Control de accesos en seguridad de la información: Una revisión sistemática de las técnicas actuales

Access control in information security: A systematic review of current techniques

Recibido: octubre 04 de 2023 | Revisado: octubre 30 de 2023 | Aceptado: noviembre 25 de 2023

Jean Pacheco[1]
Josue Chavez[1]
Alberto Mendoza De los Santos[1]

Resumen

En el dinámico escenario de la ciberseguridad actual, la gestión efectiva de accesos a sistemas y datos críticos es fundamental para salvaguardar la integridad y confidencialidad de la información. Este artículo presenta una revisión sistemática de las técnicas de control de accesos más prominentes en los últimos cinco años (2019-2023), con el objetivo de proporcionar una visión actualizada de las tendencias en seguridad de la información. La revisión, basada en una meticulosa selección de artículos de Scopus, SciELO, IEEE y Google Académico, se adhiere a la metodología PRISMA para garantizar una revisión sistemática rigurosa y completa. Se identificaron y evaluaron técnicas avanzadas como CP-ABE, ABAC, RBAC, ACE-BC, ABSE, entre otras, que representan avances significativos en el control de accesos y la protección de la información sensible. Los resultados obtenidos destacan la importancia crítica de estas técnicas en la seguridad de la información, proporcionando un panorama claro de las herramientas más eficaces en la protección de activos digitales. En última instancia, esta revisión no solo informa sobre las últimas tendencias, sino que también impulsa futuras investigaciones en el ámbito del control de accesos y la seguridad de la información.

Palabras clave: control de acceso, seguridad de la información, ciberseguridad

Abstract

In today's dynamic cybersecurity scenario, effective management of access to critical systems and data is essential to safeguard the integrity and confidentiality of information. This article presents a systematic review of the most prominent access control techniques in the last five years (2019-2023), with the aim of providing an updated view of trends in information security. The review, based on a meticulous selection of articles from Scopus, SciELO, IEEE and Google Scholar, adheres to the PRISMA methodology to ensure a rigorous and complete systematic review. Advanced techniques such as CP-ABE, ABAC, RBAC, ACE-BC, ABSE, among others, were identified and evaluated, which represent significant advances in access control and the protection of sensitive information. The results obtained highlight the critical importance of these techniques in information security, providing a clear overview of the most effective tools in the protection of digital assets. Ultimately, this review not only informs the latest trends but also drives future research in the area of access control and information security.

Keywords: Access control, information security, cybersecurity

1 Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo. Trujillo, Perú.

Autor de correspondencia:
jcpachecog@unitru.edu.pe

https://doi.org/10.24265/campus.2023.v28n36.01

Introducción

En el contexto de seguridad de la información, existen muchas estrategias que pueden ayudar a salvaguardar la información sensible, las cuales tienen una relevancia aún más importante considerando la digitalización actual. Entre las formas de proteger la información se encuentra el control de acceso, el cual se refiere a un conjunto de medidas que tienen como objetivo proteger determinados recursos de usuarios no autorizados.

En el presente artículo de revisión sistemática, nos centramos en examinar la variedad de medidas existentes para la implementación de un control de acceso, analizando cuáles son los factores diferenciales de cada una de estas. También exploramos cuáles de estas técnicas son las más utilizadas, y el motivo por el que se tiene una mayor preferencia a favor de algunas, analizando el contexto en el que fueron implementadas.

Método

Para la elaboración del presente artículo se llevó a cabo una revisión sistemática de la literatura científica, siguiendo las bases establecidas por la metodología PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), y haciendo uso del diagrama de flujo que esta metodología propone (Quispe et al., 2021). Este proceso nos permitió establecer la siguiente pregunta de investigación: ¿Cuáles son las estrategias más utilizadas para la gestión del control de accesos y cómo se han aplicado en el contexto de seguridad de la información?

Fundamentación de la metodología

Una revisión sistemática es un resumen claro y estructurado de la información disponible orientada a responder una pregunta específica, y se caracteriza por describir el proceso de elaboración transparente y comprensiblemente (Moreno et al., 2018). Este proceso hace uso de una metodología clara y sistematizada, con el fin de reducir sesgos en la identificación, selección, síntesis y resumen de los estudios (Quispe et al., 2021). Los pasos a seguir para la elaboración de una revisión sistemática según (Moreno et al., 2018) son: Planteamiento de la pregunta estructurada, búsqueda en base de datos, selección de artículos, extracción de datos, análisis críticos y estadísticos, y finalmente, la exposición de los resultados.

Por otro lado, la metodología PRISMA hace referencia a pautas que buscan orientar a los autores en la planificación de revisiones sistemáticas mediante un conjunto de ítems de inclusión, con la finalidad de proporcionar la justificación y el enfoque metodológico a la investigación (Quispe et al., 2021).

Proceso de recolección de información

Continuando con los pasos recomendados por (Moreno et al., 2018), realizamos una búsqueda de información estableciendo como términos clave a las palabras “control de acceso”, “seguridad de la información” y “técnicas” para alcanzar un mayor nivel de precisión, abarcando de esta manera a la pregunta de investigación en su totalidad.

Para el desarrollo de la presente revisión, establecimos como fuente de búsqueda a

las bases de datos Scopus, IEEE Xplore, SciELO y al motor de búsqueda Google Académico.

Criterios de inclusión y exclusión

De acuerdo a (Moreno et al., 2018), se deben establecer criterios de inclusión y exclusión que permitan analizar críticamente a los artículos y obtener aquellos que respondan claramente a nuestra pregunta de investigación planteada.

En base a ello y a los propósitos de nuestra investigación, establecimos los siguientes criterios de inclusión y exclusión.

Criterios de inclusión

- Se incluyeron solo documentos de tipo artículo y conference paper.
- Se incluyeron artículos publicados en inglés y español.
- Se incluyeron publicaciones solo desde el año 2018 al 2023.

Criterios de exclusión

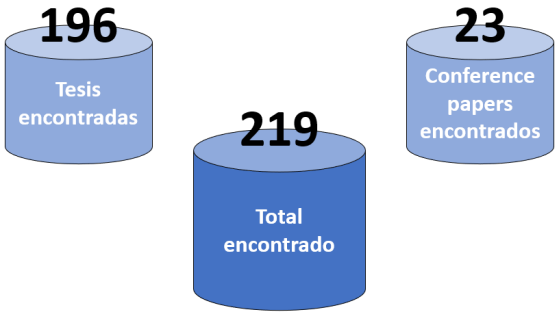
- Se excluyeron las publicaciones que pertenezcan a áreas no relevantes a nuestra investigación.
- Se excluyeron las publicaciones que no sean de acceso libre.
- Se excluyeron los artículos repetidos.

Catálogos y bases de datos

La búsqueda realizada para la elaboración de nuestra revisión sistemática nos dio un total de 219 publicaciones originales, divididas entre las siguientes fuentes: Scopus (119), IEEE Xplore (95), SciELO (2), Google Académico (3); las cuales nos brindaron tanto artículos como conference papers, tal y como se muestra en la siguiente figura.

Figura 1

Resultados de la búsqueda



Para la obtención de estos resultados, se realizaron las siguientes consultas para cada una de las fuentes:

Scopus:
TITLE-ABS-KEY (control AND access AND security AND information AND techniques) AND PUBYEAR > 2018 AND PUBYEAR < 2024 AND (LIMIT-TO (OA, "all")) AND (LIMIT-TO (SUBJAREA, "ENGI") OR LIMIT-TO (SUBJAREA, "COMP")) AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp")) AND (LIMIT-TO (LANGUAGE, "English")) AND (LIMIT-TO (EXACTKEYWORD, "Access Control") OR LIMIT-TO (EXACTKEYWORD, "Information Security"))

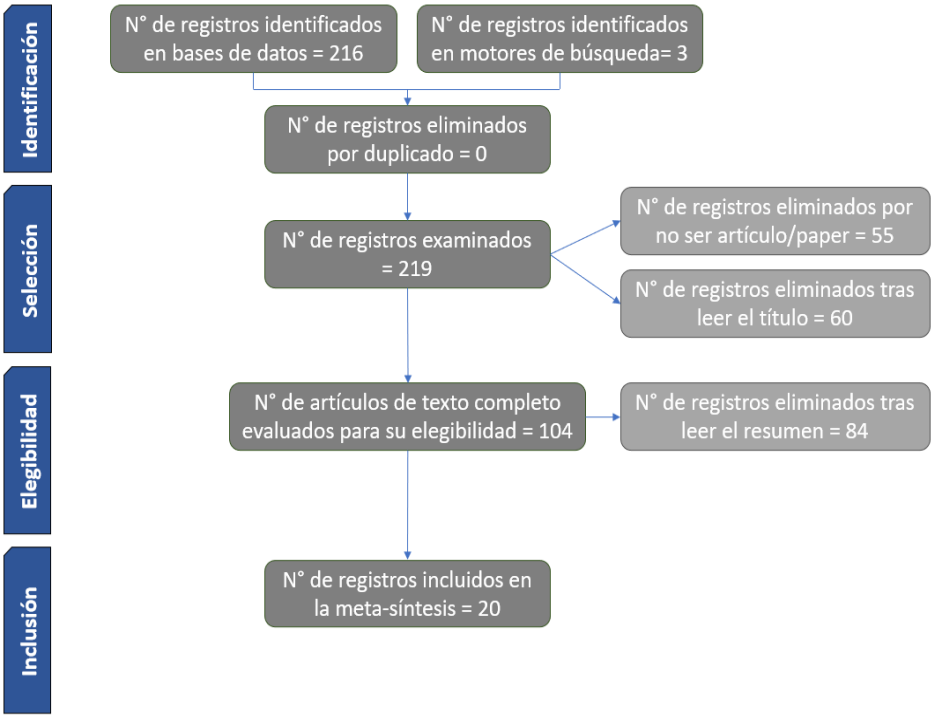
IEEE Xplore:
(control AND access AND security AND information AND techniques)

SciELO:
(control AND access AND security AND information AND techniques)

Google Académico:
Control Access and security information and techniques

Una vez realizadas las consultas mencionadas, aplicamos nuestros criterios de inclusión y excusión a las publicaciones obtenidas, tal y como se muestra en el siguiente flujograma sugerido por la metodología PRISMA, también conocido como diagrama de flujo de selección de artículos (Moreno et al., 2018).

Figura 2
Flujograma PRISMA



Resultados

Habiendo aplicado los criterios de inclusión y exclusión a los resultados obtenidos (Figura 2), rescatamos un total de 20 publicaciones, de las cuales rescatamos ALGO, tal y como se muestra en la siguiente tabla.

Tabla 1
Publicaciones seleccionadas para la revisión.

N	TÍTULO	AUTORES	AÑO	RESULTADO	TÉCNICA / TECNOLOGÍA
1	EVOAC-HP: An Efficient and Verifiable Out-sourced Access Control Scheme with Hidden Policy	Haobin Ma, Dehua Zhou, Peng Li, Xiaoming Wang.	2023	EVOAC-HP es un sistema de control de acceso que usa cifrado para proteger datos médicos. Tiene cinco etapas e implica a certificadores, dueños de datos, usuarios y proveedores de servicios en la nube. También se sugieren aplicaciones fuera de la medicina.	Utiliza la técnica de atributo de control de acceso basado en políticas (CP-ABE).

2	Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System	Abdullah Alharbi.	2023	Destacan la relevancia del intercambio de datos de ciberseguridad y cómo el marco ACE-BC asegura esta transmisión. Se menciona la importancia de un control de acceso distribuido y se introduce un sistema basado en blockchain para esto. También se hacen alusiones a otras medidas de seguridad como el aprendizaje federado y la arquitectura de seguridad de datos en la nube.	Utilizan la técnica de Access Control Enabled Blockchain (ACE-BC)
3	Secured and Privacy-Preserving Multi-Authority Access Control System for Cloud-Based Healthcare Data Sharing	Reetu Gupta, Priyesh Kanungo, Nirmal Dagdee, Golla Madhu, Kshira Sagar Sahoo, N. Z. Jhanjhi, Mehedi Masud, Nabil Sharaf Almalki, Mohammed A. AlZain.	2023	Describen un sistema de control de acceso seguro y privado para compartir datos de salud en la nube. Utiliza técnicas de cifrado y encriptación basada en atributos según políticas para permitir un control detallado y adaptable para usuarios de diferentes tipos de dominios. También se destaca su capacidad de escalar y resistir ataques de colusión.	Utiliza la técnica encriptación basada en atributos según políticas (CP-ABE).
4	PICO: Privacy-Preserving Access Control in IoT Scenarios through Incomplete Information	Sciancalepore Savio, Zannone Nicola.	2022	PICO es un marco para el control de acceso en IoT que prioriza la privacidad. Facilita la compartición de datos basándose en riesgos de divulgación de atributos. También permite evaluar políticas de acceso con información incompleta y calcular riesgos.	La tecnología o técnica de control de acceso utilizada es PICO
5	DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data	Hafida Saidi, Nabila Labraoui, Ado Adamou Abba Ari, Leandros Maglaras, Joel Herve Mboussam Emati.	2022	El DSMAC es un sistema innovador que utiliza blockchain para gestionar el acceso descentralizado a datos médicos. Emplea contratos inteligentes y un modelo de identidad auto-soberana para proteger la privacidad de los pacientes y darles control sobre quién accede a su información médica.	Utilizan las técnicas de Control de Acceso Basado en Roles (RBAC) y Control de Acceso Basado en Atributos (ABAC)
6	Blockchain Privacy Data Access Control Method Based on Cloud Platform Data	Biying Sun, Qian Dang, Yu Qiu, Lei Yan, Chunhui Du, Xiaoqin Liu	2022	El artículo propone un sistema de protección de privacidad para datos multidimensionales en la IoT en la nube. Emplea cifrado homomórfico EBGN y cifrado de atributos para un control de acceso detallado, asegurando la seguridad de los datos y simplificando operaciones. La investigación confirma mejoras en privacidad y reducción de riesgo de acceso no autorizado.	Utiliza la técnica de control de acceso basada en el cifrado de atributos con políticas de texto cifrado (CP-ABE).
7	An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad-Hoc Networks	Muhammad Asghar Khan, Insaf Ullah, Neeraj Kumar, Omar Sami Oubbati, Ijaz Mansoor Qureshi, Fazal Noor, Fahim Ullah.	2021	Proponen un esquema de control de acceso y acuerdo de clave para Redes Ad-hoc de Drones Voladores (FANETs). Utiliza Criptografía de Curva Hiperelíptica y una función hash resistente a colisiones. Este enfoque asegura la calidad de servicio en redes multi-salto y se adapta a las limitaciones de recursos de los drones	La tecnología o técnica Criptografía de Curva Hiperelíptica (HECC).

8	BFR-SE: A Blockchain-Based Fair and Reliable Searchable Encryption Scheme for IoT with Fine-Grained Access Control in Cloud Environment	Hongmin Gao, Shoushan Luo, Zhaofeng Ma, Xiaodan Yan, Yanping Xu.	2021	Muestran una solución innovadora para la privacidad y confiabilidad en el almacenamiento de datos de IoT en la nube. Utiliza un esquema de búsqueda encriptada con tecnologías como cifrado basado en políticas de atributos, filtros de Bloom y blockchain. Garantiza equidad y confiabilidad, con control de acceso preciso y buen rendimiento.	La técnica de control de acceso utilizada es el "Cifrado Basado en Políticas de Atributos" (ABSE).
9	A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection	Yingwen Chen, Linghang Meng, Huan Zhou, Guangtao Xue.	2021	Usan Hyperledger Fabric, una tecnología blockchain, para compartir datos médicos de forma segura. Se aplica K-anonimato para proteger la identidad y cifrado de búsqueda de palabras clave para la privacidad. Un contrato inteligente facilita el control de acceso. Análisis respalda la viabilidad y escalabilidad del sistema.	El artículo utiliza una técnica de control de acceso basada en atributos (ABAC, por sus siglas en inglés).
10	AES-CP-IDABE: A privacy protection framework against a DoS attack in the cloud environment with the access control mechanism	Sonali Chandel, Geng Yang, Sumit Chakravarty.	2020	Hablan de AES-CP-IDABE, un nuevo modelo de cifrado para proteger la privacidad de datos en la nube. Utiliza doble cifrado con ABE y AES. El acceso se controla con firmas digitales basadas en la identificación del usuario y claves de seguridad, y detecta ataques DoS monitoreando direcciones IP. Este modelo mejora el rendimiento y detección de ataques respecto al ABE convencional. Se sugiere adaptarlo para entornos multiusuario basados en roles en la nube en futuras mejoras.	El artículo utiliza la técnica de control de acceso basada en firmas digitales junto con atributos de usuario para proteger los datos en la nube.
11	EDES-ACM: Enigma diagonal encryption standard access control model for data security in cloud environment	Sameer, Harish Rohil.	2020	Nos muestran el framework EDES-ACM para la seguridad de datos en la nube. Utiliza el algoritmo EDES para controlar el acceso. Involucra firmas de grupo y encriptación. La supervisión y revocación de usuarios son parte del sistema. Destaca por su enfoque en seguridad y eficiencia, con planes de integrar blockchain en el futuro.	El artículo utiliza la técnica de control de acceso Enigmatic Diagonal Encryption Standard (EDES).
12	Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments	Rubina Ghazal, Ahmad Kamran Malik, Nauman Qadeer, Basit Raza, Ahmad Raza Shahid, Hani Alquhayz.	2020	Proponen el marco de control de acceso "Intelligent RBAC (I-RBAC)" para asegurar datos y recursos en entornos multi-dominio. Utiliza roles basados en ocupaciones reales y agentes inteligentes. Se demuestra su eficacia con pruebas de implementación de tiempo lineal. También se destaca el uso de ontologías y políticas de seguridad en la gestión de conocimientos.	Utilizan la tecnología de control de acceso basada en roles, conocida como "Role-Based Access Control (RBAC)".

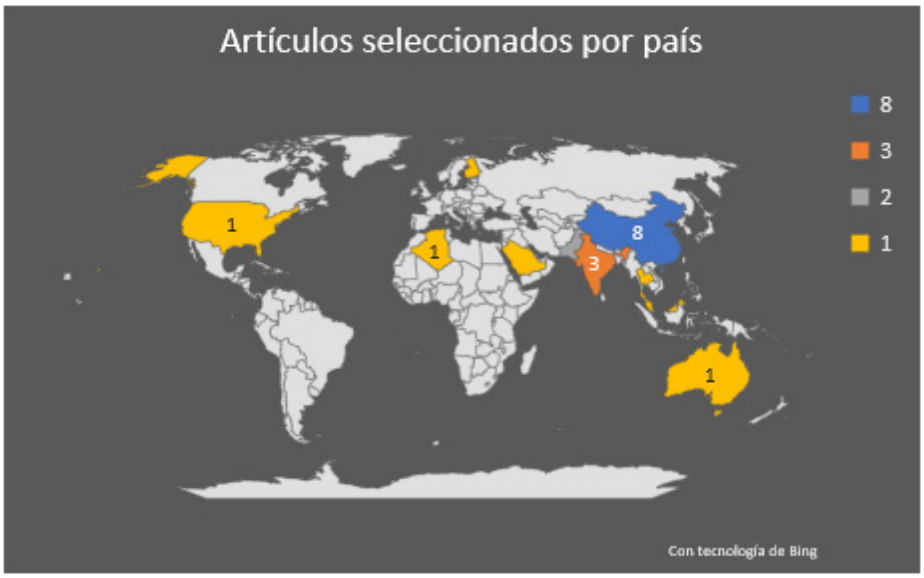
13	Key-enforced access control and performance analysis of DES and RSA cryptography in cloud computing	Y. Kiran Kumar, R. Mahammad Shafi.	2019	Enfatizan la importancia de la seguridad en la nube para proteger datos sensibles. Aborda el desafío de gestionar claves criptográficas en entornos de nube. Destaca la necesidad de que los dueños de datos mantengan el control del acceso a sus datos. Se sugiere un enfoque basado en claves. También se evalúa el rendimiento de diferentes algoritmos de cifrado. En resumen, se destaca la importancia de asegurar datos sensibles en la nube con técnicas de control de acceso y cifrado eficaces.	La tecnología de control de acceso utilizada es el "Control de Acceso Basado en Claves".
14	Fine-grained data access control with attribute-hiding policy for cloud-based IoT	Jialu Hao, Cheng Huang, Jianbing Ni, Hong Rong, Ming Xian, Xuemin Shen.	2019	Presentan un esquema de control de acceso para IoT basado en CP-ABE que protege la privacidad al ocultar atributos. Introduce un mecanismo de posicionamiento difuso para facilitar la localización eficiente. Se confirma su eficacia en seguridad y rendimiento con bajo costo computacional y de almacenamiento, evitando revelar información sensible a destinatarios no autorizados.	La técnica de control de acceso utilizada es Ciphertext-policy attribute-based encryption (CP-ABE).
15	Privacy-Preserving Data Sharing Using Multi-Layer Access Control Model in Electronic Health Environment	Shekha Chenthara, Khandakar Ahmed, Frank Whittaker.	2019	Abordan el intercambio de información de salud a través de Electronic Health Data (EHD). Propone el Modelo de Control de Acceso de Múltiples Capas (MLAC) para establecer un sistema seguro de EHR que permita a los pacientes compartir datos protegidos. Emplea el mecanismo de control de acceso PR-ABAC y la técnica de Procedencia para garantizar la integridad de los datos.	La técnica de control de acceso utilizada es el modelo de doble capa llamado "Pseudo-Role Attribute based access control (PR-ABAC)".
16	Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems	Thein Than Thwin, Sangsuree Vasupongayya.	2019	Proponen un sistema de registros de salud personales (PHR) basado en blockchain para asegurar la integridad de la información. Ofrece control de acceso detallado, consentimiento revocable, auditabilidad y resistencia a la manipulación. Un análisis de seguridad confirma su eficacia en la protección de la privacidad e integridad, superando en rendimiento a enfoques existentes.	La tecnología de control de acceso utilizada es "proxy reencryption" (re cifrado proxy).
17	Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-Based IoD Systems	Zhuo Ma, Jiawei Zhang.	2023	Abordan la protección de datos sensibles de vehículos aéreos no tripulados (UAVs) en un entorno distribuido e integrado con IoT y tecnologías 6G. Propone el esquema BPADAC, basado en blockchain, para el intercambio de datos de UAVs en la nube. Emplea técnicas de Atributos Basados en Cifrado Político (CP-ABE) para un acceso detallado y distribuido, asegurando la prestación del servicio y la privacidad de las políticas de acceso. También incluye trazabilidad de usuarios y almacenamiento distribuido con Distributed Hash Table (DHT).	Utilizan técnicas de Atributos Basados en Cifrado Político (CP-ABE).

18	The Cloud we Share: Access Control on Symmetrically Encrypted Data in Untrusted Clouds	Alexandros Bakas, Hai-Van Dang, Antonis Michalas, Alexandr Zalitko.	2020	Presentan "The Cloud we Share", un esquema híbrido de cifrado (SSE y ABE) para entornos de nube. Aborda el desafío de almacenamiento seguro de datos en crecimiento. Integra lo mejor de ambas técnicas y aprovecha Intel SGX para un control de acceso independiente de las primitivas criptográficas.	La tecnología de control de acceso utilizada es Intel SGX (Software Guard Extensions).
19	Security-Aware Information Dissemination With Fine-Grained Access Control in Cooperative Multi-RSU of VANETs	Xuejiao Liu, Wei Chen, Yingjie Xia.	2020	Describen la seguridad en la difusión de información en redes vehiculares ad hoc, específicamente en comunicaciones de vehículos a infraestructura. Propone un esquema de difusión con control de acceso detallado en estaciones cooperativas. Utiliza encriptación CP-ABE para garantizar confidencialidad y reencriptación proxy para la obtención de información en vehículos de alta velocidad.	El artículo utiliza la técnica basada en políticas de atributos (CP-ABE).
20	Enhanced security-aware technique and ontology data access control in cloud computing	Gangasandra Mahadevaiah Kiran, Narasimhaiah Nalini.	2020	Presentan un mecanismo (SA-ODAC) para seguridad y control de acceso a datos en almacenamiento en la nube, especialmente en el ámbito médico. Combina una técnica de concienciación de seguridad (SAT) con cifrado y fragmentación de archivos, y un control de acceso basado en ontologías (ODAC). Utiliza un esquema de compartición de secretos para gestionar las claves de SAT, logrando mayor eficiencia que técnicas convencionales.	El estudio utiliza la técnica de control de acceso basada en ontologías (ODAC).

Las publicaciones obtenidas y listadas en la tabla anterior, tienen diferentes lugares de origen, los cuales se ordenaron gráficamente por países en la siguiente figura.

Figura 3

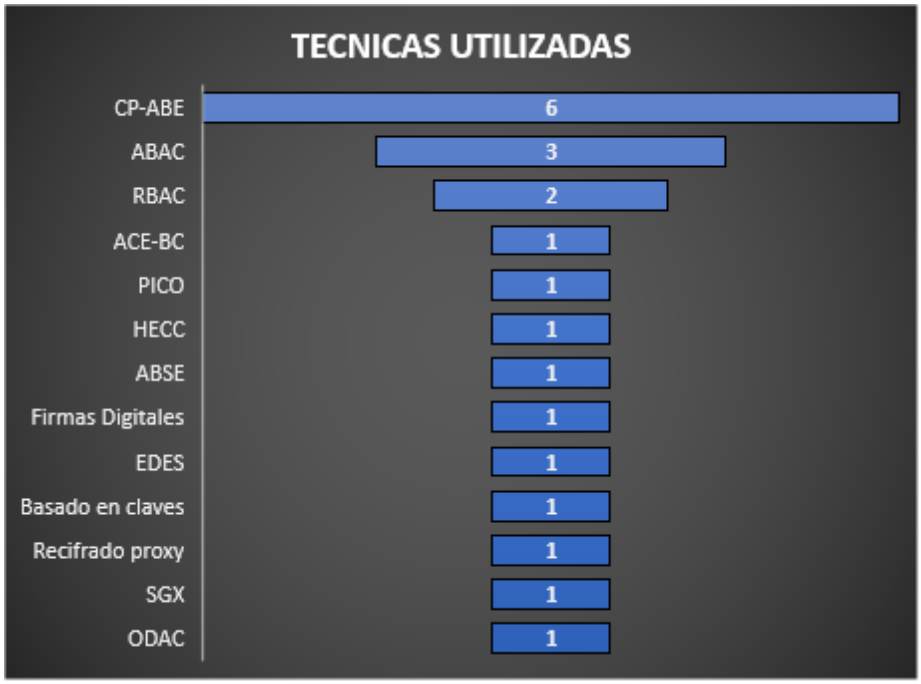
Artículos por país de origen



Las técnicas utilizadas en cada una de las publicaciones obtenidas también se ordenaron gráficamente, de modo que se pueda apreciar cuáles son las técnicas más utilizadas de acuerdo a los resultados encontrados.

Figura 4

Técnicas de control de acceso más utilizadas



Discusión

Técnica de atributos de control de acceso basado en políticas (CP-ABE)

Esta técnica consiste en asignar a cada usuario un conjunto de atributos en términos de claves secretas, las cuales se asignan según su cargo y el nivel de acceso que deben tener de acuerdo a las políticas establecidas por las autoridades de atributos de la organización, permitiendo el descifrado solo a aquellos que posean el conjunto de atributos que coincida con dicha política (Gupta et al., 2023).

Por otro lado, esta técnica tiene como defecto que deja expuesto el texto cifrado en el servidor de nube, por lo que, si alguien llega a acceder a él, no obtendría directamente los datos, pero sí podría observar las políticas que son necesarias para poder acceder a la información encriptada (Hao et al., 2019).

Técnica de control de acceso basada en atributos (ABAC)

Es una técnica de control de acceso similar a CP-ABE, que considera atributos, objetos, permisos y entorno como entradas; determina si otorgar autorización o no al objeto examinando si este contiene los atributos adecuados (Chen et al., 2021). Sin embargo, a diferencia de CP-ABE, esta técnica no encripta la información, sino que solo deniega el acceso a los usuarios que no tengan los atributos necesarios.

Técnica de control de acceso basada en roles (RBAC)

Esta técnica se basa en establecer roles a los que se les asignarán los permisos de acceso; una vez creados, a los usuarios se le asignan los roles correspondientes a la organización, para que de esta manera puedan acceder a la información adecuada (Ghazal et al., 2020). La desventaja de esta técnica es que los accesos son muy estáticos, de manera que no se podrían asignar permisos particulares que no pertenezcan a un rol específico.

Técnica Blockchain habilitada para control de acceso (ACE-BC)

Esta técnica se centra en el cifrado basado en atributos del usuario, en la cual el mecanismo de control de acceso es el encargado de limitar el acceso de usuarios no autorizados (Alharbi, 2023), de manera similar a la técnica CP-ABE. La diferencia radica en que la técnica de cifrado en este caso es blockchain, lo cual según (Alharbi, 2023) mejora el índice de confidencialidad considerablemente.

Marco de control de accesos PICO

PICO es el nombre de un marco que utiliza IoT para el control de acceso, el cual preserva la privacidad en escenarios IoT haciendo uso de información incompleta (Sciancalepore & Zannone, 2022). Este marco permite a los dispositivos evaluar los riesgos de privacidad asociados con las políticas de divulgación, y así determinar hasta qué punto se puede divulgar.

Técnica de criptografía de curva hiperelíptica (HECC)

Esta técnica consiste en un control de acceso basado en certificados y un esquema de acuerdo de claves, las cuales serán validadas para la desencriptación de la información según su nivel de acceso (Khan et al., 2021).

Técnica de cifrado basada en política de atributos (ABSE)

El modelo propuesto por (Gao et al., 2021) consiste en un algoritmo de cifrado de búsqueda basado en atributos, en el que se combinan blockchain y el filtro Bloom para establecer un esquema de cifrado confiable.

Técnica de control de acceso de firmas digitales

Esta técnica propuesta por (Chandel et al., 2020) está basada en la encriptación ABE, es decir por atributos. El punto diferencial en esta técnica es que la encriptación se realiza a través de firmas digitales, de manera que los usuarios puedan validar su identidad para descifrar la información que les corresponda según sus atributos.

Técnica enigmático estándar de cifrado diagonal (EDES)

Este modelo propuesto busca encriptar la información almacenada en la nube eficazmente, haciendo uso de estándares de encriptación diagonal basado en un generador de claves (Sameer & Rohil, 2020), buscando de esta manera que la información de la nube no sea un punto vulnerable para la información de una organización.

Técnica de control de acceso basado en claves

Al igual que la EDES, el enfoque de esta técnica se centra en los entornos de la nube;

sin embargo, esta última busca gestionar claves criptográficas para mantener protegidos los datos sensibles almacenados (Kumar & Mahammad, 2019), eliminando las vulnerabilidades con las que conviven técnicas como la CP-ABE.

Técnica de control de acceso re cifrado proxy

Mediante el proxy se busca en esta técnica establecer políticas de control de acceso detalladas y que permitan decisiones de revocación de consentimiento, tal y como lo usaron en su modelo los autores (Thein & Vasupongayya, 2019).

Técnica de control de acceso usando SGX

SGX es una tecnología de seguridad desarrollada por Intel que cuenta con un entorno aislado para el descifrado de archivos, la cual los autores (Bakas et al., 2020) usan para su modelo de cifrado, diseñando un mecanismo de revocación de accesos basándose únicamente en enclaves SGX.

Técnica de control de acceso basada en ontologías (ODAC)

Esta técnica propuesta por (Kiran & Nalini, 2020) se centra en el control de acceso a los datos de unidad de almacenamiento en la nube, manteniendo una política de permisos para los usuarios, y a su vez ayudándose de la técnica de reconocimiento seguro (SAT) para el autenticado del acceso a dichos datos.

Conclusiones

El control de acceso a los datos significa un gran desafío para todas las organizaciones que busquen invertir en la seguridad de su información sensible. Teniendo en cuenta la evidencia, podemos afirmar que existe una variedad de técnicas que cumplen un papel trascendental al controlar qué usuarios pueden acceder a cierta información, lo cual responde a nuestra pregunta de investigación planteada inicialmente: ¿Cuáles son las estrategias más utilizadas para la gestión del control de accesos y cómo se han aplicado en el contexto de seguridad de la información?

La revisión sistemática de los artículos seleccionados revela una preferencia mayoritaria que favorece a la técnica de atributos de control de acceso basado en políticas (CP-ABE), siendo esta la más utilizada de todas las encontradas. Debido a su especificidad en cuanto a los atributos que debe tener un usuario para desencriptar cierta información, es que esta técnica se ha vuelto tan adaptable para una gran cantidad de organizaciones; es por ello que incluso otras técnicas solo son una versión mejorada de esta, lo cual resalta aún más su relevancia en cuanto a control de accesos se refiere.

También es importante resaltar la eficacia de la técnica de control de acceso basada en atributos (ABAC), ya que de igual manera resulta bastante práctica y flexible al tener un enfoque similar a la CP-ABE, lo cual justifica su preferencia al permitir denegar el acceso a los usuarios que no tengan los atributos requeridos.

Por otro lado, la RBAC sugiere agrupar estos permisos en roles, y luego se asignar estos últimos a los usuarios, resultando bastante organizado para las grandes empresas que cuentan con una gran cantidad de empleados, facilitándoles la

agrupación por roles de sus empleados en lugar de asignarles permisos individualmente, he ahí el motivo de ser la tercera técnica preferida.

Cabe resaltar que, las demás técnicas también resultan útiles en sus respectivos enfoques; sin embargo, a pesar de su potencial, son propuestas nuevas y aún están por asentarse en el contexto de control de accesos, debido a ello es que aún no son muy conocidas ni utilizadas por las organizaciones a pesar de significar una mejora de las técnicas más asentadas.

Para finalizar, esperamos que el presente artículo de revisión sistemática sirva de impulso para futuras investigaciones científicas, brindando un contexto amplio y actualizado acerca de las técnicas utilizadas para el control de accesos en seguridad de la información. Además, esperamos que estos hallazgos sean de utilidad para profesionales y expertos en la rama de seguridad de la información, así como para las organizaciones que deseen informarse acerca de las técnicas que pueden implementar para la gestión de control de accesos en su empresa.

Referencias

Alharbi, A. (2023). Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System. https://doi.org/10.3390/s23063020

Bakas, A., Dang, H.-V., Michalas, A., & Zalitko, A. (2020). The Cloud we Share: Access Control on Symmetrically Encrypted Data in Untrusted Clouds. https://doi.org/10.1109/ACCESS.2020.3038838

Chandel, S., Yang, G., & Chakravarty, S. (2020). AES–CP–IDABE: A Privacy Protection Framework against a DoS Attack in the Cloud Environment with the Access Control Mechanism. http://dx.doi.org/10.3390/info11080372

Chen, Y., Meng, L., Zhou, H., & Xue, G. (2021). A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. https://doi.org/10.1155/2021/6685762

Chenthara, S., Ahmed, K., & Whittaker, F. (2019). Privacy-Preserving Data Sharing using Multi-layer Access Control Model in Electronic Health Environment. http://dx.doi.org/10.4108/eai.13-7-2018.159356

Gao, H., Luo, S., Ma, Z., Yan, X., & Xu, Y. (2021). BFR-SE: A Blockchain-Based Fair and Reliable Searchable Encryption Scheme for IoT with Fine-Grained Access Control in Cloud Environment. https://doi.org/10.1155/2021/5340116

Ghazal, R., Malik, A., Qadeer, N., Raza, B., Shahid, A., & Alquhayz, H. (2020). Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments. https://doi.org/10.1109/ACCESS.2020.2965333

Gupta, R., Kanungo, P., Dagdee, N., Madhu, G., Sahoo, K., Jhanjhi, N. Z., . . . AlZain, M. (2023). Secured

and Privacy-Preserving Multi-Authority Access Control System for Cloud-Based Healthcare Data Sharing. https://doi.org/10.3390/s23052617

Hao, J., Huang, C., Ni, J., Rong, H., Xian, M., & Shen, X. (2019). Fine-Grained Data Access Control with Attribute-Hiding Policy for Cloud-Based IoT. https://doi.org/10.1016/j.comnet.2019.02.008

Khan, M., Ullah, I., Kumar, N., Oubbati, O., Qureshi, I., Noor, F., & Ullah, F. (2021). An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad-hoc Networks. https://doi.org/10.1109/TVT.2021.3055895

Kiran, G., & Nalini, N. (2020). Enhanced security-aware technique and ontology data access control in cloud computing. https://doi.org/10.1002/dac.4554

Kumar, K., & Mahammad, S. (2019). Key-Enforced Access Control and Performance Analysis of DES and RSA Cryptography in Cloud Computing. http://www.doi.org/10.35940/ijeat.A9995.109119

Liu, X., Chen, W., & Xia, Y. (2020). Security-Aware Information Dissemination With Fine-Grained Access Control in Cooperative Multi-RSU of VANETs. https://doi.org/10.1109/TITS.2020.3034223

Ma, H., Zhou, D., Li, P., & Wang, X. (2023). EVOAC-HP: An Efficient and Verifiable Outsourced Access Control Scheme with Hidden Policy. https://doi.org/10.3390/s23094384

Ma, Z., & Zhang, J. (2023). Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-Based IoD Systems. https://doi.org/10.1109/ACCESS.2023.3272484

Moreno, B., Muñoz, M., Cuellar, J., Domancic, S., & Villanueva, J. (2018). Revisiones Sistemáticas: definición y nociones básicas. http://dx.doi.org/10.4067/S0719-01072018000300184

Quispe, A., Hinojosa, Y., Miranda, H., & Sedano, C. (2021). Serie de Redacción Científica: Revisiones Sistemáticas. http://cmhnaaa.org.pe/ojs/index.php/rcmhnaaa/article/view/906

Saidi, H., Labraoui, N., Ado, A., Maglaras, L., & Mboussam, J. (2022). DSMAC: Privacy-aware Decentralized SelfManagement of data Access Control based on blockchain for health data. https://doi.org/10.1109/ACCESS.2022.3207803

Sameer, & Rohil, H. (2020). EDES-ACM: Enigma Diagonal Encryption Standard Access Control Model for Data Security in Cloud Environment. https://dx.doi.org/10.14569/IJACSA.2020.0110841

Sciancalepore, S., & Zannone, N. (2022). PICO: Privacy-Preserving Access Control in IoT Scenarios through Incomplete Information. https://doi.org/10.1145/3477314.3508379

Sun, B., Dang, Q., Qiu, Y., Yan, L., Du, C., & Liu, X. (2022). Blockchain Privacy Data Access Control Method Based on Cloud Platform Data. https://doi.org/10.1109/CONECCT55679.2022.9865845

Thein, T., & Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. https://doi.org/10.1155/2019/8315614