Metodologías más usadas en la seguridad de bases de datos: Una revisión de la literatura científica, 2016- 2021

Most used methodologies in database security: A review ofthe scientific literature, 2016-2021

Recibido: enero 09 de 2022 | Revisado: abril 24 de 2022 | Aceptado: mayo 15 de 2022

Leodan Machuca[1]
Richard Braul[2]

Resumen

Presentamos una revisión sistemática sobre identificar las metodologías más utilizadas en seguridad de bases de datos partiendo de la revisión de publicaciones en revistas académicas en bases de datos de los últimos seis años. Se realizó una evaluacion de las bases de datos y metodologías de seguridad más comunes en la actualidad. Para desarrollar esto se revisó las bases de datos IEEE, ARXIV, HINDAWI y DIALNET. Luego, se aplicó los criterios de exclusión e inclusión ya establecidos y dio como resultado un total de 14 artículos que muestran los protocolos y metodologías para dar respuesta a la pregunta de investigación planteada. Se encontró que para la seguridad de las bases de datos se aplica usualmente la metodología de control de acceso con diferentes métodos propuestos como sistemas de autenticación y autenticaciones biométricas ya que estos métodos son los que generan un mayor nivel de seguridad.

Palabras clave: seguridad de bases de datos, metodologías de seguridad de bases de datos,protocolos de seguridad

Abstract

Our main focus is to identify the most used methodologies in database security from the review of publications on academic journals in databases from the last six years. An evaluation of the most common databases and security methodologies today was conducted. In order to develop this a systematic review of the IEEE, ARXIV, HINDAWI and DIALNET databases was done. Then, applying the established inclusion and exclusion criteria it resulted in a total of 14 articles showing the protocols and methodologies to answer the research question posed. It was found that for the security of databases the access control methodology is applied a lot with different methods proposed as authentication systems and biometric authentications since these methods are the ones that generate a higher level of security.

Keywords: Database security, database security methodologies, security protocols

[1] Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo 13011, Perú
[2] Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo 13011, Perú

Autor para correspondencia E-mail: 946793000, lmachuca@unitru.edu.pe

https://doi.org/10.24265/campus.2022.v27n33.08

Introducción

Desde el origen de las bases de datos en la década de los 60s, la seguridad de los sistemas ha avanzado significativamente, como por ejemplo, los modelos de control de acceso. Luego, con el nacimiento de Big Data en el año 2000, se desarrollarían herramientas como la minería de datos conservando la privacidad y solucionando en gran parte problemasde ciberseguridad a través de la localización y detención de intrusos y el estudio de malware.

Recientemente, debido a la internet se puede recoger cantidades enormes de datos, debido a esto se debe analizar cómo mitigar los riesgos y amenazas para brindar soluciones a problemas de seguridad (Thuraisingham, 2015). Es importante mencionar que todos los días la gran mayoría de las personas realizan actividades que tienen alguna interacción con diferentes bases de datos como realizar compras en un supermercado o usar los serviciosde un banco. Entonces, una base de datos es una colección de datos que están interrelacionados y que tienen también un significado implícito (Vélez de Guevara, 2021).

La utilización de una metodología para mantener la seguridad en cualquier base de datos es una etapa fundamental que continuar para asegurar la custodia de los datos almacenados y mitigar el mal por ataques malignos evitando la corrupción de dichos. De esta forma se logran detectar amenazas como: la pérdida de la totalidad, la pérdida de disponibilidad, la pérdida de estabilidad y privacidad. que surgen gracias a ocupaciones involuntarias o intencionales llevadas a cabo por los atacantes cibernéticos a fin de provocar un mal del contenido parcial o total y permitiendo la divulgación de la información, poniendo en peligro al organismo afectado (Surya Pratap Singh, 2016).

Para que las vulnerabilidades no perjudiquen nuestra base de datos se exige la identificación anticipada de riesgos y así, de esta manera, actuar de forma preventiva y con mucha responsabilidad (Chuquitarco, 2018).

Existen diversos trabajos de investigación sobre las metodologías de seguridad en bases de datos. Albalawi (2018) estudió una iniciativa de un marco eficaz para esconder información relevante, detectar información sensible y promover la toma de elecciones y de esta forma poder conceptualizar normas. Este marco explora la interacción entre atributos susceptibles en la base de la orientación del atributo que posibilita tomar elecciones sobre los atributos necesarios para producir información sensible.

Además, Jing-wei et al. (2019) en su artículo implementa una nueva forma de mecanismo de escaneo en la base de datos con la habilidad de corregir automáticamente el proceso de descubrimiento y corrección de vulnerabilidades, mejorando la disponibilidad y escalabilidad del código. Guclu et al. (2020) aplicó un nuevo modelo de gestión de accesos para calcular los usuarios que acceden a la base de datos según el rendimiento del modelo aplicado se pudo demostrar que entregó los permisos de accesos correctos y además produjo resultados positivos debido a que era escalable para sistemas distribuidos y además nos

ofrece resultados de autorización más consistentes en comparación con los otros modelos.

Para la seguridad de la base de datos también es necesario tener todos nuestros datos cifrados por lo que Said & Mostafa (2020) proponen un nuevo algoritmo para mejorar la seguridad de nuestra base de datos, se propone un algoritmo para detección de intrusiones de base de datos el cual consiste en la combinación de las teorías del peligro y el algoritmo de selección negativa de los mecanismos del sistema inmunológico artificial. Este algoritmo propuesto es capaz de mejorar la detección de las amenazas internas y también eliminar las violaciones de los datos al proteger la confidencialidad, mantener la disponibilidad y garantizar la integridad.

En este contexto es importante responder a la siguiente pregunta: ¿Cuáles son las metodologías más usadas en seguridad de bases de datos? Por ello, el objetivo principal de esta investigación es lograr identificar las metodologías de seguridad en bases de datos a partir de la revisión de publicaciones sobre las revistas académicas en bases de datos de los últimos seis años para poder mostrar como resultado los trabajos tecnológicos referentes al ámbito de la seguridad de bases de datos.

En este trabajo se llevó a cabo una revisión sistemática con ayuda de toda la literatura científica disponible con el fin de sintetizar información relevante respecto de un tema en particular con la aplicación de la metodología llamada PRISMA. La pregunta de investigación que se estableció para desarrollar el proceso metodológico es ¿Cuáles son las metodologías de seguridad más usadas en bases de datos según los estudios de literatura científica desde el 2016 al 2021?

Existe una gran variedad de bases de datos de publicaciones de artículos científicos. Para esta investigación nos centramos en las bases de datos como la IEEE Xplore, ARXIV, HINDAWI y DIALNET. El período de búsqueda incluye publicaciones de los últimos seis años; del 2016 hasta 2021.

Para la búsqueda se emplearon las palabras claves que tienen relacion con la pregunta de investigación: “Database Security”, “Security technologies”,” “Protocolos”, “methodology”, “techniques”, “tools”. Para ser más específicos en la búsqueda de la literatura científica, se realizaron diversas combinaciones de los términos establecidos y los operadores booleanos como se detalla a continuación:

IEEE Xplore:
(“Database Security” AND “Security technologies” AND (“Protocolos” OR “methodology” OR “techniques” OR “tools”)).

ARXIV, HINDAWI y DIALNET:
“Database Security”

Las investigaciones seleccionadas fueron importadas a un Excel, en el cual se analizó según los siguientes criterios:

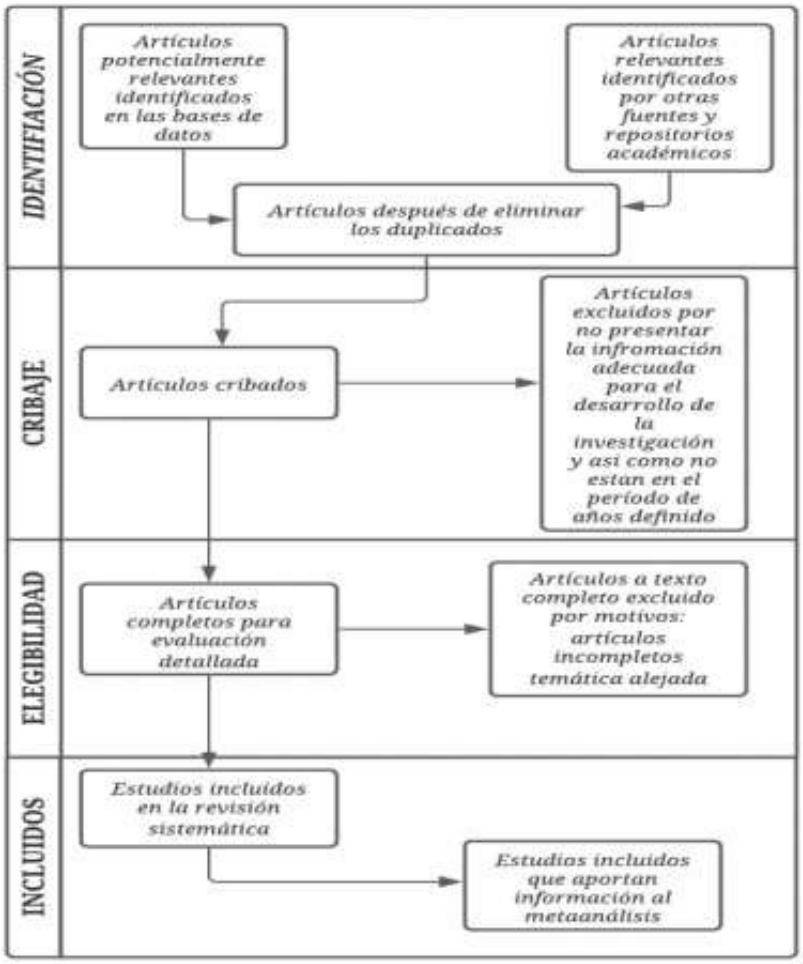
Criterios de inclusión: se incluyeron artículos en inglés y español publicados entre los años 2016 a 2021, donde se evalúan metodologías o estrategias de seguridad de bases de datos. Además, el estudio debe estar publicado en revistas o

conferencias que se encuentran indexados y por último deben ser las versiones de acceso libre en las publicaciones que se encontraron en las bases de datos.

Criterios de exclusión: se definió que los artículos que no estaban en el periodo establecido de los criterios de inclusión serían excluidos debido a que no sería una metodología de seguridad porque es muy antigüo. También se excluyó los estudios que solo se puede observar sus resúmenes ya que estaban incompletos, y por último las investigaciones con una temática alejada a las metodologías de seguridad en base de datos.

La Figura 1 nos muestra los criterios de exclusión e inclusión que se han establecido según la metodología prisma.

Figura 1
Diagrama de flujo-prisma



La búsqueda de investigaciones realizada en las diferentes bases de datos resultó en un total de 29 artículos originales en el periodo de 2016 a 2021, distribuidos de la siguientemanera: IEEE, 20 artículos; ARXIV, cinco artículos, HINDAWI, un artículo y DIALNET, tres artículos. A partir del resultado, no se removió ninguno por duplicidad de datos. Seguidamente, se aplicaron los diferentes criterios para la inclusión y para la exclusión hastalograr obtener un total de 14 artículos finales que se utilizaron para poder presentar los resultados.

De los 14 artículos finales que se seleccionaron se procedió a identificar las metodologías de seguridad en bases de datos como lo muestra la Tabla 1, detallando la metodología enfocado a bases de datos, el tipo de propuestas que muestran como resultado, el año de publicación y sus autores.

Tabla 1
Resúmenes de trabajos previos

Nro.	Autores	Metodología	Resultado
1	(Awadallah R. & Samsudin A., 2021)	Blockchain	Implementación de seguridad
2	(Fuller B. et al., 2017)	Protección criptográfica	Evaluación de la búsqueda
3	(Gernot T. & Lacharme P., 2021)	Autenticaciones biométricas	Implementación de autenticación biométrica paracontrol de acceso a datos
4	(Guclu M. et al., 2020)	Modelo de control de acceso	Modelo de seguridad de datos
5	(Guzmán M. E. et al., 2017)	Control de acceso adatos	Diseño de un middleware
6	(Jiang P. et al., 2017)	Modelo de seguridad	Palabras claves cifradas
7	(Mateen A. et al., 2018)	Control de acceso a datos	Implementación de un control de acceso con un razonamiento de percepción
8	(Samaraweera G. D. & Chang J. M.,2021)	Bases de datos NoSQL	Implementación de un sistema de seguridad
9	(Palos-Sánchez et al., 2017)	Cloud computing	Implementación en empresas
10	(Wang Y. B., 2017)	Principales bases de datos	Un análisis de seguridad
11	(Wang Z. et al., 2021)	Sistema de autenticación	Propuesta de un sistema de autenticación
12	(Yang L., 2016)	Cifrado	Encriptación de datos
13	(Zhao D., 2021)	Cifrado	Método de cifrado homomórfico
14	(Zhao X. et al., 2016)	Seguridad y calidad del servicio	Modelo de evaluación

Para responder la pregunta de investigación, se estableció una serie de metodologías como posibles respuestas, tales como control de acceso, encriptación y modelo de seguridad.

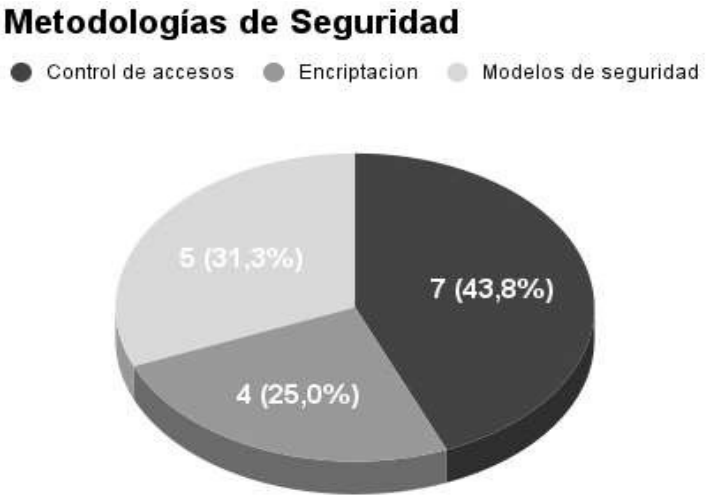
La Tabla 2 muestra los resultados de evaluación para cada artículo que hemos obtenido, como columnas número que se refiere al número de la Tabla 1 y seguidamente las opciones de respuesta respectivas.

Tabla 2
Resultados de evaluación

Nro	Autores	Control de acceso	Encriptación	Modelo de seguridad
1	(Awadallah R. & SamsudinA., 2021)	✔		
2	(Fuller B. et al., 2017)		✔	
3	(Gernot T. & Lacharme P.,2021)	✔		
4	(Guclu M. et al., 2020)	✔		✔
5	(Guzmán M. E. et al., 2017)	✔		
6	(Jiang P. et al., 2017)		✔	✔
7	(Rauf A. et al., 2018)	✔		
8	(Samaraweera G. D. & Chang J. M., 2021)			✔
9	(Sánchez P. R., 2017)			✔
10	(Wang Y.B., 2017)	✔		
11	(Wang Z. et al., 2021)	✔		
12	(Yang L., 2016)		✔	
13	(Zhao D., 2021)		✔	
14	(Zhao X. et al., 2016)			✔

La Figura 2 muestra el número de estudios encontrados según las metodologías de seguridad de bases de datos.

Figura 2
Diagrama de resultados



Como podemos observar en la Figura 2, del total de trabajos extraídos, cinco proporcionan la metodología de modelo de seguridad (4, 6, 8, 9, 14), siete de ellos representan los controles de acceso (1, 3, 4, 5, 7, 10, 11) y finalmente se

consiguió cuatro publicaciones que implementan la encriptación (2, 6, 12, 13).

Después de analizar la pregunta de investigación y cada revista se puede acordar que lasmetodologías más usadas en la seguridad de bases de datos son los controles de acceso.

Discusión

La revisión de la literatura en las revistas académicas nos brinda una variedad de metodologías de seguridad en bases de datos, de las cuales hemos logrado identificar las más usadas. Después de analizar los resultados podemos decir que el número de las metodologías de seguridad en bases de datos es directamente proporcional a la eficiencia de protección y seguridad en base de datos.

Teniendo en cuenta los controles de acceso a datos coincidimos con los autores (Guclu et al., 2020) el cual concluyó que implementando un nuevo sistema de control de acceso se obtiene un mayor nivel de seguridad en el control de acceso a las bases de datos.

Además, sugieren un modelo con el objetivo de calcular automáticamente los permisos y niveles de acceso de todos los usuarios definidos en los sistemas de las bases de datos distribuidas y así de esta forma lleguen a una decisión más eficiente en cuanto a qué objetos pueden acceder los usuarios mientras impiden su acceso a aquella información que no necesitan. Entonces, los modelos de control de acceso son una herramienta importante desarrollada para proteger los sistemas de datos actuales.

Sánchez (2017) obtuvo como resultados que para seguridad de las bases de datos lo que mayor se viene utilizando son los modelos de seguridad.

La presente investigación identificó las metodologías más usadas en seguridad de bases de datos partiendo de la revisión de Publicaciones académicas en las bases de Datos como la IEEE, ARXIV, HINDAWI y DIALNET de los últimos cinco años, en donde se observa que la metodología más usada para la seguridad de bases de datos es control de accesos (Figura 2).

Conclusiones

La presente investigación identificó las metodologías más usadas en seguridad de bases de datos partiendo de la revisión de publicaciones académicas en las bases de datos como la IEEE, ARXIV, HINDAWI y DIALNET de los últimos cinco años.

Se logró exitosamente el objetivo general y así responder a la pregunta de las metodologías de seguridad de bases de datos más comunes que fueron los controles de acceso, modelos de seguridad y encriptación, de las cuales la metodología más usada es el control de acceso, que trata sobre la verificación de si una entidad ya sea un ordenador, una persona u otro objeto que esta solicitando acceso a un determinado recurso tiene los derechos y los permisos necesarios para poder hacerlo.

Por otro lado, se sugiere como recomendación para futuros estudios que se establezcan bien los criterios de inclusión y exclusión con el fin de que se realice una buena obtención de

trabajos dependiendo de los objetivos establecidos, además es indispensable la continua investigación y actualización de las tendencias tecnológicas de seguridad que permiten favorecer la minimización de riesgos con los datos que se almacenan.

Agradecimientos

Este trabajo recibió apoyo de la Universidad Nacional de Trujillo bajo la supervisión del Ing.Alberto Carlos Mendoza de los Santos.

Referencias

Albalawi, U. (2018, del 10 al 13 de diciembre). Countermeasure of Statistical Inference in Database Security [conferencia]. *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, USA. https://doi.org/10.1109/BigData.2018.8622241

Awadallah, R. & Samsudin, A. (2021). Uso de Blockchain en la computación en la nube para mejorar la seguridad de las bases de datos relacionales. *IEEE Access, 19*, 137353-137366. https://doi.org/10.1109/ACCESS.2021.3117733

Chuquitarco, M. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas del Ecuador. *INNOVA Research Journal*, *3*(2.1.), 111-122. https://revistas.uide.edu.ec/index.php/innova/article/view/692

Fuller B., Varia M., Yerukhimovich A., Shen, E., Hamlin, A., Gadepally, V., Shay, R., Darby, J. & Cunningham R. K. (2017, del 22 al 26 de mayo). Búsqueda de base de datos protegida criptográficamente [conferencia]. *2017 IEEE Symposium on Security and Privacy (SP)*. San Jose, USA. https://doi.org/10.1109/SP.2017.10

Gernot, T. & Lacharme, P. (2021). *Biometric Masterkeys*. arXiv. http://arxiv.org/abs/2107.11636

Guclu, M., Bakir, C. & Hakkoymaz, V. (2020). Un nuevo modelo de control de acceso escalable y expandible para sistemas de bases de datos distribuidas en seguridad de datos. *Scientific Programming, 2020*(8875069). https://doi.org/10.1155/2020/8875069

Guzmán, M.E., Torres, J., Murguia, C. & Moreno, L. (2017). Middleware para acceso a bases de datos a través de Web Services basados en el modelo de seguridad. *Gerencia Tecnológica Informática, 16*(44), 17-24. https://dialnet.unirioja.es/servlet/articulo?codigo=7595874

Jiang, P., Mu, Y., Guo, F. & Wen, Q. (2017). Búsqueda privada de palabras clave para sistemas de bases de datos contra ataques internos.

Journal of Computer Science and Technology, 32, 599-617. https://doi.org/10.1007/s11390-017-1745-8

Jing-wei, P., Min, Z., Ping, C. & Wei-guang, X. (2019, del 20 al 22 de diciembre). A Lightweight Vulnerability Scanning and Security Enhanced System For Oracle Database [conferencia]. *IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Chengdu, China. https://doi.org/10.1109/IAEAC47372.2019.8997534

Mateen, A., Rauf, A., Ashraf, M. & Abdullah, A. (2018). Control seguro de acceso a datos con razonamiento de percepción. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 7*(1), 13-28. https://dialnet.unirioja.es/servlet/articulo?codigo=6512705

Said, W. & Mostafa, A. (2020). Hacia un algoritmo inmunológico híbrido basado en la teoría del peligro para la seguridad de las bases de datos. *IEEE Access*, *8*, 145332-145362. https://doi.org/10.1109/ACCESS.2020.3015399

Samaraweera, G.D. & Chang, J.M. (2021). *SEC-NoSQL: Hacia la implementación de seguridad como servicio de alto rendimiento para bases de datos NoSQL*. arXiv. http://arxiv.org/abs/2107.01640

Palos-Sánchez, P. (2017). Estudio organizacional del cloud computing en empresas emprendedoras. *3c Tecnología: glosas de innovación aplicadas a la pyme, 6*(2), 1-16 https://dialnet.unirioja.es/servlet/articulo?codigo=6034897

Shastri, A. & Chatur, P.N. (2015, del 6 al 8 de mayo). Efficient and effective security model for database specially designed to avoid internal threats [conferencia]. *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Avadi, India. https://doi.org/10.1109/ICSTM.2015.7225407

Pratap Singh, S. y Nath Tripathi, U. (2016). preserving database confidentiality using modified user supplied key based encryption. *International journal of engineering sciences & research technology, 5*(12), 274-281. https://doi.org/10.528c1/zenodo.192615

Thuraisingham, B. (2015). Database Security: Past, Present, and Future [Conferencia]. *2015 IEEE International Congress on Big Data,* New York, USA. https://doi.org/10.1109/BigDataCongress.2015.128

Vélez de Guevara L. (2021). *Gestión de Bases de Datos*. https://readthedocs.org/projects/gestionbasesdatos/downloads/pdf/latest/

Wang Y.B. (2017). Estudio sobre la estrategia de gestión de la seguridad de la base de datos de redes de Internet. En X. Tong y W. Liao (Eds.) *Proceedings of the 2016 2nd International Conference*

on Materials Engineering and Information Technology Applications (MEITA 2016) (pp. 456-461). Atlantis Press. https://doi.org/10.2991/meita-16.2017.95

Wang, Z., Zhu, H., Sun, L. & Peng, J. (2021). *SEIGuard: Un esquema engañoso y simplificado de autenticación para proteger la información de ingeniería social del lado del servidor contra ataques de fuerza bruta*. arXiv. http://arxiv.org/abs/2108.06529

Yang, L. (2016). Estudio sobre la tecnología de seguridad de bases de datos en el entorno del comercio electrónico. En L. Zhang y D. Xu (Eds.) *Proceedings of the 2016 6th International Conference on Machinery, Materials, Environment, Biotechnology and Computer* (pp. 248-251). Atlantis Press. https://doi.org/10.2991/mmebc-16.2016.52

Zhao, D. (2021). *INCHE: High-Performance Encoding for Relational Databases through Incrementally Homomorphic Encryption.* arXiv. http://arxiv.org/abs/2111.10458

Zhao, X., Lin, Q., Chen, J., Wang, X., Yu, J. & Ming, Z. (2016). Optimización de la seguridad y la calidad del servicio en un sistema de base de datos en tiempo real utilizando un algoritmo genético multiobjetivo. *Expert Systems with Applications, 64*(1), 11-23. https://doi.org/10.1016/j.eswa.2016.07.023