DOI: https://doi.org/10.46296/ig.v6i11edespjun.0100

ALGORITMOS DE SEGURIDAD PARA APLICACIONES WEB: UN MAPEO SISTEMÁTICO

SECURITY ALGORITHMS FOR WEB APPLICATIONS: A SYSTEMATIC MAPPING

Del Pozo-Durango Rodrigo Humberto [1]; Chariguaman-Asitumbay Henrry Wilfrido [2]; Quicaliquin-Rochina Alex Joel [3]; Orizaga-Trejo José Antonio [4]

[1] Universidad Estatal de Bolívar. Guaranda, Ecuador. Correo: rdelpozo@ueb.edu.ec.

[2] Universidad Estatal de Bolívar. Guaranda, Ecuador. Correo: henry.chariguaman@gmail.com.

[3] Universidad Estatal de Bolívar. Guaranda, Ecuador. Correo: joelalexqr@gmail.com.

[4] Universidad de Guadalajara. Guadalajara, México. Correo: jose.orizaga@academicos.udg.mx.

Resumen

En la actualidad, el número de usuarios en la red ha ido incrementándose de manera progresiva; como consecuencia, las amenazas y vulnerabilidades a las que se enfrentan los sistemas han aumentado considerablemente, poniendo en riesgo la confidencialidad, integridad y disponibilidad de los datos que se manejan. La implementación de algoritmos de protección en el desarrollo de sitios web es crucial para garantizar la seguridad e integridad de la información y hacer frente a las posibles amenazas informáticas. Se utilizará el método deductivo, la observación e investigación exploratoria para el análisis de la información primaria. Como resultado se presenta un mapeo sistemático sobre los algoritmos de seguridad más empleados en aplicaciones web. El impacto de esta investigación podría tener un efecto directo o indirecto para todas las aplicaciones web, que presenten problemas de seguridad.

Palabras clave: algoritmos; confidencialidad; integridad; disponibilidad; seguridad web.

Abstract

At present the number of network users has been progressively increasing; as a consequence, the treats and vulnerabilities faced by the system have also increased considerably. Putting the confidentiality, integrity and availability of the handled data at risk. The implementation of algorithms protection in the development of websites is crucial to guarantee the security and integrity of information and to face possible computer treats. The deductive method, observation and exploratory research will be used for the analysis of primary information. As a result, a systematic mapping of the most used security algorithms in web applications is presented. The impact of this research could have a direct or indirect effect for all web applications, which present security problems.

Keywords: Algorithms, confidentiality, integrity, availability, web security.

Información del manuscrito:
Fecha de recepción: 16 de marzo de 2023.
Fecha de aceptación: 02 de junio de 2023.
Fecha de publicación: 20 de junio de 2023.

1. Introducción

Con el creciente desarrollo de la ciencia y la tecnología, el comercio en línea y las aplicaciones web, se están volviendo cada vez más populares. Las organizaciones confían cada vez más en la información, para mejorar las operaciones comerciales, facilitar la toma de decisiones en la gestión y desplegar estrategias de negocios. En el negocio actual las transacciones que involucran el comercio de bienes y servicios se realizan electrónicamente.

La dependencia organizacional de los SI ha llevado a un aumento de la seguridad de la información. Por lo tanto, la (InfoSecu) es un tema crítico que ha atraído mucho la atención tanto de los investigadores, como de los profesionales de SI.

Los algoritmos de seguridad son una parte integral de la seguridad informática y son utilizados para proteger la información, los sistemas contra intrusiones y accesos no autorizados. Estos algoritmos se utilizan en una amplia gama de aplicaciones, desde transacciones financieras en línea hasta sistemas de control de acceso. En el ámbito de las aplicaciones web, los algoritmos de seguridad son utilizados para proteger los datos de los usuarios, prevenir la explotación de vulnerabilidades y garantizar la privacidad de la información.

Sin embargo, con la gran cantidad de algoritmos de seguridad disponibles, puede resultar difícil seleccionar los más adecuados para una aplicación web específica. Por lo tanto, es necesario realizar un mapeo sistemático de los algoritmos de seguridad para aplicaciones web.

Uno de los más destacados es el algoritmo AES, que resultó ganador del concurso convocado por el NIST (National Institute of Standards and Technology). Este algoritmo ha demostrado ser altamente seguro y confiable, lo que le hace ideal para su uso en aplicaciones que requieren un alto nivel de seguridad de datos. (Avelino, 2021).

Este artículo presenta un mapeo sistemático de los algoritmos de seguridad para aplicaciones web, con el objetivo de identificar los algoritmos más utilizados en la actualidad. Para ello, se realiza una revisión exhaustiva de la literatura científica.

La relevancia de este estudio radica en la necesidad de garantizar la seguridad de las aplicaciones web y la protección de los datos de los usuarios. Con la información presentada, se espera que los desarrolladores de aplicaciones web y expertos en seguridad puedan implementar algoritmos de seguridad efectivos para evitar los ataques cibernéticos y proteger la confidencialidad, integridad y disponibilidad de los datos que se manejan.

2. Metodología

Se empleó la observación e investigación exploratoria para el análisis de la información primaria y recopilación de los datos más relevantes sobre los algoritmos de seguridad. Además, se aplicó el método deductivo para inferir conclusiones específicas a partir de los resultados obtenidos.

La metodología utilizada se divide en las siguientes fases:

Planificación de la revisión

Preguntas de investigación

Definición de las preguntas de investigación:

- ¿Cuáles son los desafíos más comunes que enfrentan las aplicaciones web en términos de seguridad?
- ¿Cuáles son los algoritmos de seguridad más utilizados en aplicaciones web?

Base de datos a utilizar

La búsqueda de la información se realizó en las siguientes bases de datos: Google Académico, Scopus, IEEE Xplore, DOAJ y SciELO.

Criterios de inclusión y exclusión

Criterios de inclusión:

- Los trabajos de investigación deben estar directamente relacionados con la seguridad de aplicaciones web y los algoritmos utilizados para garantizar la protección.
- Los trabajos de investigación deben haber sido publicados entre los años 2018-2023, para asegurar que se aborden los problemas y desafíos de una manera más actualizada.

Criterio de exclusión:

- Estudios y escritos en un idioma diferente al inglés o español.

Definición de la función booleana de la búsqueda

Se empleó el operador booleano AND/OR para combinar los siguientes términos de búsqueda: web security algorithms, web encryption algorithms, web application security y web application algorithms.

Realización de la revisión

Selección de estudios

Para seleccionar los estudios pertinentes que permitan responder a las preguntas planteadas, se aplicaron los criterios de inclusión y exclusión. Como resultado de este proceso, se obtuvieron 77 artículos relevantes para esta investigación.

Tabla 1. *Resultados de búsqueda.*

Motor de búsqueda	Google Académico	Scopus	IEEE Xplore	DOAJ	SciElo
Resultados de Búsqueda	45	14	10	6	2

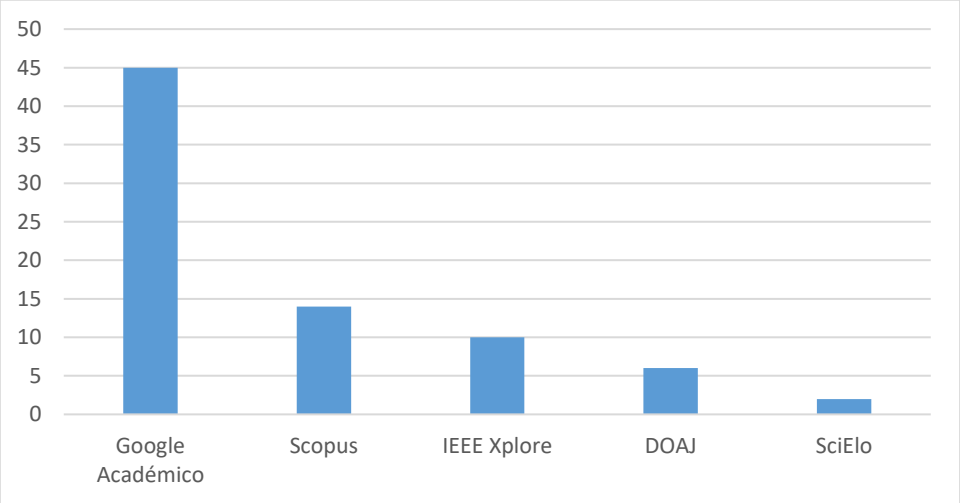
Fuente: *Los Autores (2023).*

3. Resultados

Una vez que se ha llevado a cabo la búsqueda utilizando los criterios de inclusión y exclusión, se han seleccionado un total de 77 artículos.

En la Figura 1 se muestra de manera estadística la distribución de la investigación, que presenta los aportes de cada base de datos de la Tabla 1.

Figura 1. *Distribución de los aportes de las bases de datos utilizadas en la investigación*



Fuente: *Los Autores (2023).*

Al analizar la contribución de cada base de datos, se observó que Google Académico aportó el mayor número de artículos (45), mientras que CsiElo generó la menor cantidad de resultados tras aplicar los criterios de búsqueda (2).

A continuación, se presentan los resultados de las preguntas de investigación que fueron planteadas en la etapa inicial del artículo. Los hallazgos obtenidos en este análisis proporcionan una mejor comprensión de los aspectos clave relacionados con el tema de investigación.

P1. ¿Cuáles son los desafíos más comunes que enfrentan las aplicaciones web en términos de seguridad?

En la tabla 2 se exhiben las amenazas identificadas y su correspondiente frecuencia en los artículos considerados.

Tabla 2. *Amenazas detectadas*

Tipos de amenaza	N° Artículos
Inyección SQL	25
Ataque de fuerza bruta	11
XSS (Cross-Site Scripting)	9
Interceptación de datos	8
Denegación de servicio (DoS)	8
Acceso no autorizado	8
Phishing	2
Ataques cuánticos	2
Ataque de esteganografía	1
Ataque de repetición	1
Suplantación de información	1
Ataque diferencial	1

Fuente: *Los Autores (2023).*

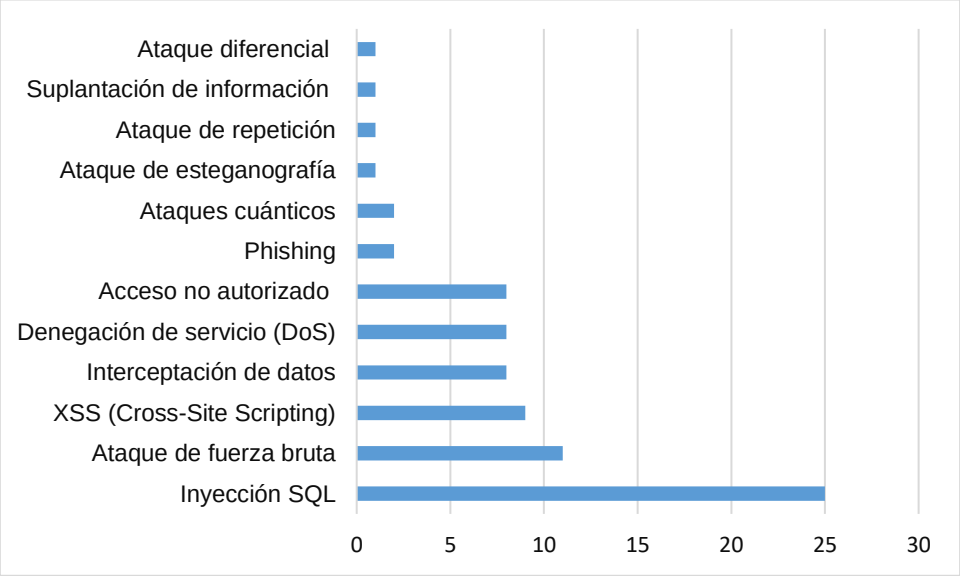
Los artículos publicados en el lapso de los años 2018-2023 exploran la implementación de algoritmos de seguridad con el objetivo de salvaguardar aplicaciones web de potenciales ataques, como la inyección SQL.

La técnica de inyección de SQL consiste en la inserción de código malicioso en campos de entrada de aplicaciones basadas en datos, con el objetivo de ejecutar consultas SQL no autorizadas. Esta técnica es utilizada para atacar

vulnerabilidades de seguridad presentes en el software y explotarlas en su beneficio. (Gitanjali et al., 2020).

En la figura 2 se muestran las amenazas de seguridad más frecuentes en aplicaciones web.

Figura 2. *Tipos de amenazas más frecuentes en aplicaciones web.*



Fuente: *Los Autores (2023)*

P2. ¿Cuáles son los algoritmos de seguridad más utilizados en aplicaciones web?

Se revisaron trabajos que emplean algoritmos de cifrado para proteger aplicaciones web en términos de seguridad. La Tabla 3, ilustra los resultados obtenidos.

Tabla 3. *Resultado de búsqueda de los algoritmos más utilizados*

Algoritmos	AES	RSA	SHA-256	MD5	Blowfish	DES	Bcrypt	LSTM	Otros
Resultado de Búsqueda	26	15	7	6	3	2	2	2	14

Fuente: *Los Autores (2023).*

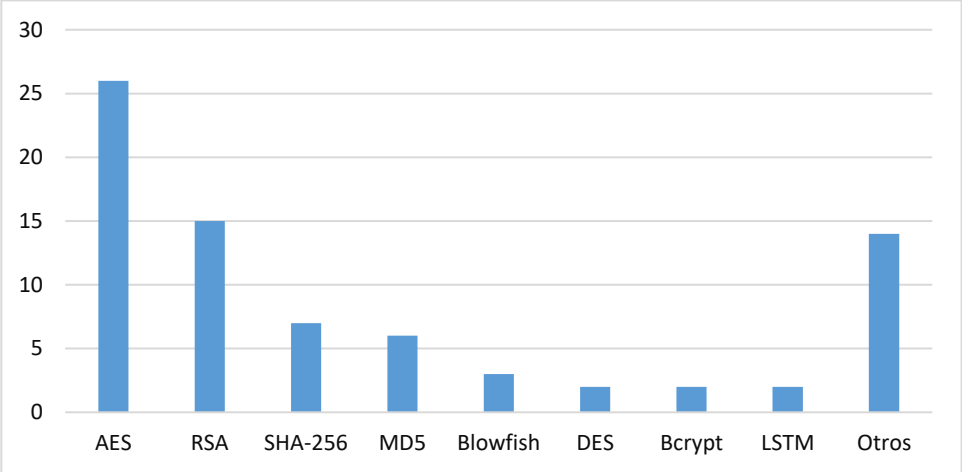
Esta tabla resume los hallazgos de la investigación y permite visualizar de manera clara y concisa los algoritmos de cifrado utilizados con mayor frecuencia.

El algoritmo de cifrado es el proceso de codificar datos para que no se puedan leer realizando varias sustituciones y transformaciones en el texto sin formato (mensaje

original) y convirtiéndolos en texto cifrado (mensajes aleatorios). Los algoritmos de cifrado se clasifican en dos categorías generales: cifrado de clave simétrica y cifrado de clave asimétrica (Pittalia, 2019).

En la figura 3 se muestran los algoritmos de seguridad más empleados en aplicaciones web.

Figura 3. *Algoritmos de seguridad más utilizados*



Fuente: *Los Autores (2023).*

El algoritmo Advanced Encryption Standard (AES) figura como el más empleado en 26 de los 77 artículos revisados. No obstante, es fundamental considerar que la selección de un algoritmo de seguridad dependerá del contexto específico de la aplicación y de las necesidades de seguridad de cada organización.

4. Conclusiones

El mapeo sistemático presentado en el artículo proporciona una vista general útil de los algoritmos de seguridad más comunes, donde se destaca que el algoritmo AES ha sido más ampliamente empleado en años recientes para garantizar la seguridad de la información en sitios web. Sin embargo, al realizar combinaciones entre ellos se obtiene una mayor protección ante las distintas amenazas que pudieran presentarse

Es importante destacar que la inyección de SQL representa una amenaza significativa para la seguridad de las aplicaciones web y puede causar daños considerables,

como la pérdida o el robo de información sensible. Por lo tanto, es esencial implementar medidas de seguridad adecuadas para prevenir la explotación de esta técnica y garantizar la protección de la información.

El presente estudio contribuye a la mejora de la seguridad, proporcionando información valiosa para los desarrolladores de aplicaciones web y profesionales de seguridad informática. Se espera que estos resultados sirvan como guía para la selección y aplicación de algoritmos adecuados en la protección contra diferentes tipos de amenazas, y que puedan ser considerados en futuras investigaciones en el ámbito de la seguridad informática.

Bibliografía

Abhishek, G., & Asha, A. (2020). Development of “RSA” Encryption Algorithm for Secure Data Transmission. Research Journal of Computer and Information Technology Sciences, 8(1), 9-12, e-ISSN: 2320-6527. https://doi.org/http://www.isca.me/COM_IT_SCI/Archive/v8/i1/2.ISCA-RJCITS-2019-009.pdf

Abood, O., & Guirguis, S. (2018). A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications, 8(7), 495-516, e-ISSN: 2250-3153. https://doi.org/http://dx.doi.org/10.29322/IJSRP.8.7.2018.p7978

Ajitha, P. (2021). Responsive Design in Web Development with Security Using Optimization Algorithms. International Journal of Research in Engineering and Science, 9(1), 16-22, e-ISSN: 2320-9364. https://doi.org/https://www.ijres.org/papers/Volume-9/Issue-1/2/C0901021622.pdf

Avelino, M. (2021). Buenos algoritmos con malas implementaciones. Revista Española de Ciberseguridad, Privacidad y Digitalización, 19-24. https://doi.org/http://www.recsi2020.udl.cat/static/site/files/Avelino-XVI-RECSI.pdf

Chavan, S., & Tamane, S. (2020). Enhancement in Cloud Security for Web Application Attacks. IEEE, 91-95. https://doi.org/10.1109/ICSIDEMPC49020.2020.9299629

Chen, C., Zhong, J., & Chen, W. (2021). Machine Learning-based web security intrusion detection system. IEEE, 173-177. https://doi.org/10.1109/IAECST54258.2021.9695557

Gitanjali, A., Kadlag, & Dhotre, P. S. (2020). Detection and prevention of data modification attack based on MD5 algorithm. International Journal of Current Engineering and Technology, 7(8), 1005-1008, e-ISSN: 2277-4106. https://doi.org/https://inpressco.com/wp-content/uploads/2021/02/Paper2101005-1008.pdf

Gondaliya, J., Savani , S., Dhaduvai, V. S., & Hossain, G. (2018). Hybrid Security RSA Algorithm in Application of Web Service. IEEE, 149-152. https://doi.org/10.1109/ICDIS.2018.00032

Naidu, S., Krishna, R., & Kumari, G. (2019). A Trusted New Method for Authentication and Security for Web Applications in Cloud Using RSA Algorithm. International Journal of Emerging Technologies and Innovative Research, 6(4), 1-8, e-ISSN: 2349-5162. https://doi.org/https://ssrn.com/abstract=3708131

Pittalia, P. (2019). A Comparative Study of Hash Algorithms in Cryptography. International Journal of Computer Science and Mobile Computing, 8(6), 147-152, e-ISSN: 2320-088X. https://doi.org/https://ijcsmc.com/docs/papers/June2019/V8I6201928.pdf

Sa’idu , S., Taneja, P., & Kalta, S. (2022). A Comparative Analysis of Cryptographic Algorithms: AES & RSA and Hybrid Algorithmfor Encryption and Decryption. International Journal of Innovative Science and Research Technology, 7, 1725-1732, e-ISSN: 2456-2165. https://doi.org/https://ijisrt.com/assets/upload/files/IJISRT22AUG773.pdf

Sholikhatin, S., Kuncoro, A., Munawaroh, A., & Gilang , S. (2022). Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security. Edu Komputika Journal, 9(1), 60-67, e-ISSN: 2252-6811. https://doi.org/https://doi.org/10.15294/edukomputika.v9i1.57389

Simarmata, J., Limbong, T., Misalina , G., Damanik, R., Padli Nasution, M. I., Halim Hasugian, A., . . . Sinambela, M. (2018). Implementation of AES Algorithm for Information Security of Web-Based Application. International Journal of Engineering & Technology, 7(4), 318-320. https://doi.org/https://doi.org/10.14419/ijet.v7i3.4.20124

Singh, P., Tripathi, V., Gangodkar, D., & Bordolo, D. (2021). A DES, AES, DSS, and RSA-Based Security System for Protecting Sensitive

Information During Communication and Providing Fast, Reliable File Identification. Webology, 18(5), 3218-3227, e-ISSN: 1735-188X. https://doi.org/https://www.webology.org/data-cms/articles/20221014114355amPaper%2057.pdf

Turnip, T. N., Aruan, H., Siagian, A. L., & Siagian, L. (2022). Web Browser Extension Development of Structured Query Language Injection Vulnerability Detection Using Long Short-Term Memory Algorithm. IEEE, 1-5. doi: https://doi.org/10.1109/ICOSNIKOM56551.2022.10034905