UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

“Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático”

AUTOR:

Cynthia Janeth Guaigua Bucheli

TUTOR:

Msg. Joe Llerena

Abril 2021

GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **Cynthia Janeth Guaigua Bucheli**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Firma del autor

Nombre: Cynthia Janeth Guaigua Bucheli

Firma del tutor

Nombre:

Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático

Cynthia Guaigua Bucheli [1][10000-0002-6571-4747] and Joe Llerena-Izquierdo [1][0000-0001-9907-7048]

[1] Universidad Politécnica Salesiana, Guayaquil, Ecuador
cguaigua@est.ups.edu.ec, jllerena@ups.edu.ec

Abstract. La nube es un concepto muy poderoso que está bajo ataque por el volumen de datos almacenados y servicios importantes para los consumidores. Tiene muchas ventajas para la tecnología una de ella es la capacidad para transmitir grandes cantidades de datos donde debe existir una gran seguridad. Se analizaron varios artículos para realizar una amplia búsqueda. El objetivo principal es analizar los algoritmos empleados en artículos relacionados para mitigar los riesgos de los datos en la nube. Esta investigación pretende utilizar la metodología teórica para obtener resultados. Para la realización de este articulo académico se realizara un mapeo sistemático que nos permitirá recopilar la información necesaria para realizar los resultados de una manera ordena respondiendo a las preguntas de investigación. Los resultados obtenidos con los artículos seleccionados nos dan un enfoque a la seguridad en la nube con el fin de mitigar los riesgos con los métodos y algoritmos propuestos en la búsqueda.

The cloud is a very powerful concept that is under attack by the volume of data stored and services important to consumers. It has many advantages for the technology one of it is the ability to transmit large amounts of data where there should be great security. Several articles were analyzed for a broad search. The main objective is to analyze the algorithms used in related articles to mitigate the risks of data in the cloud. This research aims to use theoretical methodology to obtain results. For the realization of this academic article a systematic mapping will be carried out that will allow us to gather the information necessary to realize the results in an orderly way answering the research questions. The results obtained with the selected articles give us a focus on cloud security in order to mitigate risks with the methods and algorithms proposed in the search.

Keywords: Security algorithms, Cloud security, Data storage, systematic mapping.

1 Introducción

1.1 Seguridad de la información en la nube

La nube se ha convertido en una tecnología vital pero los ataques son cada vez más frecuentes, por el crecimiento exponencial del volumen de datos en la red y la gravedad que estos pueden provocar a diferentes entornos. Ya son 20 años desde que se realizó el primer ataque DDoS y actualmente se lo considera una amenaza grave debido a que sobrecargan los sistema [1].

La naturaleza de estos ataques puede requerir técnicas logarítmicas avanzadas, gran parte de estos logaritmos estudian el comportamiento de los usuarios logrando separar los usuarios legítimos de los atacantes. En el caso de existir un sistema vulnerable internamente se comunica con otros sistemas comprometidos para lograr su objetivo sobre servicios afectados [2].

Dentro del estudió de la mitigación para proteger la nube muchos usuarios deben necesitar recursos adicionales que estén asociados a la fuerza de ataque y enfrentarse a perdidas colaterales, siendo el principal efecto las pérdidas económicas por la interrupción del servicio. Empleando protocolos DNS, SNMP o NTP para una mayor fuerza de ataque [3].

1.2 Riesgos asociados a la nube

A medida que la nube crece también incrementa la cantidad de riesgos que se puede presentar, un empleado malicioso que internamente puede afectar la confidencialidad, integridad y disponibilidad de la información de distintos usuarios. La arquitectura y funciones de la nube pueden fallar por parte del proveedor teniendo el acceso a los datos desde otra aplicación ocasionado una perdida [4].

La nube al tener una arquitectura distribuida se produce un mayor tráfico de datos y si existe una falta de confiabilidad por parte de proveedor la información confidencial se serán atacados [5]. Teniendo en cuenta que el usuario también puede ser un riesgos al compartir o perder claves privadas que pongan en peligro sus propios datos y servicios que no le permitan interactuar en la nube.

Este artículo identifica los diversos ataques en la nube lo cuáles van a ser tratados y nos centramos en un análisis de los algoritmos que mitigan los riesgos de los datos para esto es necesario realizar una amplia búsqueda.

2 Metodología

El método teórico con enfoque cuantitativo nos permitirá analizar los datos obtenidos para mitigarlos riesgos de datos en la nube. Posteriormente se realiza una comparación entre los algoritmos mencionados en esta investigación.

Mediante el siguiente estudio se procura identificar los algoritmos que protegen la información con integridad, confidencialidad y disponibilidad garantizando la seguridad de los sistemas sobre los diferentes tipos de ataques.

Los diferentes algoritmos propuestos tienen que ser capaces de prevenir, detectar y mitigar cada ataque realizado a un usuario determinado ya que estos no solo pueden ser externo sino desde el interior de la nube teniendo acceso a los servicios. Según [6] varias empresas eliminan estratégicamente otros sitios web, los gobiernos para eliminar la infraestructura de un país provocando que el ataque sea más corto con un volumen grande de datos. Las clasificaciones de riesgos de acuerdo con la norma ISO/IEC 27001 refleja las probabilidades de los ataques.

- Insignificante.
- Bajo.
- Moderado.
- Alto.
- Catastrófico.

De acuerdo con las investigaciones realizadas podemos nombrar algunos de los riesgos en la nube mencionados en la búsqueda agregándole su respectiva clasificación.

Tabla 1. Riesgos en la nube

Probabilidad	Clasificación
Perdida de datos	Catastrófico
Suplantación de dirección IP	Alto
Fallos de entidades (servidores, base de datos)	Alto
Fallo de la red	Catastrófico
Perdida de las claves	Moderado
Conflicto con el inicio de sesión	Bajo
Ataque de inyección de malware en la nube	Alto
Manipulación de los datos	Catastrófico
Fuga de información	Catastrófico
Ataques DDoS	Alto
Man in Middle Attack	Alto

Con la clasificación de los riesgos entre alto y catastrófico mayor es el daño a los servicios y un peligro para los datos, por lo que es necesario la utilización de algoritmos para proteger los datos y mitigar los riesgos.

Se opto por un mapeo sistemático que nos permitirá analizar e identificar los principales problemas del tema a investigar.

En este proceso podemos recopilar información y estructura de un tema específico categorizando los resultados de manera ordenada, precisa y concisa de temas que han

sido publicados hasta el momento de una área específica [7], [8] y [9]. En la Fig 1 encontramos las fases del mapeo sistemático a seguir en el artículo:

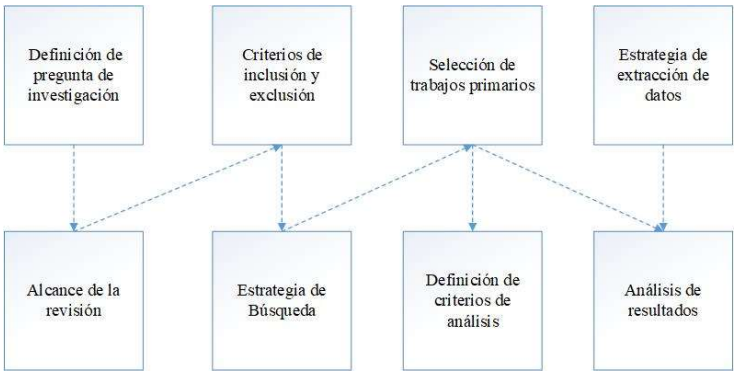

Fig. 1. Fases del mapeo sistemático.

Pregunta de investigación

Las preguntas de investigación planteadas en este articulo buscan encontrar los algoritmos para mitigar los diferentes ataques en la nube.

En la Tabla 2 podemos encontrar cada una de las preguntas y su motivación, mediante el cual se pudo seleccionar, analizar y definir cada información encontrada en esta área de estudio.

Tabla 2. Preguntas de investigación para un mapeo sistemático

Preguntas	Motivación
Q1. ¿Cuáles son los algoritmos enfocados a mitigar los riesgos que ocurren en la nube?	Determinar el número de algoritmos propuestos por las publicaciones seleccionadas.
Q2. ¿Qué evidencia empírica existe sobre los artículos seleccionados?	Determinar que método empírico se ha utilizado para proponer la mitigación de datos.

Alcance de revisión

Actualmente existen varias bases de datos y publicaciones relacionadas donde podemos enfocar nuestra investigación en la seguridad y protección de la información realizando una búsqueda por medio de algoritmos propuestos por varios autores y analizando el área de la seguridad informática.

Cada proceso se realizara a lo investigado sobre el tema propuesto y en los artículos encontrados en bases de datos como: IEEE, Scopus, Springer & Google scholar.

Teniendo en cuenta que lo artículos estudiados se comprende entre publicaciones desde el 2015 hasta el 2020.

Criterios de inclusión

En esta investigación, para la selección de los estudios se consideró los siguientes criterios de inclusión:

- Se analizo todos los artículos relacionados para la inclusión de los estudios que tengan relación con la búsqueda del área de seguridad informática y donde varios autores propusieran, evaluaran o discutieran sobre la metodología propuesta de manera ágil y precisa.
- Se incluyeron estudios cualitativos, investigativos, exploratorios y deductivos.
- También se decidió incluir a la investigación artículos en inglés y español.

Criterios de exclusión

Para este estudio se consideró los siguientes criterios:

- Se excluyeron artículos sin diseños de publicación, solo basado en opiniones.
- Publicaciones que no estaban en inglés o español.
- La versión completa de la investigación no estaba disponible con la suscripción de la institución.

Estrategia de búsqueda

En la búsqueda de los estudios primarios nos basamos en la siguiente clasificación de los filtros:

- Primer filtro: Relación con el tema propuesto.
- Segundo filtro: Lectura del resumen o abstract.
- Tercer filtro: Análisis completo del contenido de cada trabajo.

De esta manera logramos definir los artículos relacionados para realizar la búsqueda de la información.

Selección de estudios primarios

Se utilizaron los criterios de inclusión y exclusión para tener como resultado artículos relevantes para esta investigación y poder responder a las preguntas planteadas. Una vez obtenido los resultados de la búsqueda se aplicó los criterios de exclusión e inclusión, para los trabajos preseleccionado se comparó los resultados para verificar si fueron aplicados los criterios con rigurosidad. Si algún resultado generaba una duda se decidió volver a leer el abstract y la conclusión con la finalidad de mantenerlo en la investigación. De esta manera se obtuvo un total de 18 resultados de búsqueda.

Tabla 3. Resultados de la búsqueda

Motor de búsqueda	IEEE	Scopus	Springer	Google scholar
Resultados de búsqueda	50	38	40	14
Trabajos preseleccionados	20	15	10	8

Trabajos seleccionados	12	3	2	3

Estrategia de extracción de datos

Cada pregunta de investigación tiene una serie de respuestas como se puede observar en la tabla 4, nos permitirá aplicar los criterios de estrategia de búsqueda para clasificar dichas respuestas.

Tabla 4. Esquema de clasificación

Preguntas	Respuestas
Q1. ¿Cuáles son los algoritmos enfocados a mitigar los riesgos que ocurren en la nube?	1. AES 5. Blowfish 2. RSA 6. SHA-512 3. Firefly 7. Merkle 4. HBE
Q2. ¿Qué evidencia empírica existe sobre los artículos seleccionados?	a. Mapeo sistemático b. Propuesta c. Otros

3 Resultados

Una vez finalizada la búsqueda aplicando los criterios de inclusión y exclusión con un total de 18 artículos seleccionados se puede realizar la distribución de la investigación observados en la Fig 2 que se representa estadísticamente los aportes de cada base de datos de la Tabla 3.

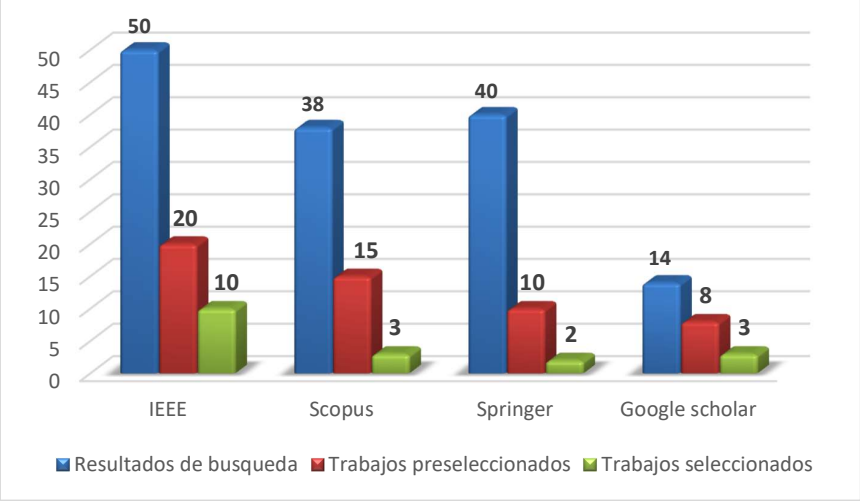

Fig. 2. Distribución de los aportes de la bases de datos en la investigación

Podemos analizar que la base de datos IEEE fue la que más contribuyó a la investigación con un total de 10 articulo primarios y la que genero menos resultados después de aplicar los criterios de búsqueda fue springer con un total de 2 artículos seleccionados.
A continuación, se presenta los resultados de la preguntas de investigación planteadas al principio de la investigación en la tabla 4 de la sección estrategia de extracción de datos.

Q1. ¿Cuáles son los algoritmos enfocados a mitigar los riesgos que ocurren en la nube?

En el estudio después de aplicar los criterios y la estrategia de búsqueda se puede observar en la Tabla 5 donde se menciona cada algoritmo propuesto de los autores relacionados con esta investigación. Cada método está enfocado a diferentes tipos de amenazas donde podemos realizar una comparación entre cada uno de ellos.

Tabla 5. Tabla comparativa de algoritmos propuestos.

Referencias	Métodos	Algoritmos propuestos	Tipos de amenazas
[10]	M1: LDAP authentication se utiliza para la identificación de un usuario válido.	Algoritmos SHA-512 y AES.	Dirección de IPs falsas por medio de un host de confianza durante la identificación.
[11]	M2: Criptografía hibrida sigue el proceso de encriptación y desencriptación.	Utiliza algoritmos Blowfish y RSA.	-Ataque MITM -Repetir ataques -Dependencia de hash
[12]	M3: Multi-cloud almacena los datos en nubes compartidas solucionando el problema de la disponibilidad.	Algoritmo 1.	-Hijacking -Phishing -Ataque de inyección SQL -Corrupción de datos -Ataque de Sybil
[13]	M4: Realiza un proceso de generación de clave, cifrado y descifrado.	Algoritmo RSA	-Ataque matemático -Ataque de tiempo -Ataque de fuerza bruta
[13]	M5: Resuelve el problema de autenticación.	Algoritmos firefly y el hash merkle.	-Ataque MITM -Hijacking -Ataque de fuerza bruta -Ataque DDoS -Ataque de inyección de malware
[15]	M6: Encripta los archivos y los almacena.	Algoritmo AES.	-Ataque DDoS -Phishing -Hijacking
[16]	M6: Sistema SAML proporciona un alto nivel de seguridad para la gestión de identidad del usuario.	Algoritmo HBE.	-Ataque de Sybil -Ataque DDoS

En los métodos tenemos una breve explicación del proceso de cada uno. Las diferentes propuestas de los autores nos proponen algoritmos para mitigar los ataques a la nube mediante la autenticación, autorización y la revisión de cuentas. En el caso de la nube, se vuelve más segura para la transmisión de datos.

Q2. ¿Qué evidencia empírica existe sobre los artículos seleccionados?

En relación con la evidencia empírica es importante destacar que los resultados que se exponen en la Fig 3 en la parte de otros tenemos que se encuentran artículos de reseñas o revisión de un área específica ([1], [2], [5], [17] y [18]).

En esta investigación se encontraron 3 artículos que son mapeo sistemático [7], [8] y [9] que se relacionó a cada fase.

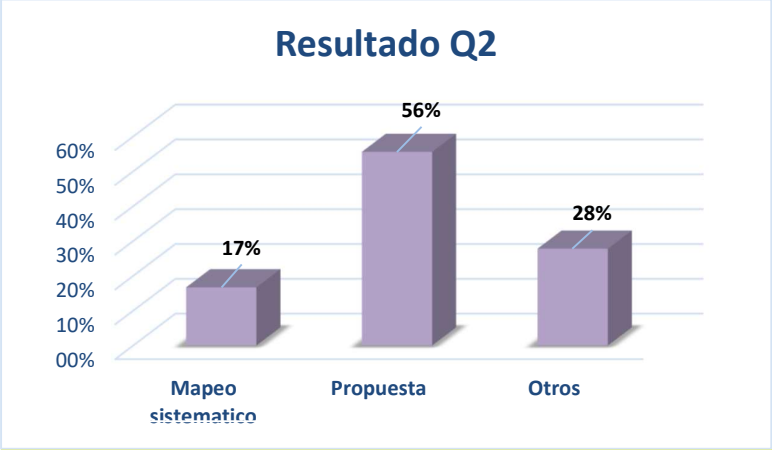

Fig. 3. Resultados gráfico de la pregunta de investigación Q2.

4 Discusión

A continuación, tras analizar los resultados obtenidos respondiendo a las preguntas de investigación, se puede afirmar:

- Los autores proponen algoritmos para mitigar los datos en la nube pero deben tener la necesidad de validar sus propuesta para que las organizaciones los consideren completos y aplicables, por medio de casos de estudios o encuestas.
- Debemos de considerar que entre el periodo seleccionado del 2015 al 2020 en este estudio es notorio la falta de artículos que propongan nuevos métodos para mitigar los datos considerando el incremento continuo de la nube.

5 Conclusiones

Los resultados están vinculados a otras investigaciones donde se identificó los diferentes tipos de ataques analizando cada método propuesto para proteger la información.

La información recopilada de este mapeo sistemático muestra la importancia de seguir implementando algoritmos y la necesidad de seguir investigando esta área en investigaciones futuras.

Es importante destacar que ateniendo una selección correcta se analizó los algoritmos realizando una comparación entre ellos y ver los procesos que cada autor proponer y los estudios realizados para llegar a los resultados.

Referencias

1. Vlajic, N., Zhou, D.: IoT as a Land of Opportunity for DDoS Hackers. Computer (Long. Beach. Calif). 51, 26–34 (2018). https://doi.org/10.1109/MC.2018.3011046.
2. Paffenroth, R.C., Zhou, C.: Modern Machine Learning for Cyber-Defense and Distributed Denial-of-Service Attacks. IEEE Eng. Manag. Rev. 47, 80–85 (2019). https://doi.org/10.1109/EMR.2019.2950183.
3. Somani, G., Gaur, M.S., Sanghi, D., Conti, M., Rajarajan, M., Buyya, R.: Combating DDoS attacks in the cloud: Requirements, trends, and future directions. IEEE Cloud Comput. 4, 22–32 (2017). https://doi.org/10.1109/MCC.2017.14.
4. Abd, S.K., Salih, R.T., Al-Haddad, S.A.R., Hashim, F., Abdullah, A.B.H., Yussof, S.: Cloud computing security risks with authorization access for secure Multi-Tenancy based on AAAS protocol. IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON. 2016-Janua, 1–5 (2016). https://doi.org/10.1109/TENCON.2015.7373063.
5. A. Stavrou, D.F. and C.K.: On the Move: Evading Distributed Denial-of-Service Attacks. Comput. 49, 104–107 (2016).
6. Ipd-, S.D.R.D.C., Mar, S.: Deteccion de ataques de Denegacion de Servicios en la Nube.
7. Cravero, A., Sepúlveda, S., Muñoz, L.: Big Data Architectures for the Climate Change Analysis : A Systematic Mapping Study. (2020).
8. Solis, A., Hurtado, J.: Reutilización de software en la robótica industrial: un mapeo sistemático. Rev. Iberoam. Automática e Informática Ind. 17, 354 (2020). https://doi.org/10.4995/riai.2020.13335.
9. Carrizo, D., Rojas, J.: Metodologías, técnicas y herramientas en ingeniería de requisitos: un mapeo sistemático. Ingeniare. Rev. Chil. Ing. 26, 473–485 (2018). https://doi.org/10.4067/s0718-33052018000300473.
10. Raipurkar, K. V., Deorankar, A. V.: Improve data security in cloud environment by using LDAP and two way encryption algorithm. 2016 Symp. Colossal Data Anal. Networking, CDAN 2016. 1–4 (2016). https://doi.org/10.1109/CDAN.2016.7570934.
11. Timothy, D.P., Santra, A.K.: A hybrid cryptography algorithm for cloud computing security. 2017 Int. Conf. Microelectron. Devices, Circuits Syst.

ICMDCS 2017. 2017-Janua, 1–5 (2017). https://doi.org/10.1109/ICMDCS.2017.8211728.

12. Razaque, A., Nadimpalli, S.S.V., Vommina, S., Atukuri, D.K., Reddy, D.N., Anne, P., Vegi, D., Malllapu, V.S.: Secure data sharing in multi-clouds. Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016. 1909–1913 (2016). https://doi.org/10.1109/ICEEOT.2016.7755020.
13. Bhandari, A., Gupta, A., Das, D.: Secure algorithm for cloud computing and its applications. Proc. 2016 6th Int. Conf. - Cloud Syst. Big Data Eng. Conflu. 2016. 188–192 (2016). https://doi.org/10.1109/CONFLUENCE.2016.7508111.
14. A. K. Bhardwaj, R.M. and S.: TTP based vivid protocol design for authentication and security for cloud. 2016 3rd Int. Conf. Comput. Sustain. Glob. Dev. (INDIACom), New Delhi. 3275–3278 (2016).
15. Nivedhaa, R., Justus, J.J.: A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption. Proc. 2018 IEEE Int. Conf. Commun. Signal Process. ICCSP 2018. 755–759 (2018). https://doi.org/10.1109/ICCSP.2018.8524257.
16. George, J.A., Veni, S., Soomroo, S.: Improving privacy and trust in federated identity using SAML with hash based encryption algorithm. 4th IEEE Int. Conf. Eng. Technol. Appl. Sci. ICETAS 2017. 2018-Janua, 1–5 (2018). https://doi.org/10.1109/ICETAS.2017.8277840.
17. Juliadotter, N.V., Choo, K.K.R.: Cloud attack and risk assessment taxonomy. IEEE Cloud Comput. 2, 14–20 (2015). https://doi.org/10.1109/MCC.2015.2.
18. Zand, A., Modelo-Howard, G., Tongaonkar, A., Lee, S.J., Kruegel, C., Vigna, G.: Demystifying DDoS as a service. IEEE Commun. Mag. 55, 14–21 (2017). https://doi.org/10.1109/MCOM.2017.1600980.