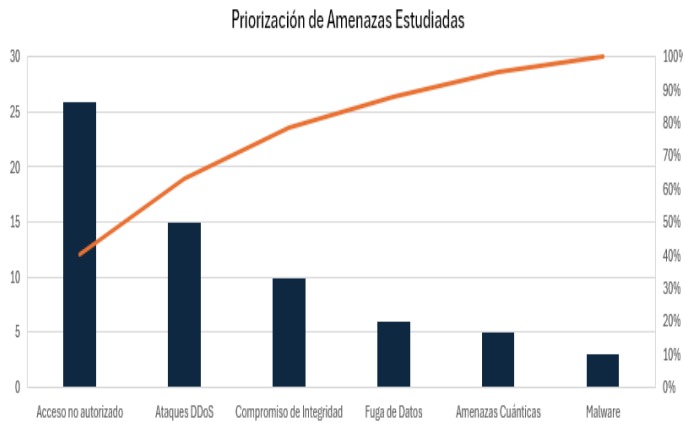


FIG. 6 CATEGORÍA DE LA RQ1

2) RQ2: ¿Qué estrategias de ciberseguridad se han implementado para mitigar esas amenazas?

En cuanto a las estrategias de ciberseguridad implementadas para mitigar las amenazas en entornos cloud, el análisis evidencia que la criptografía [16], [17], [18], [20], [23], [24], [27], [28], [30], [32], [33], [37], [39], [40], [41], [42], [43], [45], [47], [48], [49], [50], [56], [58], [65], [66], [68], [69], [73], [74], [76], [77] es la más utilizada, ya que aparece en el 49% de los estudios revisados. Le siguen la detección basada en inteligencia artificial [19], [25], [29], [31], [34], [35], [36], [38], [44], [46], [52], [53], [54], [57], [59], [61], [62], [63], [64], [67], [71], [72], [75], [79], [80] con un 38%, el control de acceso [21], [22], [26], [60], [78] con un 8% y la tecnología blockchain [51], [55], [70] con un 5%. Esta distribución revela que los métodos de criptografía y los sistemas de detección de IA continúan siendo las estrategias más adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos en la nube, mientras que tecnologías emergentes como blockchain muestran una presencia más limitada dentro de la literatura científica.

CATEGORÍA: Priorización de estrategias de seguridad

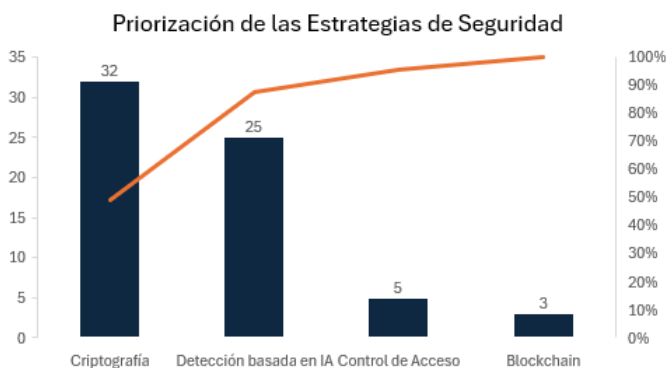


FIG. 7 CATEGORÍA DE LA RQ2

3) RQ3: ¿Cómo se comparan estas estrategias de ciberseguridad con los métodos tradicionales de seguridad en la nube?

De acuerdo con la comparación entre las estrategias de ciberseguridad aplicadas y los métodos tradicionales en cuanto entornos cloud, el análisis indica que la mayor parte de los estudios evaluados adoptan enfoques que combinan múltiples tecnologías [17], [20], [21], [24], [27], [32], [33], [35], [36],

[37], [39], [40], [41], [48], [49], [51], [52], [53], [62], [65], [66], [67], [68], [75], [78], [79], [80], representando el 42% del total. Le siguen los sistemas basados en aprendizaje automático (ML) [19], [29], [31], [34], [38], [44], [46], [47], [54], [57], [59], [61], [63], [64], [71], [72], [76] con un 26%, la criptografía clásica [18], [25], [28], [42], [43], [50], [58], [73], [74] con el 14% y los sistemas convencionales [16], [23], [26], [45], [55], [70], [77] con un 11%. En menor proporción se identifican la criptografía emergente [22], [56], [60] con el 5% y herramientas específicas [30], [69] con un 3%. El análisis de la distribución permite ver que, aunque los enfoques tradicionales siguen apareciendo en diversos estudios, en los últimos años se observa una inclinación creciente hacia propuestas mixtas que combinan herramientas avanzadas, entre ellas la criptografía y distintas técnicas de aprendizaje automático. Estas combinaciones permiten ofrecer mayores niveles de protección frente a las amenazas que persisten en los entornos de computación en la nube.

CATEGORÍA: Foco metodológico de la comparación

Foco Metodológico de la Comparación

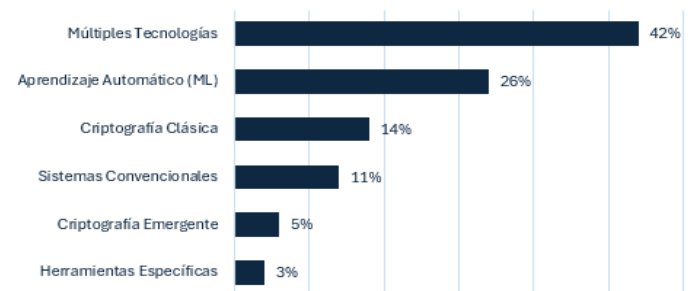


FIG. 8 CATEGORÍA DE LA RQ3

4) RQ4: ¿Qué resultados evidencia la literatura en cuanto a la efectividad de estas estrategias en garantizar la confidencialidad, integridad y disponibilidad de los datos en la nube?

En cuanto a la efectividad de las estrategias de ciberseguridad en garantizar la confidencialidad, integridad y disponibilidad de los datos en la nube, la revisión de la literatura evidencia que la mayoría de los trabajos analizados evalúa su rendimiento utilizando distintas métricas de eficiencia [16], [17], [18], [20], [21], [22], [23], [24], [25], [26], [27], [28], [30], [32], [33], [37], [40], [41], [42], [43], [45], [48], [50], [55], [56], [58], [60], [65], [68], [69], [74], [77], [78], [79], presentes en el 52% de los artículos revisados. Le siguen las métricas de precisión [19], [29], [31], [34], [35], [36], [38], [39], [44], [46], [52], [53], [54], [57], [59], [61], [62], [63], [64], [67], [71], [72], [73], [75], [76] con un 38%, mientras que las métricas específicamente orientadas a seguridad [66], [70], [80] y otras métricas [47], [49], [51] representaron únicamente el 5% cada una. Estos resultados indican que la literatura tiende a priorizar la evaluación del rendimiento y la exactitud de las estrategias implementadas, aunque los análisis centrados directamente en la seguridad siguen siendo limitados, lo que sugiere una oportunidad para estudios futuros más enfocados en la validación de la protección de datos en entornos cloud.

CATEGORÍA: Distribución de la evidencia de efectividad

Distribución de la Evidencia de Efectividad

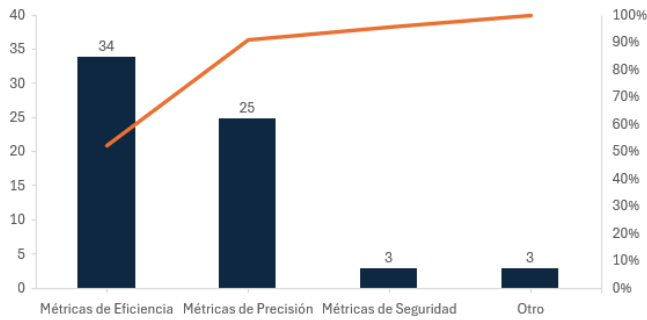


FIG. 9 CATEGORÍA DE LA RQ4

C. Contexto de implementación y limitaciones

La mayoría de los estudios no especificó el tipo de nube [16], [18], [19], [20], [21], [22], [24], [26], [28], [29], [32], [33], [34], [35], [36], [37], [38], [40], [41], [42], [43], [44], [45], [46], [47], [49], [50], [52], [53], [54], [58], [59], [60], [63], [66], [68], [69], [71], [72], [73], [74], [75], [76], [79], [80] utilizada 69%. Entre los que, si reportaron el entorno, el 15% se centró en nube híbrida [17], [23], [27], [31], [39], [48], [51], [61], [64], [67], el 11% en nubes públicas [25], [30], [46], [57], [62], [65], [78] y el 5% en nubes privadas [55], [70], [77]. Esta distribución muestra que, si bien en la literatura se reconocen diversos tipos de entornos cloud, todavía hay poca información específica sobre cómo se implementan en la práctica. Esta falta de detalle hace más difícil extrapolar o aplicar con seguridad los resultados obtenidos.

CATEGORÍA: Clasificación del entorno cloud de implementación

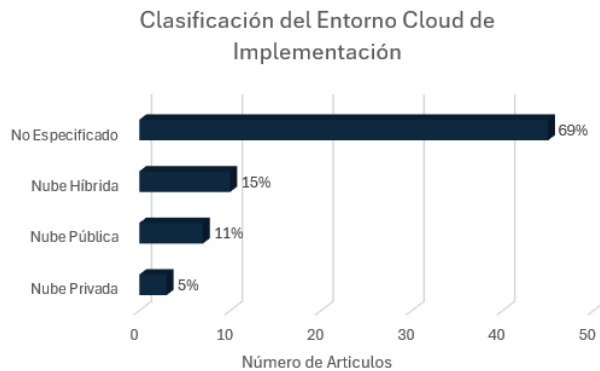


FIG. 10 CLASIFICACIÓN DEL ENTORNO CLOUD

2. Clasificación de las limitaciones reportadas en la literatura

La limitación que aparece con mayor frecuencia es la validez externa [16], [18], [19], [20], [22], [25], [28], [30], [32], [33], [36], [37], [41], [42], [43], [44], [47], [49], [50], [52], [53], [54], [57], [58], [59], [60], [61], [62], [65], [67], [69], [71], [74], [75], [76], [80], que presente en el 55% de los estudios. Esto refleja que, en muchos casos, los resultados obtenidos no pueden generalizarse fácilmente a otros contextos o entornos. Le siguen el costo computacional [17], [21], [23], [26], [31], [35], [39], [46], [48], [55], [56], [64], [66], [70], [73], [79] con un 25% la restricción de generalización [27], [38], [40], [72], [77], [78] con un 9%, el impacto operacional [29], [34], [45], [63] con un 6% y la barrera de adopción [24], [51], [68] con un 5%. En conjunto,

estos resultados muestran que, aunque las estrategias de ciberseguridad analizadas demuestran ser efectivas, su implementación real aún enfrenta obstáculos operativos, económicos y metodológicos. Lo que indica anteriormente resalta la necesidad de continuar investigando y analizando los diferentes casos de uso para poder identificar los puntos críticos en los cuales enfocarse para afrontar dichas limitaciones.

CATEGORÍA: Clasificación de limitaciones identificadas en la literatura.

Clasificación de las Limitaciones Reportadas en la Literatura

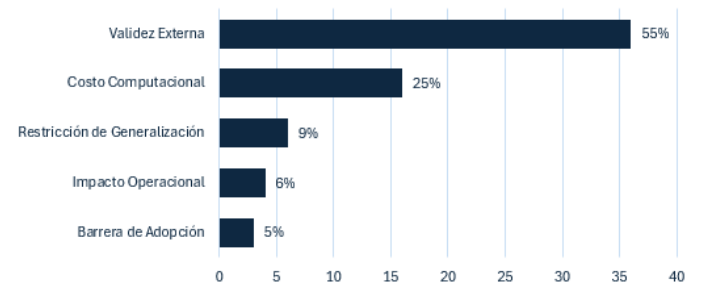


FIG. 11 CLASIFICACIÓN DE LAS LIMITACIONES REPORTADAS EN LA LITERATURA

D. Respuesta a la pregunta general PICO

A continuación, se brinda respuesta a la pregunta PICO “¿Qué estrategias de ciberseguridad se han implementado para mitigar las amenazas en entornos cloud y cómo se comparan con los métodos tradicionales en términos de efectividad?”, en función a la información revisada.

Los estudios revisados demuestran una mayor eficacia de las soluciones alojadas en nube frente a las amenazas más relevantes en materia de ciberseguridad. Entre los métodos más usados actualmente podemos encontrar la criptografía emergente, sistemas de detección impulsados por inteligencia artificial y demás soluciones que combinan distintas tecnologías, las cuales registran un desempeño mayor a métodos más tradicionales como la criptografía clásica.

Para medir la efectividad de cada alternativa, la mayoría de los estudios recurrieron principalmente a métricas de eficiencia y precisión, mientras que las mediciones centradas únicamente en seguridad fueron menos comunes. Esto sugiere que, aunque las estrategias modernas sí fortalecen la protección de los datos, la investigación todavía suele a priorizar el rendimiento y la exactitud por encima de evaluaciones directas de seguridad.

En general, la evidencia apunta a que las soluciones híbridas y basadas en tecnologías avanzadas logran mejores niveles de protección, sin embargo, su implementación efectiva aún enfrenta limitaciones de tipo operativo, económico y metodológico, lo que coincide con los puntos de dolor identificados por los estudios revisados. Finalmente, los resultados sobre la efectividad de los métodos mencionados pueden visualizarse en el gráfico presentado en la sección RQ4, el cual presenta cómo se clasifican las métricas empleadas para su evaluación.

IV. DISCUSIÓN

La presente revisión sistemática analizó 65 estudios publicados entre 2021 y 2025 para identificar la efectividad de las estrategias de ciberseguridad en la nube. Los hallazgos revelan un cambio de paradigma donde la protección de datos ha dejado de ser una disciplina estática basada únicamente en claves criptográficas para convertirse en un ecosistema dinámico impulsado por inteligencia artificial y enfoques híbridos. A continuación, se contrastan estos resultados con la literatura existente.

En este contexto, nuestros resultados indican que la criptografía se mantiene como la estrategia predominante utilizada en el 49% de los estudios analizados. Esto coincide con la literatura general, la cual sigue considerando a la criptografía como el pilar central para asegurar la transmisión y prevenir accesos no autorizados [81]. Sin embargo, se observa una disonancia crítica ya que, mientras nuestra revisión halló que la criptografía clásica es popular, otras investigaciones advierten que técnicas avanzadas como el cifrado homomórfico pueden hacer los procesos considerablemente más lentos [82]. Esto explica la razón por la cual la industria busca alternativas más ligeras para entornos IoT con recursos limitados [83], [84].

De manera simultánea, el hallazgo de que el 38% de los estudios ya implementan Inteligencia Artificial confirma la tendencia ascendente reportada en revisiones externas, las cuales posicionan a esta tecnología como fundamental para la detección dinámica de amenazas [85]. No obstante, nuestra revisión sugiere un optimismo que debe ser matizado. Mientras que nuestros estudios primarios reportan altas tasas de éxito, revisiones externas alertan sobre la vulnerabilidad de estos sistemas ante ataques adversarios y el riesgo de sobreajuste [86]. Tal situación sugiere que la alta efectividad reportada en entornos controlados podría disminuir en escenarios reales, lo que refuerza la necesidad de los enfoques híbridos detectados en el 42% de nuestra muestra para equilibrar la escalabilidad de la IA con la robustez de la criptografía [87].

Por otro lado, resulta paradójico que el acceso no autorizado y los ataques de denegación de servicio sigan siendo las amenazas más reportadas en esta revisión a pesar de la sofisticada tecnología actual. La literatura externa ofrece una explicación estructural para este fenómeno al argumentar que esto no se debe solo a fallos de software, sino a la limitación de recursos en dispositivos IoT que impide la implementación de protocolos de seguridad robustos [88], [89]. Además, la naturaleza descentralizada de las arquitecturas de computación en la niebla crea nuevas superficies de ataque que los escáneres de vulnerabilidades convencionales no logran detectar, dejando pasar amenazas desconocidas [90].

Asimismo, un hallazgo notable de este trabajo fue la baja adopción de Blockchain y de soluciones para amenazas cuánticas. Respecto a Blockchain, la literatura externa justifica este bajo porcentaje al citar problemas de rendimiento en tiempo real [91]. Diversos autores señalan que, aunque Blockchain garantiza integridad, su alta latencia y sobrecarga computacional lo hacen poco práctico para sistemas de nube que requieren alta velocidad, por lo que suele relegarse a tareas de auditoría fuera

de la cadena principal [92]. En contraste, el interés incipiente en amenazas cuánticas detectado en nuestro estudio parece ser solo el inicio de una tendencia mayor, pues existe una urgencia creciente de migrar hacia una criptografía post-cuántica ligera [84].

Quizás el aspecto más crítico revelado por esta RSL es que más de la mitad de los estudios prioriza métricas de eficiencia como el uso de CPU y tiempo, mientras que un porcentaje muy bajo se enfoca en métricas puras de seguridad. Esta tendencia es cuestionada por revisiones externas que argumentan que las métricas de precisión superiores al 90% suelen estar infladas por el uso de conjuntos de datos obsoletos o sintéticos que no reflejan la complejidad de los ataques modernos [93]. Esto revela un posible sesgo metodológico en la comunidad científica actual donde se estaría optimizando la velocidad de los algoritmos de seguridad en detrimento de la validación de su robustez real y ética [94].

Finalmente, el hecho de que una gran parte de los estudios revisados presente limitaciones de validez externa concuerda con las críticas sobre la dependencia excesiva de simuladores [93]. La falta de validación en infraestructuras de nube comerciales y la escasez de conjuntos de datos diversos y actuales limitan la capacidad de generalizar los resultados obtenidos en laboratorio a entornos empresariales reales [95].

En conclusión, el principal aporte de esta revisión sistemática consiste en evidenciar la desconexión existente entre la teoría académica y la práctica operativa. Se identificó que, mientras la literatura científica continúa produciendo soluciones aisladas evaluadas en entornos ideales, los desafíos actuales de la nube requieren arquitecturas híbridas validadas bajo condiciones de estrés real. De esta manera, este hallazgo redirige el enfoque de la discusión desde la mera innovación algorítmica hacia la validación práctica de las soluciones, lo cual proporciona una nueva hoja de ruta para futuras investigaciones en ciberseguridad.

V. CONCLUSIONES

Durante esta revisión se evidenció que, entre 2021 y 2025, las estrategias de seguridad en la nube han pasado por un proceso de cambio que no ha sido menor. Durante esos años, la protección de datos dejó de apoyarse exclusivamente en mecanismos rígidos basados en el cifrado y comenzó a incorporar enfoques más adaptativos, pensados para responder a entornos que evolucionan con rapidez. El cifrado sigue siendo un elemento fundamental, pero ya no se percibe como una solución suficiente por sí misma, sino como una pieza que necesita integrarse con tecnologías más dinámicas. La incorporación de técnicas basadas en inteligencia artificial y aprendizaje automático ha comenzado a ocupar un lugar central, sobre todo porque permiten identificar comportamientos anómalos antes de que se conviertan en incidentes críticos.

En cuanto a los resultados más relevantes, se observa que las áreas más expuestas continúan siendo el control de acceso y la disponibilidad de los servicios. Los accesos no autorizados y los ataques de denegación de servicio persisten incluso en organizaciones que han adoptado tecnologías avanzadas. Esto no

se debe únicamente a fallas técnicas; gran parte del problema tiene que ver con que los modelos de seguridad tradicionales no han logrado adaptarse del todo a arquitecturas distribuidas como las que se usan hoy, por ejemplo, en aplicaciones que integran IoT o computación en la niebla. En otras palabras, migrar a la nube sin revisar los procedimientos de gestión del tráfico y los mecanismos de control termina reproduciendo vulnerabilidades ya conocidas.

Respecto a los aportes y limitaciones de esta revisión, queda claro que la mayoría de los estudios recientes ponen más atención en medir la eficiencia computacional de las soluciones que en evaluar su seguridad en condiciones reales. En varios de los estudios analizados se observa una tendencia clara: muchas de las soluciones propuestas se prueban únicamente en entornos simulados o altamente controlados. Esto genera una dificultad evidente, porque resulta complicado prever si esos enfoques funcionarían igual de bien en sistemas reales, donde la carga de trabajo es constante y los incidentes no siguen patrones predecibles. Esta separación entre lo que se prueba en la investigación y lo que realmente ocurre en las organizaciones termina siendo un obstáculo importante para que las nuevas herramientas o modelos puedan adoptarse con confianza.

Pensando en lo que podría trabajarse más adelante, no bastaría con seguir creando algoritmos cada vez más complejos. Sería más útil contar con formas de evaluación que permitan comparar resultados y validar soluciones en condiciones que reflejen el funcionamiento real de la infraestructura empresarial. Además, el avance de la computación cuántica introduce un desafío adicional. En ese contexto, se vuelve necesario acelerar el análisis y la puesta a prueba de alternativas de cifrado post-cuántico que también puedan funcionar en equipos con recursos limitados.

REFERENCIAS

- [1] L. Bautista-Villalpando y A. Abran, "A data security framework for cloud computing services," *Comput. Syst. Sci. Eng.*, vol. 37, no. 2, pp. 203–218, 2021.
- [2] I. Gupta, A. K. Singh, C.-N. Lee y R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," *IEEE Access*, vol. 10, pp. 71247–71277, 2022.
- [3] K. Anand, A. Vijayaraj y M. Vijay Anand, "An enhanced bacterial foraging optimization algorithm for secure data storage and privacy-preserving in cloud," *Peer-to-Peer Netw. Appl.*, vol. 15, pp. 2007–2020, 2022.
- [4] T. W. Kim, A. El Azzaoui, B. Koh, J. Kim y J. H. Park, "A secret sharing-based distributed cloud system for privacy protection," *Hum.-Centric Comput. Inf. Sci.*, vol. 12, Art. no. 20, 2022.
- [5] R. Brison, H. Wimmer y C. M. Rebman Jr., "Botnet intrusion detection: A modern architecture to defend a virtual private cloud," *Issues Inf. Syst.*, vol. 23, no. 3, pp. 114–127, 2022.
- [6] K. Gai, M. Qiu y H. Zhao, "Privacy-preserving data encryption strategy for big data in mobile cloud computing," *IEEE Trans. Big Data*, vol. 7, no. 4, pp. 678–688, 2021.
- [7] R. Adey y H. Mouratidis, "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography," *Sensors*, vol. 22, no. 3, Art. no. 1109, 2022.
- [8] T. Kamble, M. Ghuge, R. Jain y S. V. Gumaste, "Secure data transmission in cloud computing using a cyber-security trust model with multi-risk protection scheme in smart IoT application," *Cluster Comput.*, vol. 28, p. 79, 2025.
- [9] R. Montasari, S. Macdonald, A. Hosseini-Far, F. Carroll y A. Daneshkhan, "Network and hypervisor-based attacks in cloud computing environments," *Int. J. Electron. Secur. Digit. Forensics*, vol. 13, no. 6, pp. 630–651, 2021.
- [10] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas y A. Rekeraho, "Enhancing cloud security—Proactive threat monitoring and detection using a SIEM-based approach," *Appl. Sci.*, vol. 13, no. 22, Art. no. 12359, 2023.
- [11] R. Siyal et al., "Adaptive attribute-based honey encryption: A novel solution for cloud data security," *Comput. Mater. Contin.*, vol. 82, no. 2, pp. 2637–2664, 2025.
- [12] C. Choudhary, N. Vyas y U. Kumar Lilhore, "Cloud security: Challenges and strategies for ensuring data protection," en *Proc. 2023 Int. Conf. Innov. Comput., Technol. and Appl. (ICTACS)*, 2023.
- [13] M. Akbar, M. M. Waseem, S. H. Mehanoor y P. Barmavatu, "Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing," *Cluster Comput.*, vol. 27, pp. 9091–9105, 2024.
- [14] A. R. A. Abusalih, K. Saravanan, B. B. Abirami, V. S. Pandi, V. V. Arulandam y S. Parthiban, "Enhancing cloud security with AI: Developing robust, scalable solutions for threat mitigation and data protection in cloud platforms," en *Proc. 2024 Int. Conf. Smart Comput., Netw. and Appl. (ICSCNA)*, Tirunelveli, India, 2024.
- [15] A. Wairagade, R. Sonani y V. Govindarajan, "AI based methods for insider threats detection for cloud risk mitigation," en *Proc. 2024 Int. Conf. IT Innov. and Knowl. Discovery (ITIKD)*, Manama, Bahrain, 2025.
- [16] W. Duan, Y. Jiang, X. Xu, Z. Zhang, and G. Liu, "An Edge Cloud Data Integrity Protection Scheme Based on Blockchain," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/5016809.
- [17] H. C. Ukwuoma, A. J. Gabriel, A. F. B. Thompson, and B. K. Alese, "Post-quantum cryptography-driven security framework for cloud computing," *Open Computer Science*, vol. 12, no. 1, pp. 142–153, 2022, doi: 10.1515/comp-2022-0235.
- [18] M. N. Ul Haq and N. Kumar, "A novel data classification-based scheme for cloud data security using various cryptographic algorithms," *International Review of Applied Sciences and Engineering*, vol. 13, no. 2, pp. 107–116, 2022, doi: 10.1556/1848.2021.00317.
- [19] F. J. Abdullayeva, "Distributed denial of service attack detection in E-government cloud via data clustering," *Array*, vol. 15, 2022, doi: 10.1016/j.array.2022.100229.
- [20] M. Mageshwari and R. Nareesh, "Improved Sunflower Optimization Algorithm Based Encryption with Public Auditing Scheme in Secure Cloud Computing," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 6, pp. 13–23, 2023, doi: 10.22266/ijies2023.1231.02.
- [21] L. Yu, M. He, H. Liang, L. Xiong, and Y. Liu, "A Blockchain-Based Authentication and Authorization Scheme for Distributed Mobile Cloud Computing Services," *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031264.
- [22] K. Riad, "Token-Revocation Access Control to Cloud-Hosted Energy Optimization Utility for Environmental Sustainability," *Applied Sciences (Switzerland)*, vol. 13, no. 5, 2023, doi: 10.3390/app13053142.
- [23] A. V. S. Siva Rama Rao, T. Kavarakuntla, S. Kanipakam, T. Murari, K. P. Kumar, and B. S. Kumar, "Blockchain-Backed Verification Systems for Enhanced Interoperability and Trust in Managing Legal Documents across Multi-Cloud Environments," *Journal of Electrical Systems*, vol. 19, no. 4, pp. 254–269, 2023, doi: 10.52783/jes.637.
- [24] M. Sumathi, S. P. Raja, N. Vijayaraj, and M. Rajkamal, "Healthcare Data Collection Using Internet of Things and Blockchain Based Decentralized Data Storage," *Advances in Distributed Computing and Artificial Intelligence Journal*, vol. 12, no. 1, 2023, doi: 10.14201/adcaij.28612.
- [25] M. Ali, L. Tang Jung, A. H. Sodhro, A. Ali Laghari, S. B. Belhaouari, and Z. Gillani, "A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security," *Alexandria Engineering Journal*, vol. 64, pp. 749–760, 2023, doi: 10.1016/j.aej.2022.10.056.
- [26] N. R. Alharbe, A. A. Aljohani, M. A. Rakrouki, and M. M. Khayyat, "An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud," *Applied Sciences (Switzerland)*, vol. 13, no. 5, 2023, doi: 10.3390/app13053187.
- [27] A. Abdo, T. S. Karamany, and A. E. Yakoub, "A hybrid approach to secure and compress data streams in cloud computing environment," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 3, 2024, doi: 10.1016/j.jksuci.2024.101999.
- [28] A. A. Hema Ambiha and R. Pragaladan, "Enhancing healthcare data security in cloud environments with dual authentication and optimal key-tuned encryption; Повышение безопасности медицинских данных в облачных средах с помощью двойной аутентификации и оптимального шифрования с настройкой ключей," *Scientific and Technical Journal of*

- Information Technologies, Mechanics and Optics*, vol. 24, no. 3, pp. 456–463, 2024, doi: 10.17586/2226-1494-2024-24-3-456-463.
- [29] S. A. Alasmari, “Optimized Blockchain-Based Deep Learning Model for Cloud Intrusion Detection,” *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 9, pp. 914–925, 2024, doi: 10.14569/IJACSA.2024.0150994.
 - [30] V. Ananthakrishna and C. S. Yadav, “QP-ChainSZKP: A Quantum-Proof Blockchain Framework for Scalable and Secure Cloud Applications,” *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 1, pp. 162–180, 2024, doi: 10.22399/ijcesen.718.
 - [31] G. J. Rosline and P. Vimala Rani, “Intrusion detection system for cloud environment based on convolutional neural networks and PSO algorithm,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 35, no. 3, pp. 1499–1506, 2024, doi: 10.11591/ijeecs.v35.i3.pp1499-1506.
 - [32] A. Jeneba Mary, K. Kuppusamy, and A. Senthilrajan, “Multi-layer access control for cloud data using improved DBSCAN, AES, homomorphic encryption, and RMAAC for text, image, and video,” *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 1, pp. 249–260, 2024, doi: 10.22399/ijcesen.837.
 - [33] H. Wang, Y. Zhang, X. A. Wang, and X. Yang, “An improved identity-based public audit protocol for cloud storage,” *Heliyon*, vol. 10, no. 16, 2024, doi: 10.1016/j.heliyon.2024.e36273.
 - [34] P. Gantela and B. B. Basaveswara Rao, “CULTIVATING RESILIENCE: A TRANSFORMATIVE APPROACH TO ENHANCING CLOUD DATA SECURITY WITH TRANSFORMER-BASED TECHNIQUES,” *Proceedings on Engineering Sciences*, vol. 6, no. 4, pp. 1551–1560, 2024, doi: 10.24874/PES06.04.014.
 - [35] C. Chang, S. Xu, K. Gao, and C. C. Chang, “Cryptanalysis of Dual-Stage Permutation Encryption Using Large-Kernel Convolutional Neural Network and Known Plaintext Attack,” *Cryptography*, vol. 8, no. 3, 2024, doi: 10.3390/cryptography8030041.
 - [36] R. Vallabhaneni, S. A. Vaddadi, S. E. Vadakkethil Somanathan Pillai, S. R. Addula, and B. Ananthan, “MobileNet based secured compliance through open web application security projects in cloud system,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 35, no. 3, pp. 1661–1669, 2024, doi: 10.11591/ijeecs.v35.i3.pp1661-1669.
 - [37] K. Samunnisa, S. V. K. Gaddam, and K. Madhavi, “Design and Evaluation of a Quantum-Resilient Cryptographic Framework for Enhancing Security and Efficiency in Distributed Cloud Environments,” *SSRG International Journal of Electrical and Electronics Engineering*, vol. 11, no. 7, pp. 1–22, 2024, doi: 10.14445/23488379/IJEEE-V11I7P101.
 - [38] T. H. Hadi, “Deep Learning-based DDoS Detection in Network Traffic Data,” *International Journal of Electrical and Computer Engineering Systems*, vol. 15, no. 5, pp. 407–414, 2024, doi: 10.32985/ijeecs.15.5.3.
 - [39] A. Triakosia, P. Rizomiliotis, C. Tonelli, F. Federici, and V. Senni, “Secure outsourcing of manufacturing compliance checks,” *International Journal of Information Security*, vol. 23, no. 1, pp. 609–627, 2024, doi: 10.1007/s10207-023-00747-2.
 - [40] J. Zhang and A. Datta, “Blockchain-enabled data governance for privacy-preserved sharing of confidential data,” *PeerJ Computer Science*, vol. 10, 2024, doi: 10.7717/peerj.cs.2581.
 - [41] J. V. S. Arundathi and V. Satyanarayana, “A Secure and Efficient Framework for Multi-User Encrypted Cloud Databases Supporting Single and Multiple Keyword Searches,” 2024. [Online]. Available: www.ijacsa.thesai.org
 - [42] S. S. Bulbul, Z. A. Abduljabbar, D. F. Najem, V. O. Nyangaresi, J. Ma, and A. J. Y. Aldarwish, “Fast Multi-User Searchable Encryption with Forward and Backward Private Access Control,” *Journal of Sensor and Actuator Networks*, vol. 13, no. 1, 2024, doi: 10.3390/jsan13010012.
 - [43] Z. A. Mohammed, H. Q. Gheni, Z. J. Hussein, and A. K. M. Al-Qurabat, “Advancing Cloud Image Security via AES Algorithm Enhancement Techniques,” *Engineering, Technology and Applied Science Research*, vol. 14, no. 1, pp. 12694–12701, 2024, doi: 10.48084/etasr.6601.
 - [44] I. AlSaleh, A. Al-Samawi, and L. A. Nissirat, “Novel Machine Learning Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements,” *Sensors*, vol. 24, no. 5, 2024, doi: 10.3390/s24051418.
 - [45] M. Xu *et al.*, “AHAC: Advanced Network-Hiding Access Control Framework,” *Applied Sciences (Switzerland)*, vol. 14, no. 13, 2024, doi: 10.3390/app14135593.
 - [46] J. Shaikh, T. A. Syed, D. S. A. Shah, S. Jan, Q. U. Ain, and P. K. Singh, “Advancing DDoS attack detection with hybrid deep learning: integrating convolutional neural networks, PCA, and vision transformers,” *International Journal on Smart Sensing and Intelligent Systems*, vol. 17, no. 1, 2024, doi: 10.2478/ijssis-2024-0040.
 - [47] V. K. Soman and V. Natarajan, “Crayfish optimization based pixel selection using block scrambling based encryption for secure cloud computing environment,” *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-86956-2.
 - [48] T. le Vinh, H. Thien Tran, and S. Bouzeffrane, “Enhancing Property-Based Token Attestation With Homomorphic Encryption (PTA-HE) for Secure Mobile Computing,” 2025, doi: 10.1109/ACCESS.2024.0429000.
 - [49] T. Ananthi and A. Sivasangari, “VFHE-DWOA: A Cloud-Based Secure Medical Data Storage and Transmission Model,” *SSRG International Journal of Electronics and Communication Engineering*, vol. 12, no. 5, pp. 310–326, 2025, doi: 10.14445/23488549/IJEE-V12I5P127.
 - [50] P. K. R. Kumar and B. A. Usha, “Geometric Cryptosystem Based Elliptic Curve Cryptography and Advanced Encryption Standard with Galois Counter Mode for Secure Cloud Storage,” *International Journal of Computer Networks and Applications*, vol. 12, no. 3, pp. 324–335, 2025, doi: 10.22247/ijcna/2025/21.
 - [51] O. Ascue, O. Valle, and J. Santisteban, “BLOCKSAGE: Blockchain-Based Cloud Architecture for Sensitive Data Management in SMEs,” *Sustainability (Switzerland)*, vol. 17, no. 4, 2025, doi: 10.3390/su17041352.
 - [52] U. K. Lilhore *et al.*, “SmartTrust: a hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture,” *Journal of Cloud Computing*, vol. 14, no. 1, 2025, doi: 10.1186/s13677-025-00764-7.
 - [53] K. Sasikumar and N. Sivakumar, “Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques,” *IEEE Open Journal of the Computer Society*, vol. 6, pp. 392–402, 2025, doi: 10.1109/OJCS.2025.3538557.
 - [54] S. A. Alzakari *et al.*, “Heuristically enhanced multi-head attention based recurrent neural network for denial of wallet attacks detection on serverless computing environment,” *Scientific Reports*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-87636-x.
 - [55] C. Regueiro-Senderos and B. Urquiza, “Blockchain-Based Evidence Trustworthiness System in Certification,” *Journal of Cybersecurity and Privacy*, vol. 5, no. 1, 2025, doi: 10.3390/jcp5010001.
 - [56] J. Jayachandran, D. Sam, and K. Nataraj, “Efficient Cloud Computing Security Using Hybrid Optimized AES-IQCP-ABE Cryptography Algorithm,” *International Journal of Computer Network and Information Security*, vol. 17, no. 2, pp. 101–114, Apr. 2025, doi: 10.5815/ijcnis.2025.02.07.
 - [57] K. Mahendar and G. Shivakanth, “A Performance Analysis of ML-Based Intrusion Detection Systems in Cloud Environments,” *International Journal of Electrical and Electronic Engineering and Telecommunications*, vol. 14, no. 4, pp. 243–252, Jul. 2025, doi: 10.18178/ijeetc.14.4.243-252.
 - [58] P. S. R. Chandra, P. Syamala Rao, K. Nareesh, and R. Malladi, “PSR: An Improvement of Lightweight Cryptography Algorithm for Data Security in Cloud Computing,” *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 1, pp. 1053–1058, 2025, doi: 10.14569/IJACSA.2025.01601101.
 - [59] P. Dahiwal and V. Khare, “Strengthening Security in Clouds Through Cloud Computing Authentication Using Facial Image Forensics,” *Journal of Computational and Cognitive Engineering*, vol. 4, no. 2, pp. 151–160, 2025, doi: 10.47852/bonviewJCCE52024248.
 - [60] S. Wang and L. Zhao, “A multi-factor access scheme for online english teaching system based on cloud computing,” *Alexandria Engineering Journal*, vol. 120, pp. 505–514, 2025, doi: 10.1016/j.aej.2025.01.131.
 - [61] A. N. Banu and S. K. B. Sangeetha, “Intruder: A Multi Module Distributed Explainable IDS/IPS for Securing Cloud Environment,” *Computers, Materials and Continua*, vol. 82, no. 1, pp. 579–607, 2025, doi: 10.32604/cmc.2024.059805.
 - [62] L. Ben-Shimol *et al.*, “Detection of compromised functions in a serverless cloud environment,” *Computers and Security*, vol. 150, 2025, doi: 10.1016/j.cose.2024.104261.
 - [63] S. Pang, J. Wen, S. Liang, and B. Huang, “FICConvNet: A Privacy-Preserving Framework for Malware Detection Using CKKS Homomorphic Encryption,” *Electronics (Switzerland)*, vol. 14, no. 10, 2025, doi: 10.3390/electronics14101982.
 - [64] P. Balasubramanian, S. Nazari, D. K. Kholgh, A. B. Z. Mahmoodi, J. Seby, and P. A. Kostakos, “A cognitive platform for collecting cyber threat

- intelligence and real-time detection using cloud computing," *Decision Analytics Journal*, vol. 14, 2025, doi: 10.1016/j.dajour.2025.100545.
- [65] M. J. Josepha and M. S. Christo, "A unified elliptic curve cryptographic algorithm for secure communication and homomorphic encryption: A multi-parameter (Built-in CIA) Approach," *Results in Engineering*, vol. 26, 2025, doi: 10.1016/j.rineng.2025.105354.
- [66] A. Mahmoud As'Ad Alnaser, H. M. D. S. Hatamleh, N. A. Almolhis, S. Duraibi, and Y. M. AlQahtani, "Secure Quantum Communication With Multi-Users in Quantum Networks," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 2397–2419, 2025, doi: 10.1109/OJCOMS.2025.3556903.
- [67] K. Nidadavolu and S. Giddaluru, "Adaptive Deep Learning Architectures for Enhanced Cloud-based Intrusion Detection and Behavioral User Authentication," *International Journal of Intelligent Engineering and Systems*, vol. 18, no. 5, pp. 54–71, 2025, doi: 10.22266/ijies.2025.0630.05.
- [68] D. N. Kashyap, K. R. Naikade, A. K. Kumar Pandey, N. K. Sharma, S. Hashmi, and S. S. Pund, "Enhancing Credit Card Data Security Using AI-integrated Encryption and Tokenization Framework," *Journal of Internet Services and Information Security*, vol. 15, no. 1, pp. 316–329, 2025, doi: 10.58346/JISIS.2025.11.020.
- [69] S. Badran, N. M. Arman, and M. Farajallah, "A Method for Secure Data Outsourcing Utilizing Hybrid Data Partitioning," *International Journal of Computing and Digital Systems*, vol. 18, no. 1, 2025, doi: 10.12785/ijcds/1571110931.
- [70] Y. Cao, "Research on the Application of Blockchain Technology in the Security Protection of Sensitive Data in Information Systems," *Journal of Mobile Multimedia*, vol. 14, no. 1, pp. 205–228, 2025, doi: 10.13052/jcsm2245-1439.1419.
- [71] H. Wasswa, H. A. Abbass, and T. M. Lynar, "ResDNViT: A hybrid architecture for Netflow-based attack detection using a residual dense network and Vision Transformer," *Expert Systems with Applications*, vol. 282, 2025, doi: 10.1016/j.eswa.2025.127504.
- [72] F. Wang and S. Xie, "Cybersecurity in Cloud Computing AI-Driven Intrusion Detection and Mitigation Strategies," *IEEE Access*, vol. 13, pp. 108051–108058, 2025, doi: 10.1109/ACCESS.2025.3580569.
- [73] T. S. Kumar, P. Sharma, X. Cheng, S. Lalar, S. Kumar, and S. R. Bansal, "Enhanced Triple Layered Approach for Mitigating Security Risks in Cloud," *Computers, Materials and Continua*, vol. 83, no. 1, pp. 719–738, 2025, doi: 10.32604/cmc.2025.060836.
- [74] J. J. Menandas and M. Subaja, "An Efficient Integrity and Authenticated Elliptic Curve Cryptography Algorithm for Secure Storage and Routing in TLS/SSL," *International Arab Journal of Information Technology*, vol. 22, no. 5, pp. 859–872, 2025, doi: 10.34028/iajit/22/5/2.
- [75] S. Punitha and K. S. Preetha, "Enhancing reliability and security in cloud-based telesurgery systems leveraging swarm-evoked distributed federated learning framework to mitigate multiple attacks," *Scientific Reports*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-12027-1.
- [76] K. Gupta *et al.*, "An Intelligent Quantum Cyber-Security Framework for Healthcare Data Management," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 6884–6895, 2025, doi: 10.1109/TASE.2024.3456209.
- [77] K. Bıçakçı, M. Sekmen, and Y. Uzunay, "Balancing Security and Usability in Enterprise FIDO Passkey Recovery With Peer Assistance," *IEEE Access*, vol. 13, pp. 150415–150425, 2025, doi: 10.1109/ACCESS.2025.3602362.
- [78] K. Wang, S. Wu, Y. Cui, Z. Huang, H. Fan, and H. Jin, "System log isolation for containers," *Frontiers of Computer Science*, vol. 19, no. 5, 2025, doi: 10.1007/s11704-024-2568-8.
- [79] F. Razvan and M. Craus, "Enhancing network security through integration of game theory in software-defined networking framework," *International Journal of Information Security*, vol. 24, no. 3, 2025, doi: 10.1007/s10207-025-01012-4.
- [80] Q. Chen *et al.*, "Shadowkube: enhancing Kubernetes security with behavioral monitoring and honeypot integration," *Cybersecurity*, vol. 8, no. 1, 2025, doi: 10.1186/s42400-025-00372-7.
- [81] K. S. Alqahtani, A. M. Albalawi y M. Frikha, "Reviewing of cybersecurity threats, attacks, and mitigation techniques in cloud computing environment," *J. Theor. Appl. Inf. Technol.*, vol. 101, no. 6, pp. 2058–2066, 2023.
- [82] S. Ali *et al.*, "Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions," *Comput. Secur.*, vol. 157, p. 104599, 2025, doi: 10.1016/j.cose.2025.104599.
- [83] M. Mamdouh, A. I. Awad, A. A. M. Khalaf y H. F. A. Hamed, "Authentication and identity management of IoT devices: Achievements, challenges, and future directions," *Comput. Secur.*, vol. 111, p. 102491, Dic. 2021, doi: 10.1016/j.cose.2021.102491.
- [84] M. Almutairi y F. T. Sheldon, "IoT-cloud integration security: A survey of challenges, solutions, and directions," *Electronics*, vol. 14, no. 7, p. 1394, Mar. 2025, doi: 10.3390/electronics14071394.
- [85] T. H. H. Aldhyani y H. Alkahtani, "Generative AI for cybersecurity: A comprehensive review," *Appl. Sci.*, vol. 15, no. 7, p. 3036, Mar. 2025, doi: 10.3390/app15073036.
- [86] Z. M. S. Saeed, A. B. Zainal, F. A. Ghaleb y B. A. S. Al-rimy, "Enhancing public cloud resilience: An analytical review of detection and mitigation strategies against economic denial of sustainability attacks," *Discov. Internet Things*, vol. 5, no. 1, p. 79, Jul. 2025, doi: 10.1007/s43926-025-00183-9.
- [87] M. Y. Arafat *et al.*, "Enhancing security in cloud-based IoT systems through blockchain and deep learning: A comprehensive survey," *Comput. Electr. Eng.*, vol. 122, p. 109937, 2025, doi: 10.1016/j.compeleceng.2025.109937.
- [88] M. M. Hossain *et al.*, "A holistic analysis of internet of things (IoT) security: Principles, practices, and new perspectives," *Future Internet*, vol. 16, no. 4, p. 110, Mar. 2024, doi: 10.3390/fi16040110.
- [89] N. Farhadighalati, L. A. Estrada-Jimenez, S. Nikghadam-Hojjati y J. Barata, "A systematic review of access control models: Background, existing research, and challenges," *IEEE Access*, vol. 13, pp. 17777–17806, Ene. 2025, doi: 10.1109/ACCESS.2025.3533145.
- [90] N. Kaur, "A systematic review on security aspects of fog computing environment: Challenges, solutions and future directions," *Comput. Sci. Rev.*, vol. 54, p. 100688, Nov. 2024, doi: 10.1016/j.cosrev.2024.100688.
- [91] L. Albshaier, A. Budokhi y A. Aljughaiman, "A review of security issues when integrating IoT with cloud computing and blockchain," *IEEE Access*, vol. 12, pp. 109560–109595, 2024, doi: 10.1109/ACCESS.2024.3436536.
- [92] S. Das, R. Priyadarshini, M. Mishra y R. K. Barik, "Leveraging towards access control, identity management, and data integrity verification mechanisms in blockchain-assisted cloud environments: A comparative study," *J. Cybersecur. Priv.*, vol. 4, no. 4, pp. 1018–1043, Dic. 2024, doi: 10.3390/jcp4040047.
- [93] S. R. Mishra, B. Shanmugam, K. C. Yeo y S. Thennadil, "SDN-enabled IoT security frameworks—A review of existing challenges," *Technologies*, vol. 13, no. 3, p. 121, Mar. 2025, doi: 10.3390/technologies13030121.
- [94] M. M. Ahmed *et al.*, "The ethics of data mining in healthcare: Challenges, frameworks, and future directions," *BioData Min.*, vol. 18, no. 1, p. 47, Jul. 2025, doi: 10.1186/s13040-025-00461-w.
- [95] O. Afolalu y M. S. Tsoeu, "Enterprise networking optimization: A review of challenges, solutions, and technological interventions," *Future Internet*, vol. 17, no. 4, p. 133, Mar. 2025, doi: 10.3390/fi17040133.