UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

"ESTRATEGIAS ALGORÍTMICAS ORIENTADAS A LA CIBERSEGURIDAD: UN MAPEO SISTEMÁTICO"

AUTOR:

CHRISTIAN ANDRÉS OROZCO BONILLA

TUTOR:

Msg. JOE LLERENA

JUNIO 2021

GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **Christian Andrés Orozco Bonilla,** declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor /es.

Orozco Bonilla Christian Andrés
C.I: 0940841265

Mag. Llerena Izquierdo Joe Frand

ESTRATEGIAS ALGORÍTMICAS ORIENTADAS A LA CIBERSEGURIDAD: UN MAPEO SISTEMÁTICO

Christian Orozco Bonilla [1][0000-0002-4538-9131] and Joe Llerena-Izquierdo[1][0000-0001-9907-7048]

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

Abstract. Existen diferentes estrategias para proteger la información que está en un ambiente cibernético, en este documento se revisaron y presentaron algunas alternativas de seguridad. El problema es la clasificación de información obtenida desde bibliotecas primarias para realizar un análisis de estrategias algorítmicas orientadas a la ciberseguridad mediante un mapeo sistemático. El objetivo es definir estrategias algorítmicas de seguridad orientados a la ciberseguridad para la protección de la información en las organizaciones mediante un mapeo sistemático en los últimos cinco años. Se utiliza la metodología de mapeo sistemático, que nos sirve para clasificaciones y obtener datos sobre el conocimiento de algoritmos de seguridad y ciberseguridad; se analizan los artículos científicos en categorías, tipos, frecuencias, y áreas de aplicación. En esta investigación resultó un Análisis de trabajos de investigación previos para la clasificación de estrategias de seguridad mediante el uso de algoritmos, revisión de técnicas de seguridad adecuadas para la protección de la información en las organizaciones con el soporte de modelos computacionales, y Metodologías utilizadas en ciberseguridad que evidencien un mejor nivel de protección de la información. Se concluyó que la ciberseguridad utiliza algoritmos de criptografía como una herramienta y buena opción para protección de un ambiente cibernético y se aplica a cualquier tipo de dato; entre 40 referencias clasificadas que aplican ciberseguridad, el 44% está en la categoría disponibilidad; el 40% está en arquitecturas distribuidas; el 80% está en áreas generales; el 32% utiliza el algoritmo AES en ciberseguridad; el 40% de las referencias se basan en modelos para aumentar el nivel de protección de la información.

Keywords: Security Algorithm, Algorithmic strategy, Cybersecurity, Distributed systems, Cryptographic Algorithms, Systematic mapping

1 Introducción

Para proteger información se utilizan algoritmos que brindan más seguridad a través de la criptografía [1]; estos algoritmos cifran la información, es decir pasar un dato legible a un formato ilegible llamado datos cifrados; para pasarlo a legible se realiza el descifrado; con esto se aumenta la seguridad y se mantiene la confidencialidad, integridad y disponibilidad (CIA); existen dos clases de algoritmos para brindar seguridad son simétricos y asimétricos; los algoritmos simétricos son DES, 3DES, AES, Blowfish, Digital Signature Algorithm; los algoritmos asimétricos son curva elíptica, Elliptic Curve, Diffie-Hellman y RSA.

La seguridad es importante para cualquier tipo de información o tipo de archivo; se afirma que los algoritmos de cifrado o encriptación son primordiales para la seguridad; un objetivo de la seguridad es mantener la confidencialidad de la información entre los usuarios, evitar la copia ilegal o ataques a los activos de información [2]. Algunas áreas que utilizan algoritmos de encriptación son militar, comunicaciones, médicas y conferencia; además se utiliza en almacenamiento y transmisión de información [3]. Hoy en día la comunicación nos conecta; en el intercambio de información existen riesgos y amenazas de ataques o visualización, por ello es necesario la protección de la información; una forma de protección es convertirla en ilegible; aquí la criptografía se aplica por seguridad; además la técnica para convertir un mensaje en formato ilegible es cifrado; la técnica para convertir un texto cifrado en formato legible es descifrado [4].

La ciberseguridad es un conjunto de herramientas, conceptos/medidas de seguridad, políticas, enfoques de gestión de riesgos, actividades, aprendizaje, mejores prácticas, aumento de garantía y tecnologías que se utilizan para proteger el ambiente cibernéticos de una organización; la ciberseguridad tiene más componentes de protección y control interno del ciberespacio; con respecto a la seguridad de la información ambas tienen un alcance diferente, son complementarias y alto nivel de importancia [5].

El problema es la clasificación de información obtenida desde bibliotecas primarias para realizar un análisis de estrategias algorítmicas orientadas a la ciberseguridad mediante un mapeo sistemático.

¿Por qué es necesario un análisis de estrategias algorítmicas orientadas a la ciberseguridad mediante un mapeo sistemático?

Para conocer la situación de los algoritmos de seguridad y ciberseguridad; entender el alcance de esta clase de algoritmo, obtener y conocer datos de investigaciones primarias, ver evidencias sobre este tema en un tiempo determinado.

El objetivo es definir estrategias algorítmicas de seguridad orientados a la ciberseguridad para la protección de la información en las organizaciones mediante un mapeo sistemático en los últimos cinco años.

Se utiliza la metodología de mapeo sistemático [6], que nos sirve para clasificaciones y obtener datos sobre el conocimiento de algoritmos de seguridad y ciberseguridad; se analizan los artículos científicos en categorías, tipos, frecuencias, áreas de aplicación.

2 Materiales and Métodos

2.1 Materiales

Los siguientes son artículos relacionados a algoritmos de seguridad:

En [2] proponen un algoritmo de encriptación para los datos subidos a la nube; los datos texto se convierten en ASCII y luego a binarios; para esto utilizan un numero primo de acuerdo a los bits y bloques del texto. Se aplicó en [3] el algoritmo AES para cifrar imágenes, la imagen es dividida en bloques por el corte en filas y columnas; luego comienza el proceso de cifrado. Se propuso una mejora del algoritmo RSA en [7], este adiciona dos números cortos para aumentar la seguridad; tiene tres procesos: generación, cifrado y descifrado; los experimentos se realizaron en lenguaje JAVA. En

[8] se propuso un algoritmo formado por AES y NTRU para mantener la integridad y confidencialidad de la información; en las pruebas de tiempo el algoritmo propuesto toma menos tiempo en ejecución. Se mejoró el algoritmo DSA [9] y se comparó en ejecución con el algoritmo RSA; en las pruebas el DSA fue mejorado toma menos tiempo en cifrar y descifrar datos. Una vez identificado los activos más importantes[10]; la información contenida en una base de datos dividida en voz, videos, texto; los métodos de contingencia después de ver sufrido una afectación sea catástrofe natural, falla masiva o daño premeditado; para la organización mitigar esta afectación se analiza para llevar procedimientos; por procesos llevar a cabo cada año pruebas de forma indispensable para simular situaciones antes mencionadas, para ello se debe contar con todo el apoyo de las gerencias involucradas en los procesos de la empresa; definir políticas de seguridad previo al desarrollo de algoritmos de seguridad, identificando un tipo de amenaza, con respuesta estratégica y tácticos minimizando el impacto de la afectación con un plan de recuperación acertada.

Los algoritmos de cifrado se aplican a imágenes médicas [11]; aquí los autores compararon la distorsión de las imágenes entre los algoritmos AES, DES, RSA, RC4 y LBS; ellos confirman que AES es más flexible en cifrado de imágenes. La propuesta de [12] para identificar y prevenir ataques informáticos en una organización es importante a motivo que el principal objetivo de los atacantes es la información vital de la organización; podemos definir el estudio en dos clases: detectar intuiciones y aplicar criptografía. En [13] se propuso un nuevo algoritmo basado en codificación de datos utilizando una tabla de codificada secreta que contiene 128 códigos ASCII; tiene el proceso de cifrado y descifrado de los datos. Para medir un ataque cibernético, en [14] se realiza una evaluación en el marco de la ciberseguridad; visualizar que el ataque puede ser prevenido si en la instalación se hubiera trabajado un modelo de evaluación referente al NIST CSF en conjunto con el marco de mitigación; se evalúa su postura de ciberseguridad para mitigar las vulnerabilidades que son llamados procesos críticos para la continuidad del negocio. La comunicación estable entre hardware y software va hacer la prioridad para garantizar la entrega de mensajes a servicios legítimos levantados [15]; manejar intermediarios para transportar mensajes sirven de mucho apoyo; los servicios distribuidos de comunicación ayudan a la infraestructura a la comunicación para mensajes acoplados.

2.2 Métodos

Se utiliza la metodología de mapeo sistemático [6], nos sirve para clasificaciones y obtener datos sobre el conocimiento de algoritmos de seguridad y ciberseguridad; se analizará los artículos científicos en categorías, tipos, frecuencias, áreas de aplicación.

El mapeo sistemático está definido en cinco fases: Definición de preguntas de investigación, Ejecutar la búsqueda referencial, Seleccionar las referencias, Clasificar las referencias, y Organizar los datos obtenidos en información.

La consulta es en las bibliotecas virtuales que tiene acceso al Universidad Politécnica Salesiana como Scopus, IEEE Xplore, Science Direct, ACM y Springer.

La búsqueda se limita a investigaciones desde año 2016; las palabras claves para la búsqueda en las librerías con: “Security Algorithm”, “Cybersecurity”, “Cybersecurity Method”

Definición de las preguntas de investigación:

- ¿Cuáles son las categorías, plataformas y áreas utilizadas en ciberseguridad?
- ¿Cuál es el algoritmo más utilizado en ciberseguridad?
- ¿Cuáles son las metodologías más utilizadas en ciberseguridad?

3 Resultados

En esta fase presentamos los resultados en base a los objetivos específicos del anteproyecto:

- Análisis de trabajos de investigación previos para la clasificación de estrategias de seguridad mediante el uso de algoritmos
- Técnicas de seguridad adecuadas para la protección de la información en las organizaciones con el soporte de modelos computacionales
- Metodologías utilizadas en ciberseguridad que evidencien un mejor nivel de protección de la información

3.1 Análisis de trabajos de investigación previos para la clasificación de estrategias de seguridad mediante el uso de algoritmos

Los autores de [16] realizaron un mapeo sistemático en seguridad, aplicaron 3 preguntas de investigación, encontraron 48 artículos de revistas, 198 en conferencias, con 5% de capítulos de libros; los artículos los clasificaron en 15 dominios; el mayor productor de artículos científico es Europa, luego Asia y América.

En [17] se obtuvieron 131 artículos de ACM e IEEE Xplore, aplicaron métodos cuantitativos y cualitativos; ellos determinaron que los estudios se concentran en sistemas de prevención y detección de intrusiones; China y Estados Unidos son los países que más publican sobre inteligencia artificial para ciberseguridad.

El estado de la gobernanza de seguridad en las nubes revisado en [18] para obtener sus tendencias; los autores plantearon cuatro preguntas y de 163 artículos relevantes solo 35 eran relacionados a ambientes en la nube; los autores consideran que es necesario aumentar la gobernanza y existen muchos desafíos.

La seguridad aplicada a computación en la nube revisada en [19] encontraron 83 artículos relevantes de ACM e IEEE Xplore; recalcan la importancia de la mantener la confidencialidad e integridad de la información.

Las tendencias sobre seguridad y usabilidad fueron revisadas en [20] de un mapeo de 179 artículos de biblioteca Web Of Science; se plantaron cuatro preguntas de investigación; en el lado de seguridad la frecuencia más alta es autenticación (99 documentos), después privacidad (67 documentos), confidencialidad e integridad.

Las tendencias sobre contratos inteligentes de blockchain fueron analizadas en [21] sobre 188 artículos relevantes, además clasificaron los documentos en 6 categorías; el 64% es sobre aplicaciones de contratos inteligentes, 21% es sobre ingeniería de software, 6% es sobre seguridad de datos.

3.2 Técnicas de seguridad adecuadas para la protección de la información en las organizaciones con el soporte de modelos computacionales.

Se revisaron trabajos basados en seguridad a través de algoritmos de cifrado para protección de información, en las bases de datos de primer nivel, se da a conocer en las tablas 1 a 5, las propuestas y métricas de los autores en las referencias aplicadas:

Table 1. Biblioteca IEEExplore.

Ref.	Propuesta	Métrica
[22]	Análisis de componentes de un algoritmo criptográfico como tiempo, precio, utilidad, longitud de la clave, eficiencia, funciones avanzadas e inconvenientes de seguridad	Comparación cualitativa
[23]	Comparación de algoritmos de seguridad simétricos y asimétricos	Comparación cuantitativa
[24]	Contrato inteligente con suscriptores y activos de información, al existir ataque se almacenan las direcciones IP en una lista negra del blockchain	11ms en acceso de transacciones
[25]	Análisis comprensivo de algoritmos de cifrado como longitud de clave, tamaño de bloque, cantidad de ciclos, calculo, eficiencia en software o hardware, escalabilidad, seguridad; RSA ejecuta el cifrado y descifrado en un ciclo	Cantidad de ciclos y tamaño de clave
[26]	Algoritmos AES y RC5 combinados en un esquema de seguridad para bases de datos distribuidas	92.06% de ejecución teórica

Table 2. Biblioteca Scopus.

[27]	Arquitectura que utiliza algoritmo Diffie-Hellman actualizado y más seguro para la generación de claves, para resistir ataques a través de valores hash en cada envío	122,990ns para descifrar, 16,450ns en cifrar
[28]	Cifrado y descifrado de archivos que están en un sistema de archivos para aumentar la seguridad en el almacenamiento	1GB cifrado en 6.08min; descifrado en 6.73min; AES en 12.97 y 14.08
[29]	Mejora en algoritmos RC4 y AES para filtrado de direcciones en el acceso a tarjeta de red inalámbrica; genera una capa de cifrado para comunicar dispositivos y redes	Hasta 79.49% de datos válidos
[30]	Algoritmo de cifrado aplicado a imágenes en color a través de encriptación de permutación y encriptación de difusión	Imagen de 512×512, tiempo de cifrado es 5.813seg
[31]	Utiliza características de tecnología de criptografía de cadena de bloques, distribución, algoritmos de cifrado para aumento de la seguridad sobre datos financieros; basado en SHA256 una cadena de datos obtiene un valor hash de 256 bits	Cifrado de datos en 500ms

Table 3. Biblioteca Science Direct.

[32]	Algoritmo de cifrado de imágenes en color con aplicación de hash 32.0.% de encripSHA-256, se combinan los planos de bits y claves; contra ataques de tación de imágenes contenido sin formato	
[33]	Aplicación de criptosistemas homomórficos para conservar el texto ci- Comparaciones frados en la nube, esto permite que otros ejecuten cálculos sobre texto cualitativas cifrados	
[34]	Algoritmo para cifrar imágenes, aplica el algoritmo hash SHA-256 y obtiene un valor hash binario de 256 bits; propuesta sensible a la imagen original	Promedio intensidad 33.46%

[35]	Método de ocultación de información médica a través de Blowfish	NO hay medida
[36]	Búsqueda sobre datos cifrados en servidores en la nube utilizan predicados booleanos o clasificados a través de algoritmo AES	NO hay medida

Table 4. Biblioteca ACM.

[37]	Proteger la ubicación del cliente y privacidad del servidor en servicios de la nube a través de algoritmo AES y Paillier; para reducir costo de almacenamiento y comunicación	fórmula de cálculo de costo bits
[38]	Aplicar seguridad a través de cifrado lógico para cubrir problemas de hardware, utiliza algoritmo SAT	Función de hard-ware 0.9; estructura hardware 0.75
[39]	Algoritmos de cifrado para interrumpir los pixeles de una fila o columna de manera aleatoria sobre archivos jpg o png	1.5 segundos
[40]	Cifrado de archivos con algoritmos AES, DES, 3DES, Blowfish, Twofish	Mejor puntuación AES
[41]	Aplica criptografía a bases de datos en la nube para garantizar confidencialidad	Entre AES, RSA y OPE; AES es mejor

Table 5. Biblioteca Springer.

[42]	Encriptar aplicaciones web de la nube a través de AES o FPE, aquí AES toma menos tiempo; se conservan los formatos de datos	1000 entradas en 60ms
[43]	Cifrado híbrido para archivos con algoritmos AES y CP-ABE; el descrifrado es de acuerdo a las políticas de acceso	Cifrado en 100 atributos en menos de 1250ms
[44]	Cifrado de árbol de búsqueda de documentos de registros médicos a través de algoritmo ORE	41.9ms para cifrar 5000 documentos
[45]	Obtener un duplicado de datos originales a través de algoritmo RCE para garantizar la integridad de los datos	Cifrado 15.423 ms; descifrado es 15.137ms para 1000 bloques
[46]	Algoritmo básico para consultas en bases de datos encriptadas para mantener la privacidad, RSA con OAEP.	Variaciones entre 1 y 5%

En tabla 5, se presentan las referencias clasificadas en sus categorías que aplicaron para protección de la información; se distingue que la mayoría da prioridad a la privacidad de los datos, esto significa que las propuestas garantizan la no intrusión de terceros y que solo los dueños de la información pueden ver solo sus propios datos.

Table 5. Referencias por categorías.

Categoría	**Referencias**
Privacidad	[25], [27], [29], [33], [35], [36], [37], [42], [43], [44], [46]
Integridad	[26], [31], [34], [38], [39], [45]
Confidencialidad	[24], [32], [40], [41]
Eficiencia	[23], [28], [30]
Disponibilidad	[22]

La Fig. 1 representa distribución de las referencias de acuerdo a la categoría para protección de la información; la Fig. 2 representa la clasificación de las referencias en las plataformas que aplicaron, aquí las arquitecturas distribuidas utilizan mucho el cifrado de la información para tener un mejor nivel de protección.

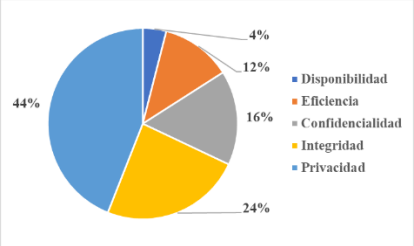

Fig. 1. Categorías.

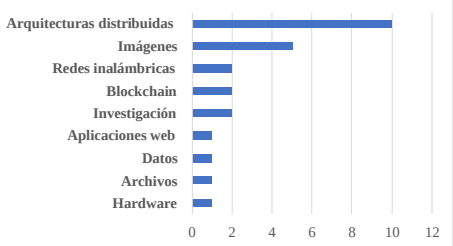

Fig. 2. Plataformas.

La Fig. 3 representa las referencias nombraron las áreas de aplicación, en los casos que no se especificó áreas se consideró como área general; la Fig. 4 representa los algoritmos más utilizados, aquí Advanced Encryption Standard (AES) es el más utilizado en 8 de las 25 referencias revisadas.

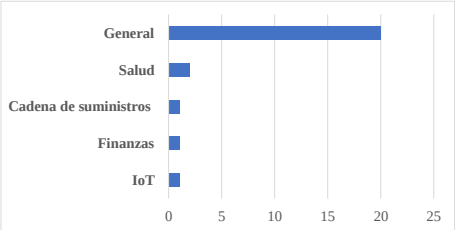

Fig. 3. Áreas.

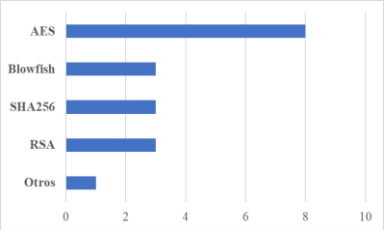

Fig. 4. Algoritmos.

3.3 Metodologías utilizadas en ciberseguridad que evidencien un mejor nivel de protección de la información

De acuerdo con las referencias obtenidas, a continuación, se presentan algunos métodos utilizados en ciberseguridad; los artículos encontrados en la Tabla 6 dan a conocer en forma muy resumida los métodos cuyos objetivos son aumentar el nivel de protección de la información, sin importar la plataforma o área.

Table 6. Metodologías encontradas en referencias.

Ref.	Método	Métrica
[47]	Modelo de aprendizaje para detectar anomalías o incoherencias en las conexiones de vehículos	0.9 en online y offline
[48]	Tecnología para ejecutar procedimientos para la descripción, valoración y simulación en los cambios de la interacción hombre-máquina.	Sin medida
[49]	Procesos para gestión de riesgos en sistemas industriales	Sin medida

[50]	Sistema de toma de decisiones para mitigar el riesgo de ataques y proteger los componentes industriales	Complejidad computacional bajo en 87.5%
[51]	Aplicación de red cognitiva primitiva que evalúa las alternativas en ciberseguridad	Fórmula para evaluar alternativas
[52]	Modelo entre Machine learning y Deep learning para detectar la intrusión	Exactitud 99.9% de SVM
[53]	Blockchain para aumentar la seguridad y mitigar el riesgo en gestión de energía	Bajo costo de operación
[54]	Lenguaje natural en la extracción de datos para determinar amenazas	83% de precisión
[55]	Modelo de datos en requisitos para proteger la aviación civil	Sin medida
[56]	Red de software para detectar intrusos en sistemas industriales	0.1ms
[57]	Marco cognitivo para representar y anticipar la conducta humana, luego reconocer amenazas	Sin medida
[58]	Modelo para seguimiento de intercambio de datos y medir el nivel de esfuerzo en ciberseguridad	Coeficiente de intercambio optimo
[59]	Modelo con técnicas defensivas para detectar ataques y activar defensa	Aumento de beneficios
[60]	Modelo para reconocimiento de entidades a través de la extracción	Precisión entre 33% y 100%
[61]	Marco de ciberseguridad NIST formado por 5 funciones	Sin medida

La Fig. 5 representa las metodologías clasificadas y obtenidas de las referencias; la mayoría son modelos (40%) para aumentar la ciberseguridad, le siguen las aplicaciones o software (34%), los procesos (13%) y marco (13%) en menor cantidad; para esto solo se consultaron 15 referencias.

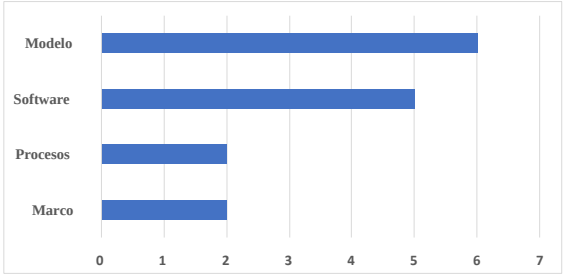

Fig. 5. Metodologías utilizadas en ciberseguridad.

Se entiende que los modelos son propuestas académicas para protección de datos; software son propuestas que comenzaron en la academia y están uso; los procesos son propuestas que comenzaron su utilización en ambientes empresariales; los marcos son propuestas ya utilizadas por empresas y profesionales como es NIST.

4 Discusión

La primera y segunda pregunta de investigación fue contestada en la sección 3.2 que describe las técnicas adecuadas para protección de información en base a las referencias; la tercera pregunta fue contestada en la sección 3.3 que describe los métodos o metodologías utilizadas en ciberseguridad en base a las referencias; se aplicó el mapeo sistemático para obtener las referencias desde las bibliotecas virtuales a las que tiene acceso la Universidad Politécnica Salesiana.

Una de las formas más segura para protección de la información es la criptografía, que utiliza algoritmos para cifrar cualquier tipo de dato; las categorías principales de la información son confidencialidad, integridad y disponibilidad, entre éstas la disponibilidad es la principal categoría con el 44% de las referencias clasificadas.

Relación de los resultados: el primer resultado que explica ciertos trabajos (6 referencias) previos tienen relación con el segundo resultado (25 referencias) y tercer resultado (15 referencias) por que se aplicó el mapeo sistemático para conocer la situación actual de la ciberseguridad en base a 40 referencias revisadas.

Nuestra investigación concuerda con las referencias descritas en el primer resultado de este documento; porque aplica el mapeo sistemático sobre bibliotecas virtuales, además se describieron y clasificaron las referencias para entregar un mínimo conocimiento sobre el estado actual de la ciberseguridad.

Excepciones: se considera que 40 referencias revisadas para obtener los resultados es pequeña, porque los trabajos relacionados mínimo trataron con 83 referencias.

La consecuencia teórica de esta propuesta es dar a conocer las categorías, plataformas, áreas y algoritmos que se utilizan para ciberseguridad; y reivindicar que el algoritmo AES es el más utilizado para cifrar información de cualquier tipo, sea texto o imagen.

5 Conclusiones

Se concluyó que la ciberseguridad utiliza algoritmos de criptografía como una herramienta y buena opción para protección de un ambiente cibernético y se aplica a cualquier tipo de dato; entre 40 referencias clasificadas que aplican ciberseguridad, el 44% está en la categoría disponibilidad; el 40% está en arquitecturas distribuidas; el 80% está en áreas generales; el 32% utiliza el algoritmo AES en ciberseguridad; el 40% de las referencias se basan en modelos para aumentar el nivel de protección de la información.

References

1. Yassein, M.B., Aljawarneh, S., Qawasmeh, E., Mardini, W., Khamayseh, Y.: Comprehensive study of symmetric key and asymmetric key encryption algorithms. 2017 Int. Conf. Eng. Technol. 1–7 (2017). https://doi.org/10.1109/ICEngTechnol.2017.8308215
2. Veeraragavan, N., Arockiam, L., Manikandasaran, S.S.: Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud. 2017 Int. Conf. Algorithms, Methodol. Model. Appl.

Emerg. Technol. ICAMMAET 2017. 2017-Janua, 1–6 (2017). https://doi.org/10.1109/ICAMMAET.2017.8186644

3. Kumar, A.D.S.: Multi Image Integration and Encryption Algorithm for Security Applications. 986–991 (2016)
4. Jha, D.P., Kohli, R., Gupta, A.: Proposed encryption algorithm for data security using matrix properties. 2016 1st Int. Conf. Innov. Challenges Cyber Secur. ICICCS 2016. 86–90 (2016). https://doi.org/10.1109/ICICCS.2016.7542316
5. Althonayan, A., Andronache, A.: Shifting from Information Security towards a Cybersecurity Paradigm. In: Proceedings of the 2018 10th International Conference on Information Management and Engineering - ICIME 2018. pp. 68–79. ACM Press, New York, New York, USA (2018)
6. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic Mapping Studies in Software Engineering. 1–10 (2007). https://doi.org/10.14236/ewic/EASE2008.8
7. Bonde, S.Y.: Analysis of Encryption Algorithms (RSA , SRNN and 2 key pair) for Information Security. 2–6 (2017)
8. Yousefi, A.: Improving the Security of Internet of Things using Encryption Algorithms. 3–7
9. Singh, D., Nand, P., Astya, R., Dixit, P.: Improved DSA cryptographic protocol and its comparative study with RSA protocol. Int. Conf. Comput. Commun. Autom. ICCCA 2015. 755–759 (2015). https://doi.org/10.1109/CCAA.2015.7148511
10. Toapanta, S.M.T., Antonio, O.T., Enrique, M.G.: A security algorithms approach to apply to the civil registry database of the Ecuador. IEEE CITS 2017 - 2017 Int. Conf. Comput. Inf. Telecommun. Syst. 287–290 (2017). https://doi.org/10.1109/CITS.2017.8035339
11. Mehta, B.: Comparative Analysis of Joint Encryption and Watermarking Algorithms for Security of Biomedical Images. 609–612 (2017)
12. Asghar, M.R., Hu, Q., Zeadally, S.: Cybersecurity in industrial control systems: Issues, technologies, and challenges. Comput. Networks. 165, 106946 (2019). https://doi.org/10.1016/j.comnet.2019.106946
13. Murtaza, A., Jahanzeb, S., Pirzada, H., Jianwei, L.: A New Symmetric Key Encryption Algorithm With Higher Performance. Presented at the (2019)
14. Gourisetti, S.N.G., Mylrea, M., Patangia, H.: Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Futur. Gener. Comput. Syst. 105, 410–431 (2020). https://doi.org/10.1016/j.future.2019.12.018
15. Fuller, N.J., Simco, G.: Software and cybersecurity: Attack resistant secure software development survivable Distributed Communication Services (DCS). 2008 IEEE Int. Conf. Technol. Homel. Secur. HST'08. 599–602 (2008). https://doi.org/10.1109/THS.2008.4534521
16. Sepúlveda, S., Bustamante, M., Cravero, A.: Identification of non-functional requirements for electronic voting systems: A systematic mapping. IEEE Lat. Am. Trans. 13, 1577–1583 (2015). https://doi.org/10.1109/TLA.2015.7112018
17. Wiafe, I., Koranteng, F.N., Obeng, E.N., Assyne, N., Wiafe, A., Gulliver, S.R.: Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access. 8, 146598–146612 (2020). https://doi.org/10.1109/ACCESS.2020.3013145
18. Witti, H., Ghedira-Guegan, C., Disson, E., Boukadi, K.: Security Governance in Multi-cloud Environment: A Systematic Mapping Study. In: 2016 IEEE World Congress on Services (SERVICES). pp. 81–86. IEEE (2016)
19. Jara Juarez, D.X., Cedillo, P.: Security of mobile cloud computing: A systematic mapping study. In: 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM). pp. 1–6. IEEE (2017)
20. MERDANOGLU, N., ONAY DURDU, P.: A systematic mapping study of usability vs security. In: 2018 6th International Conference on Control Engineering & Information Technology (CEIT). pp. 1–6. IEEE (2018)

21. Alharby, M., Van Moorsel, A.: Blockchain-Based Smart Contracts : a Systematic Mapping Study. arXiv. (2017). https://doi.org/10.5121/csit.2017.71011
22. Soomro, S., Belgaum, M.R., Alansari, Z., Jain, R.: Review and open issues of cryptographic algorithms in cyber security. Proc. - 2019 Int. Conf. Comput. Electron. Commun. Eng. iCCECE 2019. 158–162 (2019). https://doi.org/10.1109/iCCECE46942.2019.8941663
23. Rani, D.J., Roslin, S.E.: Light weight cryptographic algorithms for medical internet of things (IoT) - A review. Proc. 2016 Online Int. Conf. Green Eng. Technol. IC-GET 2016. (2017). https://doi.org/10.1109/GET.2016.7916703
24. Anwer, M., Saad, A., Ashfaque, A.: Security of IoT Using Block chain: A Review. ICISCT 2020 - 2nd Int. Conf. Inf. Sci. Commun. Technol. 0–4 (2020). https://doi.org/10.1109/ICISCT49550.2020.9079943
25. Alroubiei, M., Alyarubi, T., Kumar, B.: Critical Analysis of Cryptographic Algorithms. 8th Int. Symp. Digit. Forensics Secur. ISDFS 2020. (2020). https://doi.org/10.1109/ISDFS49300.2020.9116213
26. Toapanta, Orozco, M.: Analysis of Adequate Security Algorithms Oriented to Cybersecurity Management for a Distributed Architecture. In: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) Authorized. pp. 715–721 (2020)
27. Ali, S., Humaria, A., Ramzan, M.S., Khan, I., Saqlain, S.M., Ghani, A., Zakia, J., Alzahrani, B.A.: An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. Int. J. Distrib. Sens. Networks. 16, 155014772092577 (2020). https://doi.org/10.1177/1550147720925772
28. Kapil, G., Agrawal, A., Attaallah, A., Algarni, A., Kumar, R., Khan, R.A.: Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective. PeerJ Comput. Sci. 6, e259 (2020). https://doi.org/10.7717/peerj-cs.259
29. Li, Y., Guo, W., Meng, X., Xia, W.: Charging wireless sensor network security technology based on encryption algorithms and dynamic model. Int. J. Distrib. Sens. Networks. 16, 155014772090199 (2020). https://doi.org/10.1177/1550147720901999
30. Hu, Y., Yu, S., Zhang, Z.: On the Security Analysis of a Hopfield Chaotic Neural Network-Based Image Encryption Algorithm. Complexity. 2020, 1–10 (2020). https://doi.org/10.1155/2020/2051653
31. Chen, Y., Zhang, Y., Zhou, B.: Research on the risk of block chain technology in Internet finance supported by wireless network. EURASIP J. Wirel. Commun. Netw. 2020, 71 (2020). https://doi.org/10.1186/s13638-020-01685-6
32. Ghadirli, H.M., Nodehi, A., Enayatifar, R.: An overview of encryption algorithms in color images. Signal Processing. 164, 163–185 (2019). https://doi.org/10.1016/j.sigpro.2019.06.010
33. Kaaniche, N., Laurent, M.: Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Comput. Commun. 111, 120–141 (2017). https://doi.org/10.1016/j.comcom.2017.07.006
34. Wang, X., Xue, W., An, J.: Image encryption algorithm based on Tent-Dynamics coupled map lattices and diffusion of Household. Chaos, Solitons & Fractals. 141, 110309 (2020). https://doi.org/10.1016/j.chaos.2020.110309
35. Sajedi, H., Rahbar Yaghobi, S.: Information hiding methods for E-Healthcare. Smart Heal. 15, 100104 (2020). https://doi.org/10.1016/j.smhl.2019.100104
36. Siva Kumar, D.V.N., Santhi Thilagam, P.: Approaches and challenges of privacy preserving search over encrypted data. Inf. Syst. 81, 63–81 (2019). https://doi.org/10.1016/j.is.2018.11.004
37. Li, L., Lv, Z., Tong, X., Shi, R.: A Location Privacy Protection Scheme Based on Hybrid Encryption. In: Proceedings of the 3rd International Conference on Computer Science and Application Engineering - CSAE 2019. pp. 1–6. ACM Press, New York, New York, USA (2019)
38. Šišejković, D., Leupers, R., Ascheid, G., Metzner, S.: A Unifying logic encryption security metric. In: Proceedings of the 18th International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation. pp. 179–186. ACM, New York, NY, USA (2018)

39. Zeng, J., Zhan, Y., Yang, J.: Encryption and Decryption of Optical Images with Different Algorithms. In: Proceedings of the 2nd International Conference on Artificial Intelligence and Advanced Manufacture. pp. 256–265. ACM, New York, NY, USA (2020)
40. Pagkalinawan, A.D., Fabregas, A.C.: A Secured and Optimized Document Management tool using Advanced Encryption Standard and NoSQL. In: Proceedings of the 2017 International Conference on Information Technology - ICIT 2017. pp. 167–170. ACM Press, New York, New York, USA (2017)
41. Draidi, F., Hmedat, M., Abwe, B., Atrash, A.: CryptDBaaS. In: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. pp. 1–7. ACM, New York, NY, USA (2018)
42. Guo, X., Huang, Y., Ye, J., Yin, S., Li, M., Li, Z., Yiu, S.-M., Cheng, X.: ShadowFPE: New Encrypted Web Application Solution Based on Shadow DOM. Mob. Networks Appl. (2020). https://doi.org/10.1007/s11036-019-01509-y
43. Tu, Y., Yang, G., Wang, J., Su, Q.: A secure, efficient and verifiable multimedia data sharing scheme in fog networking system. Cluster Comput. 6, (2020). https://doi.org/10.1007/s10586-020-03101-6
44. Chen, L., Zhang, N., Sun, H.-M., Chang, C.-C., Yu, S., Choo, K.-K.R.: Secure search for encrypted personal health records from big data NoSQL databases in cloud. Computing. 102, 1521–1545 (2020). https://doi.org/10.1007/s00607-019-00762-z
45. Bai, J., Yu, J., Gao, X.: Secure auditing and deduplication for encrypted cloud data supporting ownership modification. Soft Comput. 24, 12197–12214 (2020). https://doi.org/10.1007/s00500-019-04661-5
46. Cui, N., Yang, X., Wang, B., Geng, J., Li, J.: Secure range query over encrypted data in outsourced environments. World Wide Web. 23, 491–517 (2020). https://doi.org/10.1007/s11280-019-00726-5
47. Levi, M., Allouche, Y., Kontorovich, A.: Advanced Analytics for Connected Car Cybersecurity. In: 2018 IEEE 87th Vehicular Technology Conference (VTC Spring). pp. 1–7. IEEE (2018)
48. Lavrov, E.A., Volosiuk, A.A., Pasko, N.B., Gonchar, V.P., Kozhevnikov, G.K.: Computer Simulation of Discrete Human-Machine Interaction for Providing Reliability and Cybersecurity of Critical Systems. In: 2018 Third International Conference on Human Factors in Complex Technical Systems and Environments (ERGO)s and Environments (ERGO). pp. 67–70. IEEE (2018)
49. Szabo, Z.: Cybersecurity Issues in Industrial Control Systems. In: 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY). pp. 000231–000234. IEEE (2018)
50. Qin, Y., Zhang, Q., Zhou, C., Xiong, N.: A Risk-Based Dynamic Decision-Making Approach for Cybersecurity Protection in Industrial Control Systems. IEEE Trans. Syst. Man, Cybern. Syst. 50, 3863–3870 (2020). https://doi.org/10.1109/TSMC.2018.2861715
51. Yuen, K.K.F.: Towards a Cybersecurity Investment Assessment method using Primitive Cognitive Network Process. In: 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). pp. 068–071. IEEE (2019)
52. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., Wang, C.: Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access. 6, 35365–35381 (2018). https://doi.org/10.1109/ACCESS.2018.2836950
53. Wang, B., Dabbaghjamanesh, M., Kavousi-Fard, A., Mehraeen, S.: Cybersecurity Enhancement of Power Trading Within the Networked Microgrids Based on Blockchain and Directed Acyclic Graph Approach. IEEE Trans. Ind. Appl. 55, 7300–7309 (2019). https://doi.org/10.1109/TIA.2019.2919820
54. Mendsaikhan, O., Hasegawa, H., Yamaguchi, Y., Shimada, H.: Identification of Cybersecurity Specific Content Using the Doc2Vec Language Model. In: 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). pp. 396–401. IEEE (2019)
55. Gnatyuk, S.: Multilevel Unified Data Model for Critical Aviation Information Systems Cybersecurity. In: 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD). pp. 242–247. IEEE (2019)
56. Wang, F., Qi, W., Qian, T.: A Dynamic Cybersecurity Protection Method based on Software-defined

Networking for Industrial Control Systems. In: 2019 Chinese Automation Congress (CAC). pp. 1831–1834. IEEE (2019)

57. Abie, H.: Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems. In: 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT). pp. 1–6. IEEE (2019)
58. Yang, Y., Ji, G., Yang, Z., Xue, S.: Incentive Contract for Cybersecurity Information Sharing Considering Monitoring Signals. In: 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). pp. 507–512. IEEE (2019)
59. Li, J., Zhang, Q., Zhang, D., Song, J., Wu, W.: Research on Optimal Strategies of SAS Cybersecurity based on MDP. In: 2019 IEEE Sustainable Power and Energy Conference (iSPEC). pp. 2078–2083. IEEE (2019)
60. Yi, F., Jiang, B., Wang, L., Wu, J.: Cybersecurity Named Entity Recognition Using Multi-Modal Ensemble Learning. IEEE Access. 8, 63214–63224 (2020). https://doi.org/10.1109/ACCESS.2020.2984582
61. Webb, J., Hume, D.: Campus IoT Collaboration and Governance using the NIST Cybersecurity Framework. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018. pp. 25 (7 pp.)-25 (7 pp.). Institution of Engineering and Technology (2018)