Revista Peruana de Computación y Sistemas 2024 6(2):65-77
https://doi.org/10.15381/rpcs.v6i2.28914

ISSN Online: 2617-2003
Facultad de Ingeniería de Sistemas e Informática
Universidad Nacional Mayor de San Marcos

Artículo de Revisión

Almacenamiento de la Evidencia Digital usando Cloud Computing - Una Revisión Sistemática de la Literatura

Digital Evidence Storage Using Cloud Computing - A Systematic Literature Review

Absalón Portocarrero Burgos[1,a], Javier Gamboa Cruzado[1,b], Javier Seclen[1,c]

[1] Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática. Lima, Perú

[a] Autor de correspondencia: absalon.portocarrero@unmsm.edu.pe, ORCID: https://orcid.org/0000-0001-6161-061X

[b] E-mail: jgamboac@unmsm.edu.pe, ORCID: https://orcid.org/0000-0002-0461-4152

[c] E-mail: jseclena@unmsm.edu.pe, ORCID: https://orcid.org/0000-0002-6773-5031

Resumen

El empleo de Cloud Computing y su impacto en el almacenamiento de evidencia digital en entidades que administran justicia representa actualmente un reto importante sobre los enfoques tradicionales. El objetivo de este estudio fue llevar a cabo una revisión sistemática de la literatura sobre el almacenamiento de la evidencia digital usando Cloud Computing entre los años 2016 y 2022. La estrategia de búsqueda empleada identificó 5754 estudios de bibliotecas digitales, entre las cuales se incluyen a Google Scholar, ARDI, IEEE Xplore, ProQuest, ScienceDirect, Scopus, entre otros. De estos, se seleccionaron 100 artículos basados en criterios de exclusión mediante el método PRISMA. Los resultados de la revisión sistemática se han centrado en estudios recientes acerca del almacenamiento de la evidencia digital usando Cloud Computing. En 2019 se registró la mayor cantidad de publicaciones relacionadas con la investigación. Entre los países que contribuyen con más artículos sobre el tema se encuentran India y Estados Unidos, y Amazon Web Services se destaca como el principal proveedor de servicios de Cloud Computing. Además, proporciona un mapeo de los estudios extraídos, métricas, tendencias, principales proveedores, modelos de servicios, métodos de validación para comparar la relevancia en sus diversos entornos y conclusiones.

Palabras clave: Computación en la nube, Evidencia digital, Almacenamiento, Informática forense, Revisión sistemática de la Literatura

Abstract

The use of Cloud Computing and its impact on digital evidence storage in justice-administering entities currently represents a significant challenge compared to traditional approaches. The aim of this study was to conduct a systematic literature review on digital evidence storage using Cloud Computing between 2016 and 2022. The search strategy employed identified 5754 studies from digital libraries, including Google Scholar, ARDI, IEEE Xplore, ProQuest, ScienceDirect, Scopus, among others. From these, 100 articles were selected based on exclusion criteria using the PRISMA method. The results of the systematic review focused on recent studies regarding digital evidence storage using Cloud Computing. In 2019, the highest number of publications related to the research was recorded. Among the countries contributing the most articles on the topic are India and the United States, with Amazon Web Services standing out as the leading provider of Cloud Computing services. Additionally, it provided a mapping of the extracted studies, metrics, trends, major providers, service models, validation methods for comparing relevance in various contexts, and conclusions.

Keywords: Cloud Computing, Digital Evidence, Storage, Forensic Computing, Systematic Literature Review

Recibido: 05-09-2024 - Aceptado: 16-12-2024 - Publicado: 30-12-2024

Citar como:
Portocarrero Burgos, A., Gamboa Cruzado, J. & Seclen, J. (2024). Almacenamiento de la Evidencia Digital usando Cloud Computing - Una Revisión Sistemática de la Literatura. Revista Peruana de Computación y Sistemas, 6(2):65-77. https://doi.org/10.15381/rpcs.v6i2.28914

1. Introducción

Parece que cualquier barrera potencial al crecimiento de Cloud Computig ya es historia, puesto que el uso de servicios y soluciones de Cloud Computing se ha consolidado. Se ha borrado cualquier escepticismo respecto al uso de Cloud Computing, y las mismas empresas ya están apostando por que la solución se base totalmente en la nube, tanto si implantan una nueva tecnología como si renuevan el software o adquieren un nuevo servicio. Las últimas dos décadas han sido testigos de una investigación activa en la definición y evolución de la computación en la nube. . Cloud Computing es un ejemplo de la investigación en sistemas distribuidos desde que se propuso por primera vez el modelo cliente-servidor en 1958 y está impulsada por los avances en redes y arquitecturas distribuidas. Debido a su rápido desarrollo, Cloud Computing se ha convertido en una herramienta ampliamente utilizada en la administración pública, la empresa y la educación, entre otros ámbitos de la sociedad. Las características de la computación en nube han hecho posibles nuevas tecnologías y paradigmas, como el acceso dinámico y medido a un conjunto compartido de recursos informáticos, con el fin de satisfacer las necesidades de desarrollo de aplicaciones en campos como la ciencia, la sanidad, la agricultura, las ciudades inteligentes y la gestión del tráfico [01].

La computación en la nube es la tecnología más atractiva que ofrece beneficios económicos y tecnológicos en los diferentes dominios de prestación de servicios. Sin embargo, la creciente popularidad de los servicios en la nube viene acompañada de preocupaciones sobre la garantía de seguridad de sus diferentes servicios. La aplicación de las propiedades de seguridad en una nube es una tarea desafiante. Diferentes desafíos relacionados con la seguridad a los que se enfrentan los proveedores de servicios en la nube (CSP) o los clientes de servicios en la nube (CSC) [02].

La computación ubicua hace que la conciencia del usuario sea muy compleja. Además, las regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, hacen que el consentimiento y el conocimiento sean obligatorios antes del procesamiento de datos. Por lo tanto, se espera que los procedimientos para recopilar evidencia de cantidades masivas de datos de sistemas cognitivos necesiten procedimientos y técnicas estandarizados internacionales para capturar, almacenar y procesar datos de evidencia. Este tema es particularmente relevante porque las ciudades cognitivas pueden convertirse en blanco de delitos cibernéticos y terrorismo. En este sentido, la Unión Europea está desarrollando actualmente varias iniciativas en torno a tecnologías para mejorar la lucha contra el crimen y el terrorismo, como el proyecto LOCARD, que tiene como objetivo proporcionar una plataforma para el aseguramiento de la cadena de custodia a lo largo del flujo de trabajo forense, a través de una cadena de bloques. plataforma distribuida de confianza que permite el almacenamiento de metadatos de pruebas digitales [03].

La computación en la niebla es un nuevo modelo de computación que surgió recientemente para complementar el sistema de computación en la nube. Su aparición se atribuye al aumento de la computación en Internet, la expansión web y el crecimiento de la complejidad debido al aumento de nuevas tecnologías y soluciones. La necesidad de procesamiento de datos y demandas de almacenamiento también está aumentando astronómicamente. Para abordar este fenómeno, se debe desarrollar una arquitectura web que satisfaga las necesidades de procesamiento de datos del usuario. Desde entonces, la computación en la nube se ha considerado la principal integración del sistema de Internet debido a su poder de cálculo y almacenamiento que otros dispositivos informáticos no poseen. Sin embargo, la centralización de los servicios en la nube lo ralentiza al proporcionar una respuesta oportuna y soporte de movilidad, lo que crea un retraso entre la solicitud del usuario y las respuestas en la nube. Sin embargo, la centralización de los servicios en la nube lo ralentiza al proporcionar una respuesta oportuna y soporte de movilidad, lo que crea un retraso entre la solicitud del usuario y las respuestas en la nube. Por esta razón, surgió el concepto de computación de borde. La computación perimetral ofrece capacidad computacional y de almacenamiento, al igual que la nube, pero está más cerca del usuario final, donde se alojan o generan los datos. El modelo de computación de borde es una arquitectura de varios niveles en los dispositivos de borde ubicados en el centro de datos [04].

Las brechas entre la informática forense y el almacenamiento en la nube representan importantes desafíos para la recopilación, preservación y análisis de evidencia digital. Estas brechas surgen debido a diferencias en el control físico, accesibilidad, políticas de seguridad y las características dinámicas de la nube. Para abordarlas, es necesario desarrollar nuevas herramientas, estándares y procedimientos adaptados a la naturaleza distribuida y segura de la nube, garantizando la integridad de los datos y el cumplimiento de las regulaciones legales. Este análisis realizado resalta la necesidad de adaptar las prácticas forenses y las políticas de almacenamiento digital en la nube a las nuevas tecnologías y desafíos legales, lo que podría mejorar el acceso a la evidencia digital y fortalecer su protección. La escasez de información sobre estas áreas es un desafío creciente, ya que las tecnologías emergentes y el almacenamiento en la nube están transformando la gestión de los datos. Es crucial desarrollar normativas claras y herramientas especializadas para mejorar la accesibilidad y preservación de la evidencia digital, garantizando la calidad de las investigaciones forenses.

De este proceso de revisión de literatura, se tiene en claro que la tecnología Cloud Computing hoy en día ya es una revolución tecnológica. Hay varias revisiones relacionadas acerca de Cloud Computing. Para analizar estas revisiones se han utilizado diferentes técnicas, entre las cuales se pueden mencionar a las redes bibliométricas, nubes de palabras, la objetividad y la polaridad y el

portafolio a partir de los bigramas. Este estudio se centró en identificar el estado del arte sobre el almacenamiento de la evidencia digital usando Cloud Computing.

En este estudio, el background y trabajos relacionados se discuten en la parte II, el proceso de revisión se explica en la sección III, los resultados y discusiones se explican en la sección IV, y las conclusiones y futuras investigaciones se presentan en la sección V.

2. Background y trabajos relacionados

Los servidores de correo, el almacenamiento web y los servicios de alojamiento son ya ejemplos de computación distribuida y en red, a partir de los cuales ha crecido la idea de Cloud Computing. La computación en la nube, según la definición del NIST, se conoce como: un concepto para hacer que un conjunto compartido de recursos informáticos reconfigurables (como redes, servidores, almacenamiento, aplicaciones y servicios) esté disponible bajo demanda, de forma cómoda y generalizada. Estos recursos pueden suministrarse y desplegarse rápidamente con poco trabajo de administración o contacto con el proveedor de servicios. La informática forense de Modren, la ciencia que se relaciona con técnicas y procedimientos para identificar, recopilar, preservar, analizar y presentar datos digitales ante un tribunal de justicia, requiere una cantidad cada vez mayor de recursos computacionales a medida que aumenta el número de investigaciones relacionadas con la informática. en el ámbito de la escalabilidad, la tolerancia a fallos y el procesamiento colaborativo. Los sistemas de información de hoy en día son golpeados por individuos, organizaciones, gobiernos y sistemas que se han convertido en la atención principal de los ataques de seguridad de la información y traerían un efecto catastrófico de perder múltiples recursos que son muy valiosos. Además, los delincuentes son cada vez más conscientes de las capacidades de investigación y forense digital, y hacen un uso más sofisticado de las computadoras y las redes para cometer sus delitos. Algunos incluso están desarrollando métodos y herramientas "antiforense" diseñados específicamente para ocultar sus actividades y destruir evidencia digital y, en general, socavar las investigaciones digitales. La integración de un cifrado sólido en los sistemas operativos también está creando desafíos para los examinadores forenses, lo que podría impedir que el lado recupere cualquier evidencia digital de una computadora [05].

Con la evolución de Internet en la década de 1990, el mundo de la computación ha sido testigo de muchos cambios, desde el entorno de un procesamiento hasta el procesamiento paralelo, la computación distribuida, la computación en cuadrícula, la computación ubicua, la computación omnipresente y ahora la computación en la nube. Permite a las empresas aumentar y reducir sus recursos en función de sus necesidades. Al utilizar la computación en la nube, los usuarios pueden almacenar sus datos de forma remota y disfrutar de un acceso transparente a las aplicaciones bajo demanda sin tener que invertir en infraestructura de hardware o administración de software. Por lo tanto, protege al usuario de las dificultades de la informática tradicional, como el establecimiento de infraestructuras, la concesión de licencias de software y la contratación de personal técnico, etc. La informática forense es la ciencia de identificar, extraer, preservar y presentar la evidencia digital almacenada en dispositivos digitales que puede ser legalmente admisible en los tribunales por cualquier delito cibernético o fraudulento. En otras palabras, la búsqueda de hechos, registros y rastros digitales puede ser legalmente admisible en el tribunal para el enjuiciamiento penal. La información digital es frágil porque puede modificarse, duplicarse o destruirse fácilmente, etc. En el curso de la investigación debe asegurarse que las pruebas digitales no se modifiquen sin la debida autorización. La informática forense ha tenido un gran impacto en la detección y prevención de fraudes, así como en posibles pérdidas comerciales que pueden dañar la reputación de una organización. El proceso básico de la informática forense se basa en los siguientes pasos: identificación, conservación, recuperación, análisis y presentación. El conjunto mencionado anteriormente de acuerdos de procesos en informática forense para la detección y prevención de fraudes y delitos cibernéticos, ahora nuestra principal preocupación es la utilización eficiente de estos procesos en la ciencia forense en la nube para lograr los objetivos deseados de detección y prevención de fraudes y delitos cibernéticos [06].

Forense es un proceso de análisis de evidencia digital mientras el evento aún está en proceso, que es lo opuesto al forense muerto. El análisis forense de redes es otra área del análisis forense digital que se ocupa del análisis y la investigación de ataques a la red. El análisis forense de la memoria permite el análisis y la recuperación de los datos de la memoria volátil que contiene el estado actual de las aplicaciones, el sistema operativo (SO) y los datos de la aplicación. La evidencia digital, a medida que los datos (texto, video, audio e imágenes) se procesan y almacenan en caché, a veces en un archivo de registro, o se transmiten con el apoyo o refutan una teoría de cómo ocurrió el robo de datos [07].

La ciencia forense digital es «la aplicación de métodos científicamente derivados y probados para la conservación, recogida, validación, identificación, análisis, interpretación, documentación y presentación de pruebas digitales derivadas de fuentes digitales para facilitar o promover la reconstrucción de hechos considerados delictivos o que ayuden a anticipar acciones no autorizadas perjudiciales para las operaciones previstas», según un grupo de investigadores que definió este campo en 2001. Desde que se propuso esta definición, también se han desarrollado varios marcos de investigación y modelos de procesos que tienen un enfoque en la ciencia forense digital. Anteriormente, muchos de estos modelos se diseñaron para facilitar la investigación de sistemas informáticos tradicionales, como computadoras de escritorio y servidores. Sin embargo, las investigaciones y el análisis forense digital han trascendido el proceso clásico de

recuperación de evidencia potencial de servidor de escritorio. La aparición de incidentes de seguridad en estos componentes digitales, como bases de datos, redes informáticas, dispositivos móviles e Internet de las cosas (IoT), la nube y los bordes del diseño de la red, ha hecho necesario desarrollar modelos, procesos y técnicas forenses digitales. Adecuado para sus respectivos entornos [08].

Existe un modelo de proceso de investigación para smartphone DEFSOP con el fin de brindar la ayuda necesaria a los investigadores y proporcionar una forma de prevenir la destrucción de evidencia digital. En este modelo se tienen en cuenta cuatro fases de investigación: fase de concepción, fase de preparación, fase de operación y fase de reporte. Su fase de operación, a su vez, comprende tres procesos: recolección, análisis y forense. En su modelo, la ley y los principios se toman en consideración como la primera fase, con el objetivo de proporcionar ayuda para las otras fases y evidencia digital auténtica. A diferencia del modelo NIST, este involucra procesos de capacitación y preparación antes del proceso forense. Según los diseñadores del modelo mencionado anteriormente, cuestiones como la Adquisición y el Examen / Análisis son completamente técnicas; como resultado, es mejor colocarlas en una sola fase, que es la fase de operación en este modelo. Debido a que se tiene en cuenta la legitimidad de la evidencia digital, sostienen que su modelo propuesto es de mayor confiabilidad en comparación con el NIST [09].

El proceso de examen físico y digital se utiliza para recopilar y preservar evidencia física y digital. Consta de dos procesos: examen físico y examen digital. El proceso de examen físico se utiliza para capturar y preservar evidencia de la escena física del crimen. Consta de varias actividades: preservación, relevamiento, documentación, búsqueda, recolección, reconstrucción e informe. El proceso de examen digital, por otro lado, comienza preservando la escena del crimen digital y se basa en los informes obtenidos del proceso de examen físico, así como en el análisis muerto (fuera de línea) o en vivo (en línea). Una vez completada y documentada la encuesta, se recopilan pruebas volátiles, seguidas de pruebas no volátiles. [10].

Para abordar la brecha en la literatura, este artículo ofrece la primera revisión de la literatura sobre el almacenamiento de la evidencia digital usando Cloud Computing con RQs acerca de las palabras clave que con frecuencia presentan coocurrencia en las investigaciones y también sobre las discusiones y conclusiones que se caracterizan por su alta objetividad y su baja polaridad por año. En esta revisión sistemática, se recopiló información sobre el almacenamiento de la evidencia digital usando Cloud Computing, con el propósito de obtener reseñas sobre el tema. La investigación se ha apoyado en herramientas tecnológicas como el gestor bibliográfico Mendeley y la herramienta de inteligencia artificial (RAj) de autoría del Dr. Javier Gamboa-Cruzado, la cual se utilizó para procesar la información obtenida.

Es cierto que muchos de los modelos forenses tradicionales no abordan adecuadamente el entorno de la computación en la nube debido a las características particulares de esta tecnología. La naturaleza distribuida, remota y dinámica de los datos en la computación en la nube presenta desafíos únicos para la informática forense. Los modelos tradicionales, que están diseñados para trabajar con sistemas locales y controlados, no abordan adecuadamente estos desafíos. Esto ha dado lugar a la necesidad de desarrollar nuevos enfoques y herramientas forenses que sean capaces de adaptarse a las características del entorno de la nube, permitiendo una recopilación y análisis de evidencia efectivos sin comprometer su integridad. La informática forense y Cloud Computing se relacionan en la necesidad de manejar, analizar y preservar evidencia digital en entornos distribuidos y en la nube. A medida que la computación en la nube se vuelve más prevalente, los expertos en informática forense deben adaptar sus herramientas y procedimientos para enfrentar los desafíos únicos que presenta esta tecnología.

3. Método de revisión

El enfoque de la revisión se creó teniendo en cuenta los principios de revisión sistemática de la literatura de B. Kitchenham [11]. Según el enfoque de la revisión, se explican los objetivos de la investigación, las fuentes de datos, el proceso de búsqueda, los criterios de exclusión, la evaluación de la calidad, la extracción de datos y la síntesis de datos. La revisión sistemática pasa por diferentes etapas de manejo para poder llevarse a cabo, tal y como se muestra en la Figura 1.

3.1. Problemas y objetivos de investigación

Las preguntas de investigación son cruciales para el enfoque de búsqueda, extracción y análisis de datos en

Figura 1
Etapas para una RSL

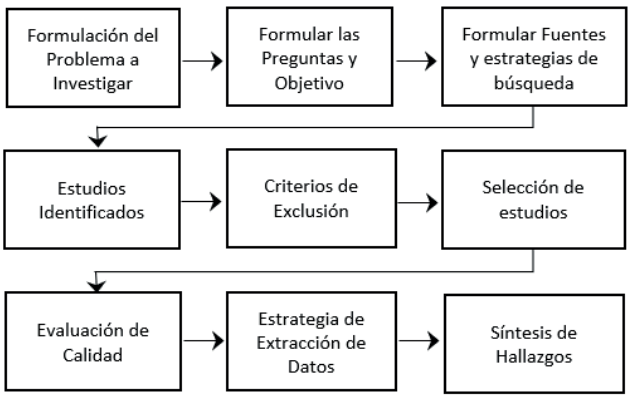


Tabla 1

Preguntas y objetivos de investigación

Pregunta de investigación	Motivación
RQ1: ¿Qué medios de publicación son los principales objetivos de la producción de investigación en el área?	Identificar los medios de publicación son los principales objetivos de la producción de investigación en el área
RQ2: ¿Cuántos estudios se publicaron a lo largo de los años sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?	Determinar cuántos estudios se publicaron a lo largo de los años sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital
RQ3: ¿Cuáles son los conceptos (tópicos) más utilizados sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?	Identificar los conceptos (tópicos) más utilizados sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital
RQ4: ¿Cuáles son los artículos más citados sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital cuyas discusiones y conclusiones se caracterizan por su alta objetividad y su baja polaridad?	Determinar los artículos más citados sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital, cuyas discusiones y conclusiones se caracterizan por su alta objetividad y su baja polaridad
RQ5: ¿Cuáles son las palabras clave que con frecuencia presentan coocurrencia en las investigaciones sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?	Determinar las palabras clave que con frecuencia presentan coocurrencia en las investigaciones sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital
RQ6: ¿Cuáles son las palabras clave más utilizadas y más relevantes por resúmenes en las investigaciones sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?	Identificar las palabras clave más utilizadas y más relevantes por resúmenes en las investigaciones sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital
RQ7: ¿Cuáles son los principales modelos de servicios de Cloud Computing?	Identificar los principales modelos de servicios de Cloud Computing.
RQ8: ¿Cuáles son los principales proveedores que brindan el servicio de Cloud Computing?	Determinar los principales proveedores que brindan el servicio de Cloud Computing

una revisión sistemática de la literatura. Los objetivos, que se muestran en la Tabla 1, se determinaron junto con las preguntas del estudio.

3.2. Fuentes, ecuación y descriptor de búsqueda

Las bibliotecas que se utilizaron para buscar los trabajos de investigación son las siguientes: ARDI, Google Scholar, IEEE Xplore, ProQuest, ScienceDirect, Scopus, Springer, Taylor & Francis, Web of Science y Wiley Online Library.

La estrategia de búsqueda incluye la búsqueda de palabras clave relevantes para el estudio. El procedimiento de búsqueda se ha llevado a cabo utilizando la ecuación de búsqueda para el estudio, según se muestra en la Tabla 2.

3.3. Estudios identificados

Al finalizar la búsqueda de artículos se obtiene la cantidad de 5754 artículos.

Tabla 2

Fuentes, ecuación y descriptor de búsqueda

Fuente	Ecuación	Descriptor
ARDI	("cloud computing") AND (storage) AND ("digital evidence" OR “computer forensics”) AND (methodology OR method OR model)	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
Google Scholar	“cloud computing” AND storage AND (“digital evidence” OR “computer forensics”) AND (methodology OR method OR model)	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
IEEE Xplore	"All Metadata": “cloud computing” AND "All Metadata": storage AND "All Metadata": “digital evidence” OR “computer forensics” AND ("All Metadata”: methodology OR method OR model)	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
ProQuest	("cloud computing") AND (storage) AND ("digital evidence" OR “computer forensics”) AND (methodology OR method OR model)	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
Science Direct	("cloud computing") AND storage AND ("digital evidence” OR “computer forensics”) AND (methodology OR method OR model)	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
Scopus	ALL (“cloud computing” AND storage AND (“digital evidence” OR “computer forensics”) AND (methodology OR method OR model))	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
Springer	"cloud computing" AND (storage) AND ("digital evidence" OR "computer forensics") AND (methodology OR method OR model)	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
Taylor & Francis	[All: "cloud computing"] AND [All: storage] AND [[All: "digital evidence"] OR [All: "computer forensics"]] AND [[All: methodology] OR [All: method] OR [All: model]]	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
Web of Science	(“cloud computing”) AND storage AND (“digital evidence” OR “computer forensics”) AND (methodology OR method OR model)	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo
Wiley Online Library	"cloud computing" anywhere and "storage" anywhere and ""digital evidence" OR "computer forensics"" anywhere and "methodology OR method OR model" anywhere	Computación en la nube
		Almacenamiento + evidencia digital / informática forense
		Metodología / método / modelo

3.4. Criterios de exclusión

Los criterios de exclusión se han definido para evaluar con precisión la calidad de la literatura. Los artículos fueron revisados por estos criterios:

- CE1: Los artículos tienen una antigüedad mayor a 5 años.
- CE2: Los artículos no están escritos en idioma inglés.
- CE3: Los artículos no se publicaron en conferencias o revistas revisadas por pares.
- CE4: No se dispone del texto completo del artículo.
- CE5: Los títulos y los keywords de los artículos no son muy adecuados.
- CE6: El abstract de los artículos no es muy relevante.

3.5. Selección de estudios

En la fase de identificación se seleccionaron 5754 documentos. Luego, durante la fase de selección, se aplicaron los criterios de exclusión CE1 y CE2, lo que llevó a la exclusión de 2228 artículos, dejando un total de 3526. En esta misma fase, se utilizaron los criterios de exclusión CE3 y CE4, excluyendo 3283 artículos y quedando con 243 documentos. En la fase de elegibilidad, se aplicaron los criterios de exclusión CE5 y CE6, lo que resultó en la exclusión de 143 documentos, quedando finalmente con 100 artículos incluidos, como se puede ver en la Tabla 3.

3.6. Evaluación de la calidad

Para determinar la lista final de trabajos incluidos en este artículo de revisión, se evaluaron las normas de evaluación de la calidad. La calidad de los artículos de investigación se evaluó mediante QAs de acuerdo con las preguntas de investigación predeterminadas. Para evaluar la calidad de los artículos, se emplearon las siguientes QAs:

Tabla 3

Aplicación de los criterios de exclusión a los resultados base

Fuente	Identificación	Selección				Elegibilidad		Inclusión
		CE1	CE2	CE3	CE4	CE5	CE6	
ARDI	86	43	43	39	39	9	9	9
Google Scholar	4300	2580	2580	185	77	54	54	54
IEEEXplore	9	0	0	0	0	0	0	0
ProQuest	5	5	5	5	5	2	2	2
ScienceDirect	219	124	124	79	21	9	9	9
Scopus	515	363	358	308	92	25	25	25
Springer	403	278	270	78	2	0	0	0
Web of Science	5	4	4	3	0	0	0	0
Wiley Online Library	192	126	126	32	5	1	1	1
Taylor & Francis	20	16	16	11	2	0	0	0
TOTAL	5754		3526		243		100	100

- QA1. ¿El documento está bien organizado?
- QA2. ¿Los objetivos de investigación se identifican claramente en el documento?
- QA3. ¿El propósito de la investigación está claramente explicado?
- QA4. ¿Explica el contexto en el que se realizó la investigación?
- QA5. ¿El artículo pertenece a un libro, publicación o conferencia?
- QA6. ¿Se dispone del texto completo?

Durante esta etapa se analizó la calidad de la investigación por los artículos que habían cumplido con los criterios de exclusión. La revisión fue realizada por el autor y el co-autor, lo cual es una buena práctica que aumenta la confiabilidad del proceso. Para analizar la rigurosidad, credibilidad y relevancia de los estudios, se evaluó independiente cada estudio según 6 criterios (QA). Para cada documento, se leyó el artículo completo, frente a dudas que se presentaron conforme se llevaba a cabo la revisión, se procedió a realizar una lectura más rigurosa, mejorando la calidad de la selección de estudios. Los artículos seleccionados en su totalidad cien (100) cumplieron con cada uno de los QAs.

3.7. Estrategias de extracción de datos

En esta parte se utilizó todos los artículos seleccionados para extraer información necesaria para responder el conjunto de preguntas de investigación. Entre los datos extraídos de cada artículo se encontraban campos como el ID del artículo, el título del artículo, la URL, la fuente, el año, el país, el número de páginas, el idioma, el tipo de publicación, el nombre de la publicación, los autores, la afiliación, el número de citas, el resumen, las palabras clave y el tamaño de la muestra. PgsRQ1, PgsRQ2, PgsRQ3, PgsRQ4, PgsRQ5, PgsRQ6, PgsRQ7 y PgsRQ8.

3.8. Síntesis de hallazgos

La información extraída para las preguntas de investigación RQ1 – RQ8 se tabuló y se presentó como datos cuantitativos que se utilizaron para desarrollar una comparación estadística entre diferentes hallazgos para cada pregunta de investigación.

Estas estadísticas desarrolladas ayudaron a descubrir ciertos patrones de investigación, así como direcciones de investigación que se llevaron a cabo durante la última década

4. Resultados y Discusión

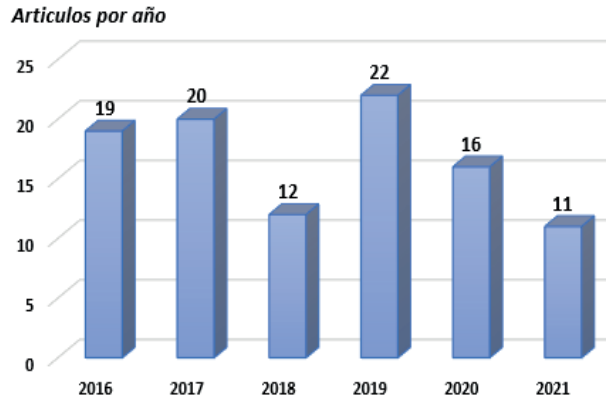
4.1. Descripción general de los estudios

Como resultado del proceso de selección se obtuvieron 100 estudios que se utilizaron para la extracción y análisis de datos. La Figura 2 muestra la distribución de los estudios publicados desde el 2016 hasta el 2021.

De acuerdo con los autores Alghofaili, Albattah, Alrajeh, Rassam y Al-rimy [12], evidencia que en el

Figura 2

Distribución de los artículos publicados por año



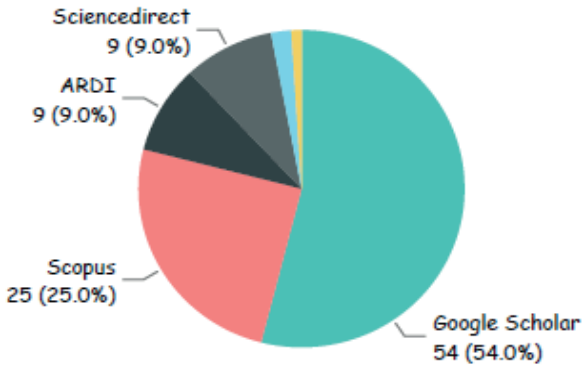
año 2019 se publicaron la mayor cantidad de artículos relacionados a la investigación.

La Figura 3 muestra la asignación de las fuentes más productivas para la obtención de los 100 artículos seleccionados para el presente estudio. Se observa que Google Scholar y Scopus aportaron 54 y 25 artículos, respectivamente.

De acuerdo con los autores Al-Dhaqm, Ikuesan, Kebande, Razak, Grispos, Choo y Alsewari [08], corrobora el uso de una de las fuentes para la búsqueda de artículos relacionados a la investigación. Así mismo, según Al-Dhaqm, Abd Razak, Ikuesan, Kebande y Siddique [09], también validan el uso de una de las fuentes para la búsqueda de artículos. Además, los autores Norouzi, Bruder, Belna, Mutter, Turgut y Welch [13], ratifican el uso de una de las fuentes para la búsqueda de artículos.

Figura 3

Distribución de los artículos publicados por fuente



La Tabla 4 presenta la distribución de los autores más productivos que analizan Cloud Computing para el almacenamiento de la evidencia digital. Se observa que existen dos grupos de autores más productivos, en el primer grupo tenemos a R. Kalaiprasath, R. Elankavi, R. Udayakumar y en el segundo grupo tenemos a Sebastian Lins, Stephan Schneider, Ali Sunyaev. Estos dos grupos de autores obtuvieron un total de 127 y 121 citas, respectivamente.

De acuerdo con los autores Yakubu, Christopher, Chiroma y Abdullahi [04], evidencia que el año 2017 se publicaron la mayor cantidad de citas relacionadas a la investigación.

La Figura 4 muestra la asignación de los países más productivos sobre Cloud Computing en los últimos 5 años. Se observa que la India y los Estados Unidos aportaron la mayor cantidad con 21 y 11 artículos, respectivamente.

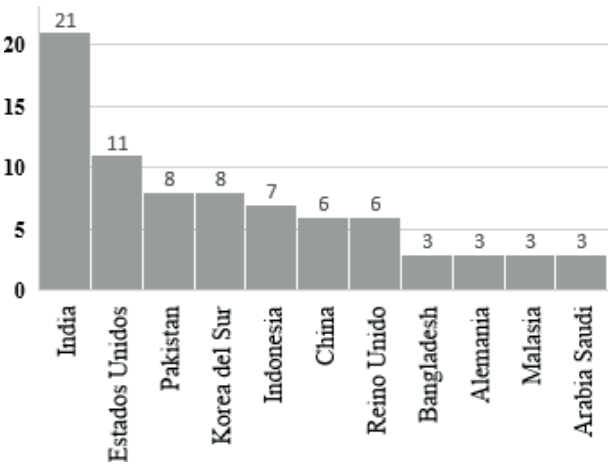
Tabla 4

Autores más productivos por número de citas

Autores	Total
R. Kalaiprasath, R. Elankavi, R...	127
Sebastian Lins, Stephan Schneider...	121
Xingshuo An, Xianwei Zhou, Xing Lü...	71
Shancang Li, Kim-Kwang Raymond...	68
Victor R. Kebande, H. S. Venter	39
Nurul Huda Nik Zulkipli, Ahmed...	34

Figura 4

Distribución de los artículos publicados por país



4.2. Respuestas a las preguntas de investigación

RQ1. ¿Qué medios de publicación son los principales de la producción de investigación en el área?

Los principales medios de producción científica en el área son revistas con un 84% del total de artículos revisados. Además, en un segundo lugar tenemos a las conferencias con un 15% del total, como se muestra en la Figura 5.

Según Sjöstrand [14], validan el uso de uno de los tipos de publicación para la selección de artículos. Además, los autores Norouzi, Bruder, Belna, Mutter, Turgut y Welch [13], ratifican el uso de una de las fuentes para la búsqueda de artículos

RQ2. ¿Cuántos estudios se publicaron a lo largo de los años sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?

La Tabla 5 muestra la estadística de las investigaciones que se realizan a lo largo de los años, donde se aprecia la cantidad de artículos encontrados en la Revisión de la Literatura desde el 2016 hasta el 2021 por fuente de búsqueda. Los resultados de la revisión encontraron que en Google Scholar en el año 2017 y 2019 se publicaron 13 artículos respectivamente.

De acuerdo con los autores Alghofaili, Albattah, Alrajeh, Rassam y Al-rimy [12], evidencia que hace mención a una de las fuentes de búsqueda. Según Coronel, Cedillo, Campos, Camacho y Bermeo [15], validan el uso de una de las fuentes para la búsqueda de artículos.

Figura 5

Distribución de los artículos por medio de publicación

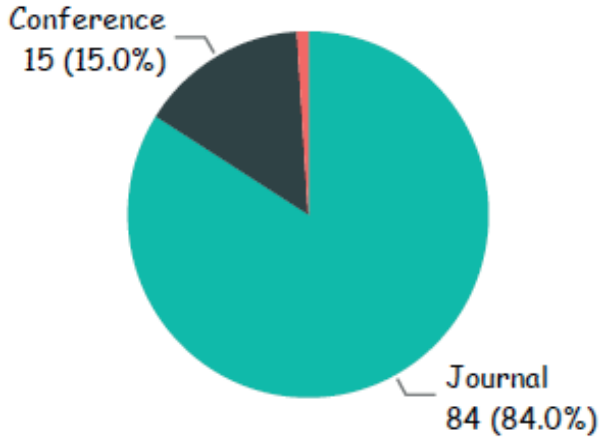


Tabla 5

Artículos por años y fuente de búsqueda

Fuente	2016	2017	2018	2019	2020	2021	Total
Google Scholar	12	13	6	13	6	4	54
Scopus	4	3	4	5	6	3	25
ARDI	1	1	2	3	2		9
Sciencedirect	2	3		1	2	1	9
ProQuest						2	2
Wiley Online Library						1	1
Total	19	20	12	22	16	11	100

RQ3. ¿Cuáles son los conceptos (tópicos) más utilizados sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?

La Tabla 6 muestra los principales bigramas, es decir, dos palabras juntas, que aparecen en los resúmenes de los estudios. Principalmente se encuentra el concepto "Cloud Computing", seguido por digital evidence y digital forensics. Según los autores Al-Dhaqm, Abd Razak, Ikuesan, Kebande y Siddique [09], ratifican el uso de uno de los conceptos.

RQ4. ¿Cuáles son los artículos más citados sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital, cuyas discusiones y conclusiones se caracterizan por su alta objetividad y su baja polaridad?

La Tabla 7 muestra, ordenado por los artículos más citados, la objetividad y polaridad de las discusiones y conclusiones. Se puede observar que el artículo más citado es subjetivo y de polaridad positiva, esto último quiere decir que fue escrito de manera formal.

En cambio, los artículos siguientes muestran ser neutros tanto en su objetividad y polaridad. Los artículos más citados pertenecen a Google Scholar y Scopus.

Tabla 6

Bigrama de los resúmenes de artículo

Bigrama	ARDI	Google Scholar	Science Direct	Scopus	Total
Cloud Computing	3	40	4	11	58
Digital evidence	3	27	2	9	41
Digital forensics	5	28	2	7	42
Digital forensic	4	23	3	7	37
Cloud forensics		19	3	7	29
Forensic investigation	2	13	1	9	25

Tabla 7

Artículos más citados caracterizados por su alta objetividad y baja polaridad

Source	N° Citas	Objetividad	Polaridad	Fuente
Cloud Security...	127	0.46	0.25	Google Scholar
Trust is Good Control...	121	0.59	0.04	Scopus
Sample Selected...	71	0.54	-0.11	ARDI
IoT Forensics: Amazon...	68	0.68	0.008	Scopus
On Digital Forensic	39	0.55	-0.17	Scopus
IoT Forensic: Bridging...	34	0.5	0.00	Google Scholar
Blockchain based digital...	32	0.42	0.11	Scopus
The impact of Cloud...	31	0.68	0.08	Scopus
SCARF: a container...	28	0.61	0.09	Science direct
Cloud forensics Framework...	26	0.89	0.06	Science direct
Scenario-Based Digital...	24	0.69	0.06	Scopus
Greening Cloud Enable...	24	0.69	-0.07	Scopus

RQ5. ¿Cuáles son las palabras clave que con frecuencia presentan coocurrencia en las investigaciones sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?

La Figura 6, es una red bibliométrica, la cual permite mostrar la coocurrencia entre las palabras clave más relevantes. Se visualiza a "Cloud Computing" y "digital forensics".

Esto principalmente se debe a una minuciosa selección de variables para la investigación. Estas palabras clave más frecuentes también tienen conexiones importantes.

RQ6. ¿Cuáles son las palabras clave más utilizadas y más relevantes por resúmenes en las investigaciones sobre Cloud Computing y su impacto en el almacenamiento de la evidencia digital?

Los autores de cada estudio seleccionado utilizaron varios términos en los resúmenes de sus artículos.

Para ayudar a los lectores a ver todos estos términos utilizados, empleamos la nube de palabras como se muestra en la Figura 7.

Cabe mencionar que el tamaño de fuente de cada término en la nube de palabras representa la frecuencia. Del mismo modo, cuanto más pequeña es la palabra, menor es la frecuencia de uso.

Según los autores Al-Dhaqm, Abd Razak, Ikuesan, Kebande y Siddique [09], corrobora el uso de una de las palabras clave.

Además, Sjöstrand [14], valida el empleo de una de las palabras clave. Otros autores como Mat Kamal, Ibrahim, y Nilashi [16] ratifican el uso de una de las palabras clave.

Figura 6

Red bibliométrica de palabras clave que presentan coocurrencia

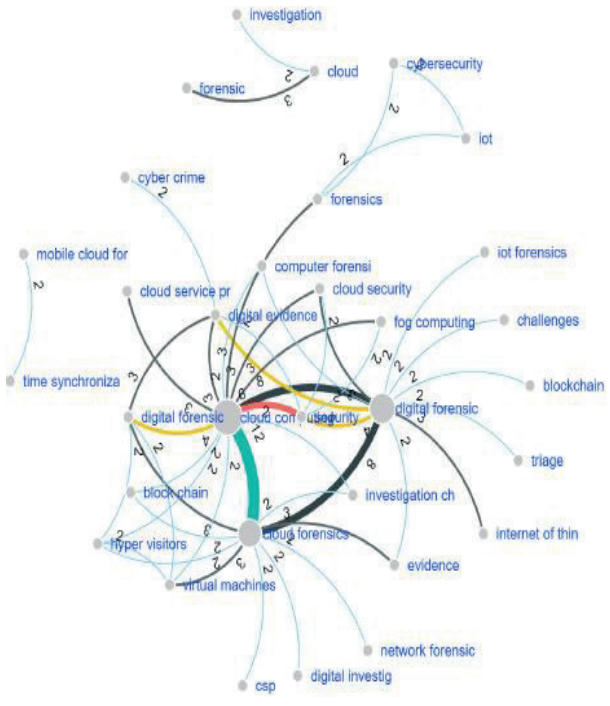
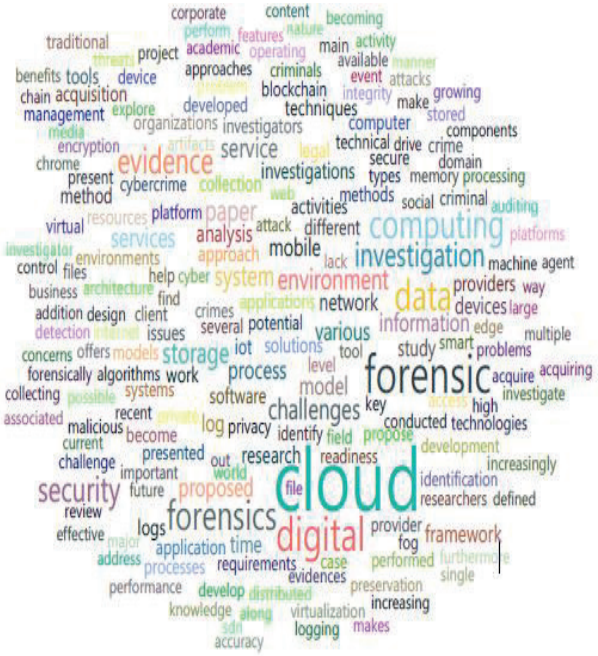


Figura 7

Términos más usados en los resúmenes de los artículos



Según los resultados de la revisión de la literatura, existen tres modelos de servicios de Cloud Computing, los cuales son SaaS (36%), PaaS (36%) y IaaS (43). La Tabla 8 muestra los modelos de Servicios de Cloud Computing.

De acuerdo con los autores Al-Dhaqm, Ikuesan, Kebande, Razak, Grispos, Choo y Alsewari [08] indican que se desarrolló un modelo común para el análisis forense de redes en Infraestructura como servicio (IaaS). El cual, se ha definido como una arquitectura para "Forensics-as-a-Service" es decir, una infraestructura de gestión de la nube.

Tabla 8

Modelo de servicios Cloud Computing

Modelos de Servicios Cloud Computing	Referencia	Cant. (%)
SaaS	[17][18][19][20][06][21][22][23] [24][25][26][27][28][29][30] [31][05][32][33][34][35][36] [37][38][39][40][41][42][43] [44][45][46][47][48][49][50]	36 (31)
PaaS	[17][18][19][20][06][21][22][23] [51][24][25][52][27][28][29] [30][31][05][32][33][34][35] [37][38][39][40][53][41][42] [43][44][45][47][48][49][50]	36 (31)
IaaS	[17][18][19][20][06][21][22][23] [51][24][25][54][27][28][29] [55][30][31][05][32][33][34] [35][56][36][37][38][39][40] [41][42][57][58][59][43][44] [60][45][46][47][48][49][50]	43 (38)

De acuerdo con los autores Alghofaili, Albattah, Alrajeh, Rassam y Al-rimy [12], también se evidencia que hace mención a uno de los modelos de servicios de Cloud Computing.

Así mismo, según Coronel, Cedillo, Campos, Camacho y Bermeo [15] también hacen mención de la utilización de los modelos de servicios de Cloud Computing.

RQ8. ¿Cuáles son los principales proveedores que brindan el servicio de Cloud Computing?

Con base a las revisiones de los artículos, existen seis proveedores que brindan el servicio de Cloud Computing como se muestra en la Tabla 9.

Los resultados de la revisión consideraron a Amazon Web Services (30%) como el principal proveedor, seguido por Microsoft Azure (20%) y Salesforce (20%).

De acuerdo con los autores Alghofaili, Albattah, Alrajeh, Rassam y Al-rimy [12], mencionan a uno de los proveedores que brindan servicio de Cloud Computing. Así mismo, los autores Gill, Tuli, Xu, Singh, Singh, Lindsay y Garraghan [01] también hacen mención a uno de los proveedores que brindan el servicio de Cloud Computing.

Se observa que en 2019 se publicó la mayor cantidad de artículos relacionados con la investigación. Además, es relevante destacar que la fuente más productiva para obtener los 100 artículos seleccionados en este estudio fue Google Scholar, una plataforma que facilita el acceso, descubrimiento y seguimiento de literatura académica de alta calidad. Dependiendo de las necesidades de búsqueda, se puede optar por Google Scholar o por otras plataformas, ya que cada una presenta fortalezas y limitaciones en distintos contextos de investigación. Según los resultados de la revisión, Amazon Web Services (AWS) es considerado el principal proveedor. AWS ha revolucionado la forma en que las organizaciones gestionan su infraestructura tecnológica, ofreciendo soluciones en la nube para almacenamiento, cómputo y bases de datos altamente escalables, flexibles y rentables, lo que la convierte en la opción más completa para la mayoría de las empresas. En cuanto a los modelos de servicios de Cloud Computing, se identifican tres principales: SaaS, PaaS e IaaS. Para este estudio, IaaS resulta ser el modelo más adecuado para las empresas que desean tener control total sobre sus recursos informáticos sin necesidad de mantener hardware físico, ya que ofrece escalabilidad, flexibilidad y reducción de costos, siendo adecuado para diversas aplicaciones, desde el desarrollo de software hasta el almacenamiento de datos y recuperación ante desastres. El modelo IaaS también presenta ventajas significativas para la informática forense, como escalabilidad, acceso remoto y almacenamiento de grandes volúmenes de datos. Sin embargo, también plantea desafíos relacionados con la accesibilidad de la evidencia, el cumplimiento normativo y la integridad de los datos. Entre las palabras clave más utilizadas en la investigación se encuentran Cloud Computing, evidencia digital e informática forense, lo que demuestra que Cloud Computing está transformando el panorama de la informática forense al introducir nuevos enfoques en el almacenamiento, procesamiento y acceso a los datos. A medida que más organizaciones adoptan soluciones en la nube, es crucial que los investigadores forenses ajusten sus métodos y herramientas para abordar los desafíos que presenta este entorno. Las investigaciones futuras deberían centrarse en desarrollar nuevas soluciones que permitan a los expertos acceder a la evidencia digital en la nube de manera eficiente, asegurando su integridad y cumpliendo con los requisitos legales y éticos.

Tabla 9

Proveedores de servicios Cloud Computing

Proveedores	Referencia	Cant. (%)
Microsoft Azure	[30] [34] [56] [50]	4 (20)
Amazon Web Services (AWS)	[61] [34] [43] [47] [49] [50]	6 (30)
Google Cloud	[34] [56]	2 (10)
Salesforce	[37] [38] [62] [50]	4 (20)
IBM	[25] [57] [58]	3 (15)
Alibaba Cloud	[63]	1 (5)

5. Conclusiones y futuras investigaciones

En resumen, en este estudio se empleó la Revisión Sistemática de la Literatura (RLS), un procedimiento iterativo que recopila toda la investigación previa sobre un determinado tema o cuestión de investigación. El propósito de la SLRC es abordar los problemas identificando, evaluando críticamente e integrando los hallazgos de todos los estudios individuales relevantes de alta calidad que aborden una o más preguntas de investigación. Este método empleado determinó cuánto han progresado los estudios actuales sobre el almacenamiento de la evidencia digital usando Cloud Computing. Además, identifica relaciones, contradicciones, lagunas e inconsistencias en la literatura, y explora razones para seguir estudiando el tema. También ayuda a formular declaraciones generales, desarrollar teorías y describir instrucciones para futuras investigaciones. Se realizó una revisión sistemática de la literatura para recopilar, analizar y sintetizar datos sobre el almacenamiento de la evidencia digital usando Cloud Computing. El límite de tiempo que se empleó para los artículos que se revisaron en diferentes bases de datos fue entre 2016 y 2021. Teniendo como base la fórmula de palabras clave, se encontraron 5.754 artículos, luego, aplicando los criterios de exclusión, se analizaron profunda y extensamente 100 artículos y respondimos las preguntas de investigación, las analizamos, discutimos las brechas, los desafíos y las direcciones futuras.

A pesar de la profundidad y amplitud del estudio, se reconocen algunas limitaciones, ya que el enfoque se centra en una revisión de literatura y análisis según las publicaciones y autores, sin la intención de ofrecer una

síntesis o perspectiva particular. Aunque la selección de documentos se realizó de manera objetiva, utilizando técnicas y análisis basados en las palabras clave definidas en este estudio, tanto en inglés como en español, durante la revisión y análisis posterior se identificaron artículos con ambigüedades en la delimitación de conceptos, principios, enfoques y términos, que en algunos casos relacionaban áreas de estudio ajenas o emergentes que no tienen una conexión directa con el tema investigado. Además, el uso predominante de Google Scholar puede ser visto como una limitación, ya que, aunque es una de las bases de datos más grandes e importantes, omite algunas revistas y publicaciones que no están indexadas. No obstante, se incluyeron estudios relevantes de otras fuentes científicas para completar el análisis integral de conceptos y contribuciones en este campo de investigación. Por lo tanto, resulta necesario ampliar este estudio utilizando otras bases de datos para contrastar los resultados obtenidos.

Cloud Computing y la evidencia digital son temas de investigación cruciales para abordar los desafíos que surgen con la adopción creciente de la computación en la nube y las complejidades inherentes al almacenamiento y análisis de datos en estos entornos. A continuación, se destacan algunas recomendaciones para futuras investigaciones:

- Investigar el uso de herramientas especializadas que puedan adaptarse a los nuevos modelos de servicio de la nube (IaaS, PaaS, SaaS), facilitando la recuperación de datos en entornos virtualizados y distribuidos. Estas herramientas deberían abordar los retos del cifrado, la preservación de la integridad de los datos y la extracción de evidencia digital de sistemas que no son físicamente accesibles.
- Establecer normativas universales que regulen el almacenamiento y acceso a la evidencia digital en la nube. Esto incluye la creación de estándares internacionales para la preservación de evidencia y la jurisdicción en los casos que involucran múltiples ubicaciones geográficas.
- Con la creciente adopción de múltiples proveedores de servicios en la nube, es importante investigar cómo garantizar que las herramientas forenses sean interoperables entre plataformas como Amazon Web Services (AWS), Microsoft Azure, Google Cloud, y otros servicios de nube, facilitando el análisis de datos distribuidos.

Referencias

[1] S. S. Gill et al., “Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges,” Internet of Things (Netherlands), vol. 8, no. December, 2019, doi: 10.1016/j.iot.2019.100118.

[2] A. Shukla, B. Katt, L. O. Nweke, P. K. Yeng, and G. K. Weldehawaryat, “System Security Assurance: A Systematic Literature Review,” vol. 1, no. 1, pp. 1–35, 2021, [Online]. Available: http://arxiv.org/abs/2110.01904.

[3] J. Machin, E. Batista, A. Martínez-Ballesté, and A. Solanas, “Privacy and security in cognitive cities: A systematic review,” Appl. Sci., vol. 11, no. 10, 2021, doi: 10.3390/app11104471.

[4] J. Yakubu, S. M. Abdulhamid, H. A. Christopher, H. Chiroma, and M. Abdullahi, “Security challenges in fog-computing environment: a systematic appraisal of current developments,” J. Reliab. Intell. Environ., vol. 5, no. 4, pp. 209–233, 2019, doi: 10.1007/s40860-019-00081-2.

[5] M. S. Chang, “Cloud Storage Forensics : Amazon Cloud Drive on Ubuntu,” IJISET -International J. Innov. Sci. Eng. Technol. Impact Factor, vol. 3, no. 7, pp. 161–165, 2016. Available: http://ijiset.com/vol3/v3s7/IJISET_V3_I7_14.pdf

[6] A. R. MATHEW and J. A. AL ZAHLI, “Cloud Technology and the Challenges for Forensics Investigators,” DEStech Trans. Comput. Sci. Eng., no. cnsce, pp. 267–273, 2017, doi: 10.12783/dtcse/cnsce2017/8914.

[7] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, “Impact and key challenges of insider threats on organizations and critical businesses,” Electron., vol. 9, no. 9, pp. 1–29, 2020, doi: 10.3390/electronics9091460.

[8] A. Al-Dhaqm et al., “Digital Forensics Subdomains: The State of the Art and Future Directions,” IEEE Access, vol. 9, pp. 152476–152502, 2021, doi: 10.1109/ACCESS.2021.3124262.

[9] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, “A review of mobile forensic investigation process models,” IEEE Access, vol. 8, pp. 173359–173375, 2020, doi: 10.1109/ACCESS.2020.3014615.

[10] A. Al-Dhaqm et al., “Database forensic investigation process models: A review,” IEEE Access, vol. 8, pp. 48477–48490, 2020, doi: 10.1109/ACCESS.2020.2976885.

[11] Crisol Moya, E., Herrera Nieves, L. B., & Montes Soldado, R. (2020). Educación virtual para todos: una revisión sistemática. Education in the knowledge society: EKS, doi.org/10.14201/eks.23448

[12] Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy, “Secure cloud infrastructure: A survey on issues, current solutions, and open challenges,” Appl. Sci., vol. 11, no. 19, 2021, doi: 10.3390/app11199005.

[13] N. Norouzi, G. Bruder, B. Belna, S. Mutter, D. Turgut, and G. Welch, “A Systematic Review of the Convergence of Augmented Reality, Intelligent Virtual Agents, and the Internet of Things,” pp. 1–24, 2019, doi: 10.1007/978-3-030-04110-6_1.

[14] B. D. Project, I. T. It, H. P. Spring, M. Sj, and M. Nohlberg, “Combatting the data volume issue in digital forensics: A structured literature review,” vol. i, 2020, [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1453501&dswid=-8382

[15] B. Coronel, P. Cedillo, K. Campos, J. Camacho, and A. Bermeo, “A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective,” 2018 IEEE 3rd Ecuador Tech. Chapters Meet. ETCM 2018, no. January, 2018, doi: 10.1109/ETCM.2018.8580266.

[16] S. N. I. Mat Kamal, O. Ibrahim and M. Nilashi, “Critical factors influencing decision to adopt digital forensic by Malaysian law enforcement agencies: a review of PRISMA,” Insight Journal: International, Refereed, Open Access, Online Journal, vol. 4, no. 8, pp. 78-93, [Online]. Available: https://ir.uitm.edu.my/id/eprint/41878/

[17] A. Ali, S. A. Razak, S. H. Othman, A. Mohammed, and F. Saeed, A metamodel for mobile forensics investigation domain, vol. 12, no. 4. 2017, doi: 10.1371/journal.pone.0176223.

[18] A. Amirullah, I. Riadi, and A. Luthfi, "Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System," Int. J. Comput. Appl., vol. 143, no. 1, pp. 1–7, 2016, doi: 10.5120/ijca2016907696.

[19] A. I. Ahmed, "Software Agent and Cloud Forensics : A Conceptual Framework," vol. 1, pp. 166–172, 2016, [Online]. https://www.iaras.org/iaras/filedownloads/ijc/2016/006-0024.pdf.

[20] A. Khan, A. Yaqoob, K. Sarwar, M. Tahir, and M. Ahmed, "Secure Logging as a Service Using Reversible Watermarking," Procedia Comput. Sci., vol. 110, pp. 336–343, 2017, doi: 10.1016/j.procs.2017.06.103.

[21] A. Rukayat, O. Charles, and A. Florence, "A Survey and Critique of Digital Forensic Investigative Models," Academia. Edu, vol. 14, no. 12, pp. 496–508, 2016, [Online]. https://www.academia.edu/download/51650295/60_Paper_301116137_IJCSIS_Camera_Ready_496-508.pdf.

[22] D. Barrett, "Applying a Contingency Framework to Digital Forensic Processes in Cloud Based Acquisitions," J. Digit. Forensics, Secur. Law, vol. 12, no. c, 2017, doi: 10.15394/jdfsl.2017.1473.

[23] D. Sudyana and N. Lizarti, "Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method," Sci. J. Informatics, vol. 6, no. 1, pp. 125–137, 2019, doi: 10.15294/sji.v6i1.18424.

[24] E. M. Lopez, S. Y. Moon, and J. H. Park, "Scenario-based digital forensics challenges in cloud computing," Symmetry (Basel)., vol. 8, no. 10, 2016, doi: 10.3390/sym8100107.

[25] F. Freiling, T. Glanzmann, and H. P. Reiser, "Characterizing loss of digital evidence due to abstraction layers," DFRWS 2017 EU - Proc. 4th Annu. DFRWS Eur., vol. 20, pp. S107–S115, 2017, doi: 10.1016/j.diin.2017.01.012.

[26] G. M. Jones and S. G. Winster, "Forensics Analysis On Smart Phones Using Mobile Forensics Tools," Int. J. Comput. Intell. Res., vol. 13, no. 8, pp. 1859–1869, 2017, [Online]. http://www.ripublication.com/ijcir17/ijcirv13n8_03.pdf.

[27] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," Digit. Investig., vol. 9, no. 2, pp. 81–95, 2012, doi: 10.1016/j.diin.2012.05.015.

[28] J. Shurson, "Data protection and law enforcement access to digital evidence: Resolving the reciprocal conflicts between EU and US law," Int. J. Law Inf. Technol., vol. 28, no. 2, pp. 167–184, 2020, doi: 10.1093/ijlit/eaaa011.

[29] M. A. Alotaibi, M. A. Alzain, B. Soh, M. Masud, and J. F. Al-Amri, "Computer Forensics: Dark Net Forensic Framework and Tools Used for Digital Evidence Detection," Int. J. Commun. Networks Inf. Secur., vol. 11, no. 3, pp. 424–432, 2019, [Online]. Available: https://www.ijcnis.org/index.php/ijcnis/article/download/4407/370.

[30] M. Hirano, N. Tsuzuki, S. Ikeda, and R. Kobayashi, "LogDrive: a proactive data collection and analysis framework for time-traveling forensic investigation in IaaS cloud environments," J. Cloud Comput., vol. 7, no. 1, pp. 1–25, 2018, doi: 10.1186/s13677-018-0119-2.

[31] M. N. A. Khan, S. W. Ullah, A. R. Khan, and K. Khan, "Analysis of Digital Investigation Techniques in Cloud Computing Paradigm," Int. J. Next-Generation Comput., vol. 9, no. 3, pp. 251–259, 2018, doi: 10.13140/RG.2.2.26989.03045.

[32] M. S. Das, A. Govardhan, and V. L. Doddapaneni, "A model of cloud forensic application with assurance of cloud log," Int. J. Digit. Crime Forensics, vol. 13, no. 5, pp. 114–129, 2021, doi: 10.4018/IJDCF.20210901.oa7.

[33] M. Y. Arafat, B. Mondal, and S. Rani, "Technical Challenges of Cloud Forensics and Suggested Solutions," Int. J. Sci. Eng. Res., vol. 8, no. 8, pp. 1142–1149, 2017, doi: 10.14299/ijser.2017.08.004.

[34] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT forensic: Bridging the challenges in digital forensic and the internet of things," IoTBDS 2017 - Proc. 2nd Int. Conf. Internet Things, Big Data Secur., no. IoTBDS, pp. 315–324, 2017, doi: 10.5220/0006308703150324.

[35] N. Zahadat, "Digital Forensics, A Need for Credentials and Standards," J. Digit. Forensics, Secur. Law, vol. 14, no. 1, 2019, doi: 10.15394/jdfsl.2019.1560.

[36] P. Chauhan and P. Bansal, "Emphasizing on Various Security Issues in Cloud Forensic Framework," Indian J. Sci. Technol., vol. 10, no. 18, pp. 1–7, 2017, doi: 10.17485/ijst/2017/v10i18/112116.

[37] P. Dubey, V. Tiwari, and S. Chawla, "Implementing an authentication mechanism for machine deletion on the cloud," ACM Int. Conf. Proceeding Ser., vol. 12-13-Augu, no. 3, pp. 395–400, 2016, doi: 10.1145/2979779.2979878.

[38] P. Garad and B. B. Meshram, "SAAS Attacks Defense Mechanisms and Digital Forensic," pp. 2372-2377, 2019. https://www.irjet.net/archives/V6/i7/IRJET-V6I7343.pdf

[39] P. Savaridassan and G. Maragatham, "Forensics in private cloud leveraging the techniques in machine learning," Int. J. Adv. Trends Comput. Sci. Eng., vol. 9, no. 4, pp. 4627–4632, 2020, doi: 10.30534/ijatcse/2020/63942020.

[40] P. Sharma, D. Arora, and T. Sakthivel, "Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications," Procedia Comput. Sci., vol. 167, no. 2019, pp. 907–917, 2020, doi: 10.1016/j.procs.2020.03.390.

[41] Q. Waseem, S. S. Alshamrani, K. Nisar, W. Isni, and S. Wan, "Future Technology : Software-Defined Network(SDN) Forensic," 2021, doi: https://doi.org/10.3390/sym13050767.

[42] R. YANG, J. REN, S. BAI, and T. TANG, "A Digital Forensic Framework for Cloud Based on VMI," DEStech Trans. Comput. Sci. Eng., no. cst, pp. 868–878, 2017, doi: 10.12783/dtcse/cst2017/12595.

[43] S. Makura, H. S. Venter, V. R. Kebande, N. M. Karie, R. A. Ikuesan, and S. Alawadi, "Digital forensic readiness in operational cloud leveraging ISO / IEC 27043 guidelines on security monitoring," Secur. Priv., vol. 4, no. 3, pp. 1–19, 2021, doi: 10.1002/spy2.149.

[44] S. N. Kane, A. Mishra, and A. K. Dutta, "Preface: International Conference on Recent Trends in Physics (ICRTP 2016)," J. Phys. Conf. Ser., vol. 755, no. 1, 2016, doi: 10.1088/1742-6596/755/1/011001.

[45] S. Tosza, "Internet service providers as law enforcers and adjudicators. A public role of private actors," Comput. Law Secur. Rev., vol. 43, p. 105614, 2021, doi: 10.1016/j.clsr.2021.105614.

[46] T. Balon, K. Herlopian, I. Baggili, and C. Grajeda-Mendez, "Forensic Artifact Finder (ForensicAF): An Approach & Tool

for Leveraging Crowd-Sourced Curated Forensic Artifacts," ACM Int. Conf. Proceeding Ser., vol. 2021, no. Ares, pp. 1–10, 2021, doi: 10.1145/3465481.3470051.

[47] V. R. Kebande and H. S. Venter, "On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges," Aust. J. Forensic Sci., vol. 50, no. 2, pp. 209–238, 2018, doi: 10.1080/00450618.2016.1194473.

[48] V. Roussev, A. Barreto, and I. Ahmed, "API-based forensic acquisition of cloud drives," IFIP Adv. Inf. Commun. Technol., vol. 484, pp. 213–235, 2016, doi: 10.1007/978-3-319-46279-0_11.

[49] Y. Y. Teing, A. Dehghantanha, K. K. R. Choo, Z. Muda, and M. T. Abdullah, "Greening Cloud-Enabled Big Data Storage Forensics: Syncany as a Case Study," IEEE Trans. Sustain. Comput., vol. 4, no. 2, pp. 204–216, 2019, doi: 10.1109/TSUSC.2017.2687103.

[50] Z. Fu, P. Dong, S. Li, and Y. Ju, "An intelligent cross-border transaction system based on consortium blockchain: A case study in shenzhen, China," PLoS One, vol. 16, no. 6 June, pp. 1–23, 2021, doi: 10.1371/journal.pone.0252489.

[51] E. Jang, "System Access Control Technique for Secure Cloud Computing," J. Korea Soc. Comput. Inf., vol. 24, no. 8, pp. 67–76, 2019, doi: 10.9708/JKSCI.2019.24.08.067.

[52] G. Grubor, M. Heleta, N. Ristić, and I. Barać, "Integrirani model upravljanja korporativnom digitalnom forenzičkom istragom," Teh. Vjesn., vol. 23, no. 6, pp. 1591–1600, 2016, doi: 10.17559/TV-20141121105105.

[53] P. Sharma, D. Arora, and T. Sakthivel, "Mobile cloud forensic readiness process model for cloud-based mobile applications," Int. J. Digit. Crime Forensics, vol. 12, no. 3, pp. 58–76, 2020, doi: 10.4018/IJDCF.2020070105.

[54] G. M. Jones, S. G. Winster, M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 8, pp. 1859–1869, 2019, doi: 10.14569/ijacsa.2019.0100880.

[55] M. Electric, "Audit Logs Management and Security - A Survey Ahmad," vol. 48, no. 3, pp. 1–18, 2021, doi: https://doi.org/10.48129/kjs.v48i3.10624.

[56] O. Chaudhary, "Sustaining Security in Cloud Network Through Cyber Forensics Methodology," vol. 15, no. 5, pp. 363–369, 2017, [Online]. Available: https://www.academia.edu/33413155/Sustaining_Security_in_Cloud_Network_Through_Cyber_Forensics_Methodology

[57] S. Ahmed Ali, S. Memon, and F. Sahito, "Challenges and solutions in cloud forensics," ACM Int. Conf. Proceeding Ser., pp. 6–10, 2018, doi: 10.1145/3264560.3264565.

[58] S. Haque and T. Atkison, "A Forensic Enabled Data Provenance Model for Public Cloud," J. Digit. Forensics, Secur. Law, vol. 13, no. 3, 2018, doi: 10.15394/jdfsl.2018.1570.

[59] S. K. A. Manoj and D. L. Bhaskari, "Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment," Procedia Comput. Sci., vol. 85, no. Cms, pp. 149–154, 2016, doi: 10.1016/j.procs.2016.05.202.

[60] S. Park, Y. Kim, G. Park, O. Na, and H. Chang, "Research on digital forensic readiness design in a cloud computing-based smart work environment," Sustain., vol. 10, no. 4, pp. 1–24, 2018, doi: 10.3390/su10041203.

[61] D. R. Rani and P. L. Sravani, "Challenges of digital forensics in cloud computing environment," Indian J. Sci. Technol., vol. 9, no. 17, 2016, doi: 10.17485/ijst/2016/v9i17/93051.

[62] V. Miranda-López, A. Tchernykh, M. Babenko, A. Avetisyan, V. Toporkov, and A. Y. Drozdov, "2Lbp-RRNS: Two-levels RRNS with backpropagation for increased reliability and privacy-preserving of secure multi-clouds data storage," IEEE Access, vol. 8, pp. 199424–199439, 2020, doi: 10.1109/ACCESS.2020.3032655.

[63] W. Jo et al., "Digital Forensic Practices and Methodologies for AI Speaker Ecosystems," Digit. Investig., vol. 29, pp. S80–S93, 2019, doi: 10.1016/j.diin.2019.04.013