INVESTIGACIÓN & DESARROLLO, Vol. **23**, No. **1**: 107 – 116 (2023)
ISSN 2518-4431

MÉTODOS EMERGENTES DE AUDITORÍA EN INTEGRIDAD DE DATOS EN LA NUBE: UNA REVISIÓN SISTEMÁTICA DE LAS ÚLTIMAS TENDENCIAS

EMERGING METHODS OF DATA INTEGRITY AUDITING IN THE CLOUD: A SYSTEMATIC REVIEW OF RECENT TRENDS

Jairo Aldair Ríos Reyes, Renzo Yanpier Vásquez Chiclayo, Alberto Carlos Mendoza de los Santos
Facultad de Ingeniería
Universidad Nacional de Trujillo, Perú
jariosr@unitru.edu.pe
(Recibido el 14 de mayo 2023, aceptado para publicación el 21 de julio 2023)

RESUMEN

Los métodos de auditoría de integridad de datos en la nube son esenciales para garantizar la protección y confidencialidad de los datos almacenados. En este sentido, se han desarrollado diversas técnicas de auditoría que se centran en la detección y prevención de manipulaciones de datos maliciosas o no autorizadas. La revisión sistemática examinó diferentes enfoques de auditoría de integridad de datos, incluyendo la auditoría basada en políticas, la auditoría dinámica, la auditoría multi-copia y la auditoría basada en identidades, entre otras. Se identificó que algunos de los métodos más exitosos y prometedores son aquellos que utilizan técnicas criptográficas avanzadas, como la encriptación de atributos basada en políticas y la encriptación de identidades. Además, se encontró que la mayoría de los métodos propuestos utilizan estructuras de árbol de Merkle y tablas hash para mejorar la eficiencia y la escalabilidad de los procesos de auditoría. En general, esta revisión sistemática proporciona una visión general de los métodos emergentes de auditoría de integridad de datos en la nube, lo que puede ser útil para investigadores y profesionales de la seguridad de la información que buscan implementar soluciones eficientes y efectivas para la protección de datos.

Palabras Clave: Auditoría de Integridad de Datos, Computación en la Nube, Técnicas Criptográficas, Técnicas de Auditoría.

ABSTRACT

Data integrity auditing methods in the cloud are essential to ensure the protection and confidentiality of stored data. In this regard, various auditing techniques have been developed that focus on detecting and preventing malicious or unauthorized data manipulations. The systematic review examined different approaches to data integrity auditing, including policy-based auditing, dynamic auditing, multi-copy auditing, and identity-based auditing, among others. It was identified that some of the most successful and promising methods are those that use advanced cryptographic techniques, such as policy-based attribute encryption and identity encryption. Additionally, it was found that most of the proposed methods use Merkle tree structures and hash tables to improve the efficiency and scalability of auditing processes. Overall, this systematic review provides an overview of emerging data integrity auditing methods in the cloud, which may be useful for information security researchers and professionals seeking to implement efficient and effective solutions for data protection.

Keywords: Data Integrity Auditing, Cloud Computing, Cryptographic Techniques, Auditing Techniques.

1. INTRODUCCIÓN

En los últimos años, la adopción de la nube se ha convertido en una tendencia creciente para el almacenamiento y procesamiento de grandes cantidades de datos. Sin embargo, esta adopción también ha traído preocupaciones sobre la seguridad y la integridad de los datos almacenados en la nube. El almacenamiento en la nube es un modelo de almacenamiento de datos en el que los datos digitales se almacenan en grupos lógicos que se extienden a través de múltiples servidores y ubicaciones. Por lo general, este entorno físico es administrado por una empresa de alojamiento. Este modelo de almacenamiento se ha vuelto cada vez más popular debido a los beneficios en términos de accesibilidad, costo y flexibilidad que ofrece a los usuarios. Sin embargo, también ha surgido la preocupación por la seguridad y la privacidad de los datos almacenados en la nube [1].

Los datos almacenados en la nube pueden estar sujetos a amenazas como ataques malintencionados, fallas de hardware o software, errores humanos y desastres naturales, lo que puede llevar a la pérdida de datos y la violación de la privacidad de los usuarios.

DOI: 10.23881/idupbo.023.1-8i

En la verificación de integridad de datos, se garantiza que los datos almacenados en la nube no han sido modificados maliciosamente o dañados. El proceso de verificación de integridad de datos puede llevarse a cabo por medio de una auditoría, que se realiza a través de un tercero de confianza [2].

La auditoría de integridad de datos en la nube es un tema muy importante que ha sido ampliamente investigado. Su objetivo principal es garantizar que los datos almacenados en la nube no hayan sido alterados o eliminados maliciosamente. Este enfoque es clave para asegurar que los datos almacenados en la nube sean precisos y confiables [3]. Por consiguiente, para verificar el correcto almacenamiento de los datos en la nube se proponen esquemas de auditoría de integridad de datos remotos. En estos esquemas el dueño de los datos como actividad principal debe crear firmas que se les va a asignar a los bloques de datos antes de que estos sean cargados a la nube. La finalidad de estas firmas es que en la fase de auditoría de integridad estos bloques de datos se encuentren almacenados en la nube. Posterior a ellos el dueño sube los bloques con sus respectivas firmas a la nube [4].

En la actualidad, existen diversos métodos de auditoría en integridad de datos en la nube, que se están desarrollando y mejorando constantemente para satisfacer las necesidades de los usuarios de la nube.

En esta revisión sistemática y comparativa, se examinan los métodos emergentes de auditoría en integridad de datos en la nube, se compara su eficacia y se evalúan sus ventajas y desventajas. Se han seleccionado y analizado un conjunto de artículos relevantes que abordan diferentes aspectos de la auditoría en integridad de datos en la nube, incluyendo técnicas criptográficas, diseño de políticas de auditoría, eficiencia computacional y privacidad de los datos [2, 4, 5, 6, 7].

Cada uno de los artículos que fueron analizados para la revisión sistemática, proporciona una perspectiva única sobre la auditoría en integridad de datos en la nube y propone soluciones innovadoras y eficaces para garantizar la integridad y la seguridad de los datos almacenados. Algunos de los métodos propuestos incluyen el uso de técnicas de criptografía como el cifrado basado en atributos de políticas de texto claro (CP-ABE) y el cifrado basado en identidad (IBE) [2, 7, 8], la implementación de árboles de hash Merkle jerárquicos para garantizar la integridad de los datos en la nube [9, 10], y el uso de técnicas de compartición de secretos para garantizar la privacidad y la seguridad de los datos de los usuarios [4].

En general, esta revisión sistemática presenta una amplia gama de métodos emergentes de auditoría en integridad de datos en la nube. Se espera que esta revisión sistemática ayude a los usuarios, auditores y proveedores de la nube a comprender mejor las opciones disponibles para la auditoría en integridad de datos y a seleccionar el método más adecuado para sus necesidades específicas.

2. METODOLOGÍA

2.1. Tipo de Estudio

La metodología que se seleccionó como base para la presente revisión sistemática fue la de PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) [11]. Para lo cual se estableció, consecuentemente al proceso de la metodología, la siguiente interrogante: ¿Cuáles son los métodos emergentes de auditoría en integridad de datos en la nube?

2.2. Fundamentación de la metodología

Llevar a cabo una revisión sistemática implica realizar un análisis exhaustivo y detallado de toda la investigación disponible, lo cual es esencial para abordar una pregunta de investigación específica o de interés en un área determinada [12]. Este proceso implica llevar a cabo investigaciones tanto cuantitativas como cualitativas con el propósito de resumir la información relevante sobre el tema en cuestión.

Dadas las definiciones mencionadas, se recomienda sintetizar la información más importante debido a la gran cantidad de estudios científicos que se generan de manera continua. El objetivo es obtener resultados prácticos que permitan identificar y evaluar diversos estudios en el mismo campo y con objetivos similares, considerando problemas en cuanto a la duplicidad y clasificación de los trabajos. Actualmente, adquirir conocimientos se vuelve complicado debido a la sobrecarga de información publicada.

La estrategia para realizar la búsqueda desempeña un papel importante para desarrollar las preguntas específicas y obtener una síntesis correcta de la investigación básica. Esta estrategia debe ser minuciosa, detallada y diseñada de manera que recupere las investigaciones relevantes para la interrogante de investigación definida. Esto garantiza una

separación adecuada de toda la información para analizar el problema planteado, así como resultados más precisos y acorde a los objetivos de la investigación.

Las estrategias empleadas en la revisión sistemática constituyen una valiosa herramienta para minimizar los sesgos y los errores al azar. Esto se logra mediante una exhaustiva búsqueda de los artículos más pertinentes, la aplicación de criterios explícitos y repetibles en la selección de estudios, y la meticulosa síntesis e interpretación de los resultados obtenidos. La revisión sistemática se realiza de manera objetiva y rigurosa, con el propósito de generar evidencia confiable y concisa, empleando métodos y técnicas metodológicas para recopilar datos a partir de estudios primarios [12]. De esta manera, se logra rescatar el efecto individual de cada estudio obtenido. En resumen, la revisión sistemática es una técnica útil y rigurosa para garantizar la calidad y fiabilidad de la evidencia científica en un campo determinado.

2.3. Proceso de recolección de Información

En el proceso de recolección de información, se establecieron criterios de búsqueda mediante grupos de términos o palabras clave las cuales están relacionadas con nuestra interrogante de investigación, las cuales se presentan a continuación: “auditing”, “cloud” e “data integrity”. Dado nuestro objetivo de obtener resultados precisos y en menor cantidad, se realizaron combinaciones de estos términos para optimizar la búsqueda, añadiendo también operadores booleanos para su correcto análisis: [(“auditing”) AND (“cloud”) AND (“data integrity”)]. También, se consideró artículos base dentro de los artículos obtenidos y/o filtrados para abarcar una mejora en el tema, y así poder responder claramente a la interrogante de la investigación, dado que algunos de los artículos importantes escapan de los resultados hechos solo en búsquedas mediante palabras clave. Además, las bases de datos que fueron seleccionadas son SCOPUS e IEEExplore, en donde se realizaron las búsquedas correspondientes.

Las consultas de búsqueda específicas se detallarán a continuación:

Scopus: (TITLE (auditing) OR TITLE (audit) AND TITLE-ABS-KEY (cloud) AND TITLE-ABS-KEY (data AND integrity)) AND (LIMIT-TO (PUBYEAR , 2023) OR LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018)) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "re"))

IEEExplore: ("All Metadata":auditing) AND ("All Metadata":cloud) AND ("All Metadata":data integrity)

Se aplicaron las restricciones de “Journals” y en cuanto a los años de publicación, estos deben ser del 2018 hasta 2023.

Google Scholar: “auditing”, “cloud”, “data integrity”

Se aplicó el año de publicación a partir del 2019 y que estos documentos sean artículos de revisión.

TABLA 1 - RESULTADOS POR BASES DE DATOS

Términos de Búsqueda / Bases de datos	Scopus	IEEExplore	Google Scholar
“auditing”, “cloud”, “data integrity”	103	76	15
Total	103	76	15

2.4. Criterios de Inclusión y Exclusión

En el desarrollo de la investigación, se recopilaron artículos de carácter original que fueron publicados en bases de datos científicos tanto inglés como español, dentro de un rango de 5 años desde el año 2018 hasta 2023. Estos artículos desarrollan nuevas metodologías en auditoria en integridad de datos en la nube.

En cuanto al criterio de exclusión, se definió que deben desecharse aquellos artículos que cumplan con las descripciones detalladas en la Tabla 2.

Ambos revisores realizaron individualmente la organización de la búsqueda y la obtención de información. Para lo cual, cada uno de los revisores realizó su análisis, síntesis y conclusión respectivamente. Para concluir, se realizó un acuerdo en base a los resultados de ambos revisores.

TABLA 2 - DESCRIPCIÓN DE LOS CRITERIOS DE EXCLUSIÓN

Identificador	Criterio de Exclusión
CE1	Aquellos artículos no originales o sin algún aporte sobre nuevas investigaciones.
CE2	Aquellos artículos sin tema principal en la auditoría de integridad de datos en la nube.
CE3	Aquellos artículos que fueron publicados antes del año 2018, debido a que se hace una búsqueda de los métodos emergentes en el tema.
CE4	Aquellos artículos sin disponibilidad del texto completo o sin acceso a los repositorios oficiales y fiables.

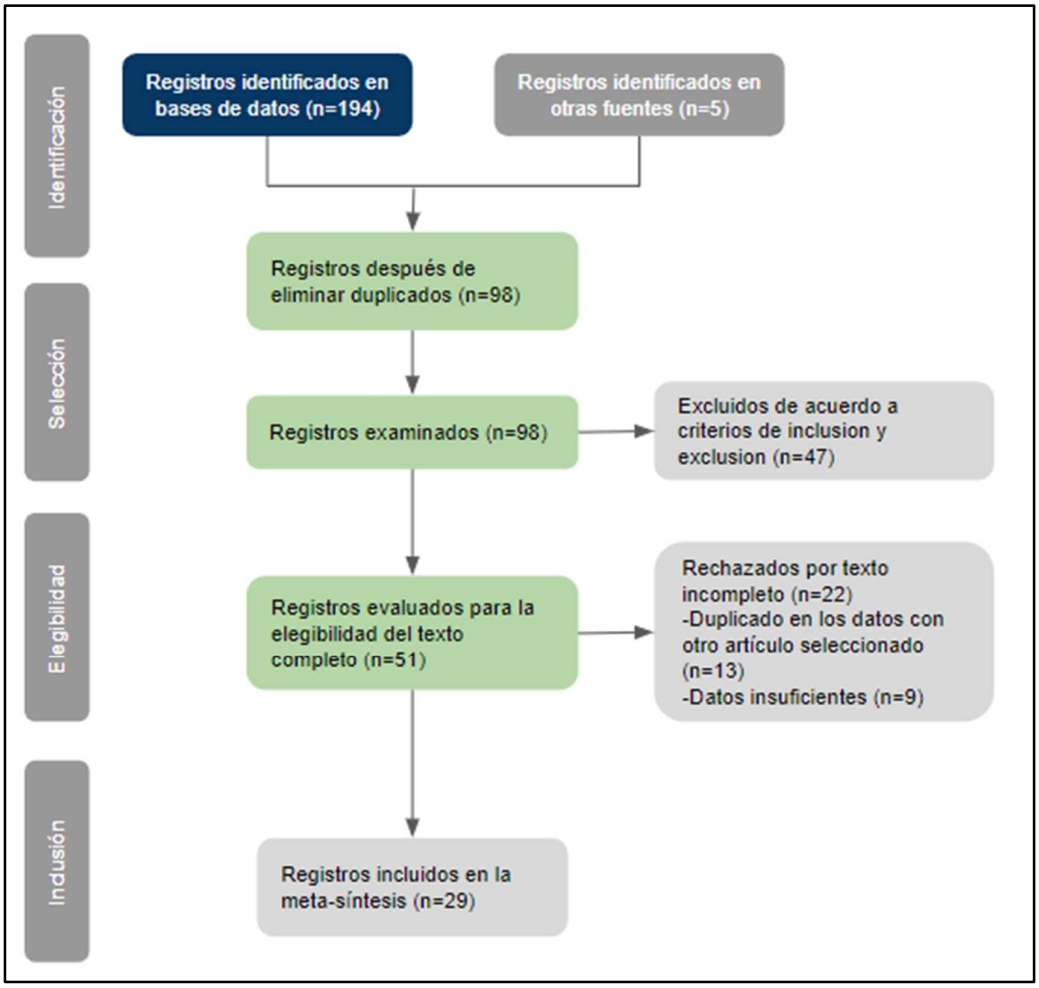

Figura 1: Flujograma de la metodología PRISMA.

Fuente: Elaborada por los autores.

3. RESULTADOS

Luego de aplicar los criterios de inclusión y exclusión, quedaron aproximadamente 29 artículos publicados al realizar una búsqueda en diferentes bases de datos. Estos artículos se distribuyen de la siguiente manera: 15 en IEEExplore, 10 en Scopus y 2, tanto en Google Scholar así como en otras. Además, se observó que el país en donde se realizan más investigaciones y/o artículos de investigaciones es China, como se puede observar en la Figura 2.

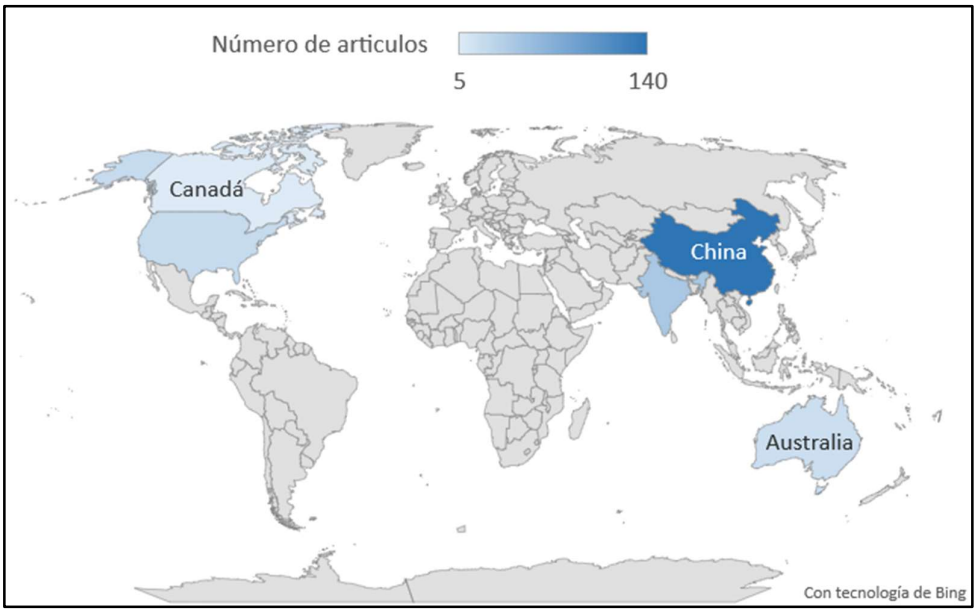

Figura 2: Proporción de artículos encontrados por país.

Fuente: Elaborada por los autores.

Además, en base a todos los artículos filtrados, se organizó y destacó los métodos emergentes que se aplicaron en auditoría en integridad de datos en la nube, destacando y clasificándolos mediante su año de publicación y método desarrollado, como se puede mostrar en la Tabla 3.

Tabla 3 - Métodos emergentes encontrados por artículos

Método emergente	Año de publicación	Artículo	Principales resultados
Auditoría basada en identidad	2023	[2]	Se presenta un esquema de auditoría pública para garantizar la integridad de datos en la nube. Se utilizan técnicas de encriptación y ocultación de información para proteger la privacidad de los usuarios y garantizar la confidencialidad de los datos.
	2019	[4]	Propone un método para habilitar la auditoría de integridad basada en identidad y el intercambio de datos con ocultación de información sensible para el almacenamiento en la nube seguro.
	2019	[9]	Propone un método de auditoría pública de preservación de privacidad para el almacenamiento seguro de datos en la nube.
Auditoría basada en atributos	2023	[6]	Se propone un esquema de encriptación basado en atributos que permite ocultar información sensible y garantizar la integridad de los datos en la nube. Se muestra cómo el uso de esta técnica puede mejorar la eficiencia y seguridad del almacenamiento de datos en la nube en el sector de la salud.
	2022	[13]	Propone un esquema de auditoría basado en atributos que permite a los usuarios compartir datos en la nube de forma segura.
Auditoría multi-copia	2023	[5]	Se propone un esquema de auditoría para garantizar la integridad de datos en la nube utilizando técnicas de almacenamiento redundante. Se muestra cómo el uso de

			múltiples copias de los datos permite detectar y corregir errores de almacenamiento.
	2023	[3]	Se presenta un esquema de auditoría para garantizar la integridad de datos en la nube y en sistemas de Internet de las cosas (IoT). Se utilizan técnicas de almacenamiento redundante para mejorar la seguridad y eficiencia del almacenamiento de datos.
Auditoria basada en árboles Merkle	2021	[1]	Propone un método de integridad de datos para auditoría dinámica en entornos en la nube.
	2023	[7]	Se presenta un esquema de auditoría dinámica basado en árboles de hash de Merkle jerárquicos para garantizar la integridad de datos en la nube. Se muestra cómo el uso de esta técnica permite detectar y corregir errores de almacenamiento en tiempo real.
	2020	[28]	El protocolo propuesto es públicamente verificable y admite operaciones dinámicas en los datos. Además, se menciona que la seguridad del protocolo propuesto se basa en la estabilidad del problema computacional de Diffie Hellman en un modelo aleatorio de Oracle.
Auditoría difusa	2019	[14]	Se presentan dos esquemas de auditoría para garantizar la integridad de datos en la nube utilizando técnicas de encriptación y almacenamiento redundante. Se muestra cómo estas técnicas pueden mejorar la eficiencia y seguridad del almacenamiento de datos en sistemas de almacenamiento masivo.
		[29]	El esquema propone utilizar datos biométricos (como escaneo de iris o huella digital) como una clave privada difusa del usuario, con el objetivo de realizar la auditoría de integridad de datos sin depender de un token de hardware para almacenar la clave privada.
Verificación de integridad en nube	2018	[8]	Propone un esquema de auditoría de datos para dispositivos móviles en almacenamiento en la nube.
	2020	[10]	Propone un enfoque para hacer la auditoría de almacenamiento en la nube más utilizable y adaptable a diferentes requisitos de auditoría.
	2018	[15]	Propone un esquema de auditoría de Big Data en la nube que utiliza tablas divididas y conquistadas para mejorar la eficiencia de la auditoría.
	2019	[16]	Propone un esquema de auditoría de integridad en tiempo real para imágenes en sistemas de almacenamiento en la nube con arbitraje de privacidad
Privacidad en auditoría en nube	2020	[17]	Propone un protocolo de auditoría de nube que preserva la privacidad de los usuarios en grupos
	2019	[18]	Propone un esquema de auditoría de datos en la nube que preserva la privacidad de los datos de los usuarios

	2020	[19]	Propone un esquema de auditoría en la nube que preserva la privacidad de múltiples usuarios y tiene autorización y trazabilidad
	2022	[20]	Propone un protocolo de auditoría en la nube que preserva la privacidad de los datos médicos de los pacientes

Como se puede apreciar en la Tabla 3, se realizó la agrupación de artículos mediante un método emergente en común, teniendo cada una de ellas un resultado distinto claramente. Cabe mencionar dos enfoques diferentes que han sido investigados anteriormente y dado que no son técnicas emergentes solo se les brindará un breve concepto, esto no quiere decir que no sean importantes sino son de suma relevancia en la auditoría de almacenamiento en la nube, el primer enfoque es la prueba de esquemas basados en recuperabilidad (PoR). Comenzaremos definiendo qué es la recuperabilidad de datos para que puedan entender mejor el enfoque. La recuperabilidad es una necesidad de seguridad que brinda a los usuarios la certeza que una sección de datos está realmente en el almacenamiento [23]. Habiendo determinado lo que es la recuperabilidad de datos definiremos el primer enfoque. Este primer enfoque para el proceso de auditoría comprueba que los datos que que son externalizados cuenten con valores difíciles de descifrar previamente incrustados en posiciones ocultas. Esto permite que los datos seguros cuenten con alta protección mediante el constante cambio aleatorio de los datos externalizados, con el fin de que todos los bloques de datos no aparenten ser correlacionados sino aleatorios. Por eso si los datos ocultos se dañan, el usuario se dará cuenta del daño y comprobará que los datos están quebrados [10][22][23].

El segundo enfoque son los esquemas basados en posesión de datos demostrables (PDP). Este enfoque aplica la autenticación homomórfica, es decir exige a la nube que le proporciona una combinación lineal aleatoria de bloque de datos que han sido externalizados con su información de autenticación correspondiente. Si los datos que ha respondido la nube no pasan las validaciones de autenticación, se concluye que los datos están dañados [24]-[29].

Se realizó un gráfico, detallado en la figura 3, para que se aprecie la proporción de artículos por métodos emergentes y permita una mejor visión a los autores, y en base a estas proporciones tomar decisiones de aceptación de cada método.

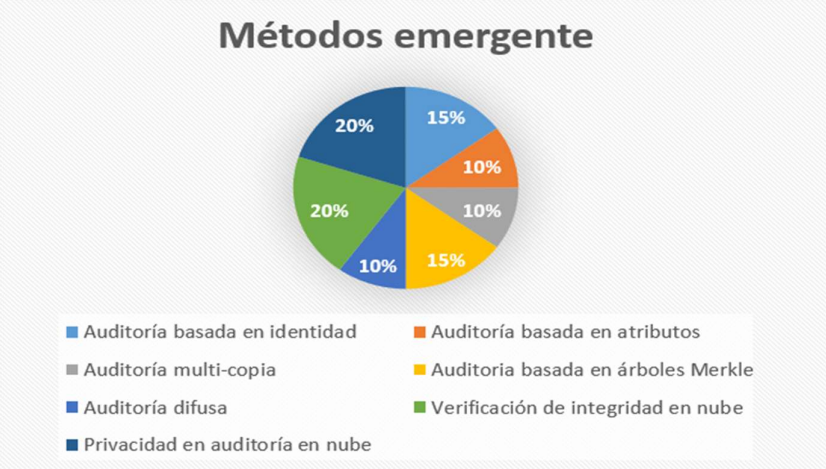

Figura 3: Gráfico de proporción de artículos por método.

Fuente: Elaborada por los autores

La seguridad de la integración en la nube es tema fundamental para las personas u organizaciones interesadas en la integración de datos en la nube, puesto que pueden contar con información confidencial además con la seguridad de que esos datos se mantengan su integridad en la nube con el transcurrir del tiempo y no hayan sido adulterados o manipulados.

Es por eso que en la Figura 4, adaptada de [10] por los autores, se muestra el modelo típico de auditoría de integración de datos en la nube, con la finalidad de que el lector obtenga conocimiento de cuál es la secuencia en la integración de datos en la nube.

Figura 4: Modelo de auditoría de integración de datos en la nube.

Como se observa, existen dos entidades, el usuario y la nube; como ya sabemos la integración de datos en la nube no asegura la integridad de estos. Es por eso que el usuario añade una clave de autenticación secreta cuando se externaliza sus datos a la nube.

Luego el usuario debe auditar la nube cada cierto tiempo para verificar si los datos externalizados están dañados, esto se hace mediante un protocolo de respuesta de desafío. Durante esta fase, el usuario hace una consulta de datos a la nube. La nube recibe esta consulta y responde una prueba al usuario mostrando que los datos están intactos. Finalmente, el usuario verifica si la prueba es convincente por medio de un esquema de auditoría de integración de datos en la nube. La ventaja de un esquema de auditoría de integración de datos en la nube es que el usuario puede detectar si existe algún daño de los datos utilizando la prueba corta devuelta, incluso cuando la nube intenta engañar sobre los daños de los datos [10].

Habiendo explicado el modelo de auditoría, es momento de mencionar los diferentes métodos de KeyGen para externalizar de manera segura los datos a la nube; y para ellos se ha observado en los diferentes artículos algunas metodologías que proponen los autores:

- **Criptografía Homomorfa de Paillier:** La criptografía homomórfica de Paillier se utiliza para la generación de claves públicas y privadas para el cifrado y descifrado mediante la función de Euler [8].
- **Criptografía de clave pública:** Se utilizan 2 claves, una se encarga de cifrar y la segunda de descifrar el mensaje además solo debe ser conocido por el emisor del mensaje [2].
- **Criptografía hash:** Algoritmo matemático que convierte los bloques de información en una nueva serie de caracteres que tienen tamaño fijo [7].
- **Criptografía de atributos:** El descifrado del mensaje secreto solo es posible si los atributos de la clave del destinatario coinciden con los atributos del mensaje cifrado [6].
- **Árbol de Merkle:** Está compuesta por hashes de diferentes bloques de datos, esto sirve como resumen de todas las transacciones posibles [7].
- **Cifrado basado en identidad:** Es una técnica en donde da la posibilidad a los usuarios de cifrar y descifrar datos utilizando identificadores, como direcciones de correo electrónico o nombres de usuario, en lugar de claves criptográficas tradicionales [14].

4. DISCUSIÓN

Los resultados presentados en este artículo responden a la pregunta de investigación al mencionar y describir los métodos emergentes de auditoría en la integridad de datos en la nube. Sin embargo, todavía existen numerosos desafíos relacionados con la seguridad y privacidad de los datos en la nube que están siendo investigados y esperando una solución. Es importante destacar que el propósito principal de este artículo es informar sobre los métodos emergentes encontrados en otros estudios, y no proporcionar una solución completa para cada uno de ellos. Por lo tanto, se debe utilizar este artículo como referencia para profundizar en el tema y desarrollar sus propios métodos de auditoría, con el objetivo de integrar sus datos en la nube de manera segura.

5. CONCLUSIONES

Los métodos de auditoría en integridad de datos en la nube están evolucionando constantemente, y se han desarrollado numerosos enfoques innovadores para abordar los desafíos actuales de seguridad en la nube. Los enfoques propuestos tienen como objetivo garantizar la integridad de los datos almacenados en la nube, sin comprometer la privacidad de los usuarios.

Estos métodos emergentes presentados, se basan en criptografía y diferentes técnicas para garantizar la integridad de los datos almacenados en la nube.

Como se observa en la Figura 3 la privacidad de auditoría en la nube y privacidad en la nube tienen el 20% siendo el más alto más alto y por consiguiente los más usados, por el contrario, se observa que auditoría basada en atributos, multi-copia y difusa representa al porcentaje más bajo con 10%, concluyendo que son los menos usados.

Por otro lado, se debe tomar en consideración métodos que a la actualidad son obsoletos pero que en su momento fueron importantes y daban un gran aporte para la realización de la auditoría que son las pruebas basadas en recuperabilidad y las pruebas basadas en posesión de datos, que ambos tienen la finalidad de detectar si los datos almacenados están dañados utilizando diferentes caminos.

Los métodos emergentes también son capaces de detectar la corrupción de datos y proporcionan mecanismos de recuperación de datos para garantizar la disponibilidad y la fiabilidad de los datos en la nube. Sin embargo, existe la necesidad de soluciones de auditoría en la nube que sean más eficientes en términos de costo y computacionalmente menos intensivas para abordar las limitaciones de rendimiento y escalabilidad de los enfoques actuales.

Para concluir, la revisión sistemática muestra que los métodos emergentes de auditoría en integridad de datos en la nube tienen un gran potencial para mejorar la seguridad de los datos en la nube, pero todavía hay desafíos que necesitan ser abordados para lograr una implementación efectiva en entornos del mundo real.

REFERENCIAS

[1] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu, J. Ma. "Data integrity method for dynamic auditing in cloud environment." *IEEE Transactions on Cloud Computing*, vol. 9, pp. 1408-1421. 2021.

[2] B. Shao, L. Zhang, G. Bian. "Incentive Public Auditing Scheme with Identity-Based Designated Verifier in Cloud." *Electronics (Switzerland)*, vol. 12, Marzo. 2023.

[3] T. Sang, P. Zeng, K. Choo. "Provable Multiple-Copy Integrity Auditing Scheme for Cloud-Based IoT." *IEEE Systems Journal*, vol. 17, pp. 224-233, Marzo. 2023.

[4] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu. "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage." *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 331-346, Febrero. 2019.

[5] Z. Tu, X. An Wang, W. Du, Z. Wang, M. Lv. "An improved multi-copy cloud data auditing scheme and its application." *Journal of King Saud University - Computer and Information Sciences*, vol. 35q, pp. 120-130, Marzo. 2023.

[6] H. Wang, J. Liang, Y. Ding, S. Tang, Y. Wang. "Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health." *Computer Standards and Interfaces*, vol. 84, Marzo. 2023.

[7] Z. Liu, S. Wang, S. Duan, L. Ren, J. Wei. "Dynamic Data Integrity Auditing Based on Hierarchical Merkle Hash Tree in Cloud Storage." *Electronics (Switzerland)*, vol. 12, Febrero. 2023.

[8] L. Krithikashree, S. Manisha, M. Sujithra. "Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage." in *Proc. ICCCNT*, 2018, pp. 1-5.

[9] H. Tian, F. Nan, C. Chang, Y. Huang, J. Lu, Y. Du. "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing." *Journal of Network and Computer Applications*, vol. 127, pp. 59-69, Febrero. 2019.

[10] F. Chen, F. Meng, T. Xiang, H. Dai, J. Li, J. Qin. "Towards Usable Cloud Storage Auditing." *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, pp. 2605-2617, Noviembre. 2020.

[11] M. Page, et al. "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews". 2021. doi: 10.1136/bmj.n71

[12] C. Manterola. "Revisiones sistemáticas de la literatura. Qué se debe saber acerca de ellas". 2013. doi: 10.1016/j.ciresp.2011.07.009

[13] A. Fu, S. Yu, Y. Zhang, H. Wang, C. Huang. "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users." *IEEE Transactions on Big Data*, vol. 8, pp. 14-24, Febrero. 2022.

[14] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni. "Fuzzy identity-based data integrity auditing for reliable cloud storage systems." *IEEE Transactions on Dependable and Secure Computing*, vol. 16, pp. 72-83, Enero-Febrero. 2019.

[15] M. Sookhak, R. Yu, A. Zomaya. "Auditing Big Data Storage in Cloud Computing Using Divide and Conquer Tables." *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, pp. 999-1012, Marzo. 2018.

[16] X. Tang, Y. Huang, C. -C. Chang, L. Zhou. "Efficient Real-Time Integrity Auditing with Privacy-Preserving Arbitration for Images in Cloud Storage System" in *IEEE Access*, vol. 7, pp. 33009-33023, Marzo. 2019.

[17] J. Zhang, B. Wang, X. Wang, H. Wang, S. Xiao. "New group user based privacy preserving cloud auditing protocol" *Future Generation Computer Systems*, vol. 106, pp. 585-594, Mayo. 2020.

[18] S. Anbuchelian, C. Sowmya, C. Ramesh. “Efficient and secure auditing scheme for privacy preserving data storage in cloud” *Cluster Comput*, vol. 22, pp. 9767-9775, Julio. 2019.
[19] X. Yang, M. Wang, T. Li, R. Lui, C. Wang. “Privacy-Preserving Cloud Auditing for Multiple Users Scheme with Authorization and Traceability” in *IEEE Access*, vol. 8, pp. 130866-130877, Julio. 2020.
[20] X. Li, S. Liu, R. Lu, M. Khurram, K. Gu, X. Zhang. “An Efficient Privacy-Preserving Public Auditing Protocol for Cloud-Based Medical Storage System” IEEE J Biomed Health Inform., Mayo. 2022.
[21] Y. Zhang, H. Zhang, R. Hao, J. Yu. “Authorized identity-based public cloud storage auditing scheme with hierarchical structure for large-scale user groups” in China Communications, vol. 15, pp. 111-121, Noviembre. 2018.
[22] A. Juels, B. Kaliski. “Pors: proofs of retrievability for large files” in *Proceedings of the 14th ACM conference on Computer and communications security (CCS '07)*, pp 584–597, Octubre 2007.
[23] M. Azraoui, K. Elkhiyaoui, R. Molva, M. Önen. “StealthGuard: Proofs of Retrievability with Hidden Watchdogs.” in *Computer Security - ESORICS 2014*, vol 8712, pp 239–256, 2014.
[24] H. Tian, Y. Chen, H. Jiang, Y. Huang, F. Nan, Y. Chen, “Public Auditing for Trusted Cloud Storage Services”, in IEEE Security & Privacy, vol. 17, no. 1, pp. 10-22, Jan.-Feb. 2019.
[25] L. Zhou, A. Fu, S. Yu, M. Su, B. Kuang, “Data integrity verification of the outsourced big data in the cloud environment: A survey”, Journal of Network and Computer Applications, vol 122, pp 1-15, Noviembre. 2018.
[26] H. Wang, D. He, J. Yu, Z. Wang, "Incentive and Unconditionally Anonymous Identity-Based Public Provable Data Possession", in IEEE Transactions on Services Computing, vol. 12, no. 5, pp. 824-835, Octubre. 2019.
[27] J. Li, H. Yan, Y. Zhang, "Identity-Based Privacy Preserving Remote Data Integrity Checking for Cloud Storage" in IEEE Systems Journal, vol. 15, no. 1, pp. 577-585, Marzo 2021.
[28] N. Garg, S. Bawa, N. Kumar. “An efficient data integrity auditing protocol for cloud computing” in Future Generation Computer Systems, vol. 109, pp. 306-316. 2020.
[29] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu y J. Ma, "Data Integrity Auditing without Private Key Storage for Secure Cloud Storage", en IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1408-1421, 1 Oct.-Dec. 2021, doi: 10.1109/TCC.2019.2921553.