ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.1355

Implementation of Standard Symmetric Algorithms for Data Encryption: Systematic Review

Yachas Granados, Alberto Vicente[1], Alata Linares, Vicky Leonor[1], Menacho Navarrete, Karem[1]
[1]Universidad Tecnológica del Perú, Perú, U19214054@utp.edu.pe, C22553@utp.edu.pe, C24686@utp.edu.pe

Abstract*-- Summary—With the advancement of technology, ways to compromise information security continue to be the Achilles heel for many web ventures. This article analyzes the symmetric encryption algorithms applied to a virtual store. To find out what these are, a PICO question was asked to delimit the research topic together with the PRISMA Model. After obtaining the optimal amount, we proceed to show results such as the optimization of algorithms in the anticipation of distributed denial of service, in turn its accuracy and precision. Improvement in password management and the security of economic transactions. through graphs and tables. Followed by a post-results analysis, the importance and validity of the results obtained are detailed and interpreted here.

***Keywords*—Symmetric algorithm, encryption, cryptography, privacy, secret key, DDoS**

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Implementación de Algoritmos Simétricos Estándar para la encriptación de datos: Revisión Sistemática

Yachas Granados, Alberto Vicente[1], Alata Linares, Vicky Leonor[1], Menacho Navarrete, Karem[1]
[1]Universidad Tecnológica del Perú, Perú, U19214054@utp.edu.pe, C22553@utp.edu.pe, C24686@utp.edu.pe

***Resumen*— Con el avance de la tecnología, las formas de corromper la seguridad de información siguen siendo el talón de Aquiles para muchos emprendimientos Web. En la presente Revisión Sistemática (RS) se analiza los algoritmos de encriptación simétrica de datos. Para conocer cuáles son estos, se realizó una pregunta PICO para delimitar el tema de revisión junto con el Modelo PRISMA. Luego de obtener la cantidad óptima se procede a mostrar resultados como la optimización de algoritmos en la anticipación de denegación de servicio distribuido, a su vez la exactitud y precisión de este. La mejora en gestión de contraseñas y en la seguridad de transacciones económicas. mediante gráficos y tablas. Seguido de un análisis post-resultados, aquí se detalla e interpreta la importancia y validez de los resultados obtenidos.**

***Palabras Claves*— Algoritmo simétrico, cifrado, criptografía, privacidad, clave secreta, DDoS**

I. INTRODUCCION

En un mundo cada vez más interconectado y dependiente de la tecnología, las tiendas virtuales se han convertido en un componente esencial del comercio global y las únicas formas de vender sus productos es mediante redes sociales y contacto directo. Este tipo de plataformas en línea permiten a los consumidores explorar y adquirir una amplia variedad de productos y servicios desde la comodidad de sus hogares. Con el constante avance de la tecnología, la empresa se ve en la necesidad de implementar la encriptación de datos en su entorno web. Es aquí donde entra en juego la encriptación simétrica, esta es una técnica fundamental en el mundo de la seguridad de la información, especialmente cuando se trata del cifrado de archivos que se envían a través de redes. En este proceso, se utiliza una única clave, conocida como "clave de cifrado, tanto para encriptar como desencriptar los datos.

La pregunta que se hace es, ¿Están preparados para prevenir el descifrado masivo de datos por parte de los atacantes? La protección de los datos en el sector sanitario de manera tradicional tiene tiempos medios de confidencialidad extenso y de cifrado con eficiencia baja [1]. Los atacantes evalúan la vulnerabilidad del sistema computacional que poseen los emisores de claves públicas, volviendo así los ataques mucho más rápidos. Además, la elección de claves fuertes o difíciles de adivinar es esencial al momento de mitigar dichos ataques, pero esto trae costos elevados de gestión. La integridad y la verificación se pueden utilizar debido a las siguientes características: En el cifrado del tráfico de Internet intervienen chips de bloques simétricos como papel esencial, y los estándares de cifrado de datos (DES) y de cifrado avanzado (AES) garantizan la privacidad de cifrado subyacente brindando seguridad de la información y protección de datos [2].

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Por ello, se considera que el análisis de encriptación de datos es esencial para el desarrollo educativo y profesional. Esta iniciativa permite adquirir habilidades críticas, estar al tanto de las tendencias tecnológicas y contribuir al conocimiento en seguridad de la información. Además, brinda una base sólida para proteger datos personales y fomentar prácticas éticas en el entorno digital.

El objetivo principal de la investigación es evaluar la implementación de la encriptación simétrica en el entorno web. Se busca analizar la eficacia de este método de cifrado como medida de seguridad ante posibles ataques de fuerza bruta que busquen descifrar la clave de encriptación utilizada. La investigación se enfoca en comprender cómo la encriptación simétrica, con énfasis en estándares como el Data Encryption Standard (DES) y el Advanced Encryption Standard (AES), contribuye a garantizar la privacidad y seguridad de los datos transmitidos a través de la plataforma.

Por consiguiente, la estructura de la RSL está organizado de la siguiente manera. La sesión I con la Introducción presenta un panorama del problema, la justificación y estructura del contenido de la revisión. La sesión II Metodología, como parte de este apartado se expone la pregunta PICO, describiendo los componentes como Problema, Intervención, Comparación, Resultados y Contexto. Luego de pasar por un filtro que sirve para delimitar la revisión sistemática, la sección III, presenta los Resultados luego de evaluar exhaustivamente los estudios delimitados y recabar información relacionada con la encriptación simétrica de datos y la detección de ataques DDoS. Sigue la sección IV, aquí se expone la Discusión, que se dedica a interpretar y analizar los resultados obtenidos a la luz de los objetivos de la investigación, revisando la literatura existente, y proporcionando una interpretación crítica de los hallazgos. Finalmente, en la sección V, se presentan las Conclusiones, donde se resumen los hallazgos obtenidos, también ofrecen una reflexión significativa sobre su impacto, relevancia y las posibles direcciones futuras que podrían explorarse en el estudio de RS. Este análisis final pretende consolidar el conocimiento y contribuir al crecimiento continuo del campo de investigación al que se ha dedicado.

II. METODOLOGÍA

A. *Pregunta PICO*

En primer lugar, se detalla un punto clave para comenzar con la búsqueda sistemática sobre los algoritmos de encriptación simétrica y analizar las distintas técnicas que ayuda con la implementación de una mejora en la seguridad de la clave pública.

Para ello, se ha desarrollado la pregunta RQ de acuerdo con cada uno de los componentes del PICO que tiene como objetivo limitar la búsqueda y obtener los resultados

esperados. RQ: ¿Qué algoritmos de encriptación simétrica serán aplicados en la seguridad e implementación de buenas prácticas de diseño en el envío de datos para la proteger las claves públicas y canales de comunicación en la plataforma virtual?

Para desglosar la pregunta global RQ se describe en la Fig. 1 las preguntas importantes de cada componente PICO.

RQ: ¿Qué algoritmos de encriptación simétrica serán aplicados en la seguridad e implementación de buenas prácticas de diseño en el envío de datos para la proteger las claves públicas y canales de comunicación en la plataforma virtual?

RQ1: ¿Cuál es el impacto de un ataque de fuerza bruta hacia la seguridad de claves y canales de comunicación?

RQ2: ¿Qué algoritmos de encriptación simétrica serán utilizados?

RQ3: ¿La aplicación de algoritmos en los canales de comunicación mejoraron la seguridad de claves de encriptación de los que no la tienen?

RQ4: ¿Cuáles son las apreciaciones tras la optimización en seguridad de claves y canales de comunicación?

RQ5: ¿Cuáles son los sitios web donde se presencia una mayor consulta masiva hacia los canales de comunicación?

Fig. 1 Preguntas PICO

Seguidamente, a partir de las preguntas se muestra en la Tabla I. La especificación del componente PICO junto con su correspondiente función y palabras claves descritas en inglés.

TABLA I
ESCPECIFICACIÓN DEL COMPONENTE PICO

Componente PICO			Palabras claves en inglés
P	Problema	Seguridad en claves de encriptación	security, encryption, computing, encryption keys
I	Intervención	Algoritmos de encriptación simétrica	algorithms, encryption, cryptography, symmetric encryption, symmetric encryption algorithms
C	Comparación	Seguridad, buenas prácticas en el diseño de manera general en algoritmos de clave simétrica.	Security, good practices, design, symmetric key, algorithms
O	Resultados	Optimizar la seguridad en canales de comunicación y claves simétricas.	security, optimization, communication channels, symmetric keys
C	Contexto	Sitio web	Web page, website

B. *Ecuación de Búsqueda en Scopus*

A continuación, con las palabras claves en inglés se creó la ecuación que delimitó la búsqueda de información en Scopus relacionadas con el tema de revisión sistemática: (security or encryption or computing or “encryption keys”) and (algorithms or encryption or cryptography or “symmetric encryption” or “symmetric encryption algorithms”) and (security or “good practices” or design or “symmetric key” or “design algorithms”) and (security or optimization or “communication channels” or “symmetric keys”) and (“web page” or website).

Una vez creada la ecuación que delimita la búsqueda y amplia la revisión, se realizó filtros. Para ello, con el fin de obtener documentos más específicos que tengan relación con el tema de estudio se plantearon los siguientes criterios:

1) *Criterios de Inclusión:*
   - Investigaciones que profundicen en encriptación simétrica.
   - Estudios que apliquen el algoritmo AES, DES, ChaCha20.
   - Estudios relacionados en la seguridad de claves públicas.
   - Los estudios deben contener la aplicación de algoritmos a un caso de ataque real.
2) *Criterios de Exclusión:*
   - Estudios anteriores a 2021.
   - Estudios diferentes a un entorno de sitio web.
   - Estudios que estén en idiomas diferentes de inglés y español.

C. *Modelo PRISMA*

Con la ecuación inicial se obtuvo 2459 documentos en total, debido a que no hubo ninguna restricción respecto a las palabras claves que se indica en el modelo PICO. Se utilizó una base de datos para la búsqueda. Por ello, no se presenta ningún documento duplicado.

Seguidamente, con el fin de limitar los resultados de la búsqueda se planteó el Diagrama de flujo PRISMA, que a través de filtros arrojó una cantidad óptima para la revisión sistemática.

Como se muestra en la Fig. 2, luego de obtener 2459 documentos, se aplicaron las herramientas de automatización o también llamados criterios de inclusión y exclusión (no se aplicaron todos los criterios de exclusión, específicamente se plantea el rango de fecha 2021 – 2023), y así se obtuvo un total de 394 investigaciones.

Continuando con el cribado se analizaron los títulos y resúmenes de los documentos encontrados bajo los criterios ya mencionados anteriormente, el resultado en esta fase es de 317 estudios que no cumplen con los criterios planteados. Se hace un hincapié en los criterios, como por ejemplo que trate sobre encriptación simétrica, tenga un enfoque hacia sitios web, se apliquen técnicas de un buen manejo de diseño, entre otros.

Luego, se obtiene un total de 77 publicaciones recuperadas sujetas a evaluación luego a texto completo; los seleccionados como aptos para la revisión sistemática pasaron por un nuevo filtro donde se dividen de aquellos que si se logran recuperar de los que no. De estos documentos, 31 no fueron recuperados a texto completo y se quedó con 46 publicaciones que son evaluadas frente a los criterios de exclusión propuestos. Finalmente, quedan 32 estudios luego de excluir 14 documentos que son catalogados como no aptos para la revisión sistemática.

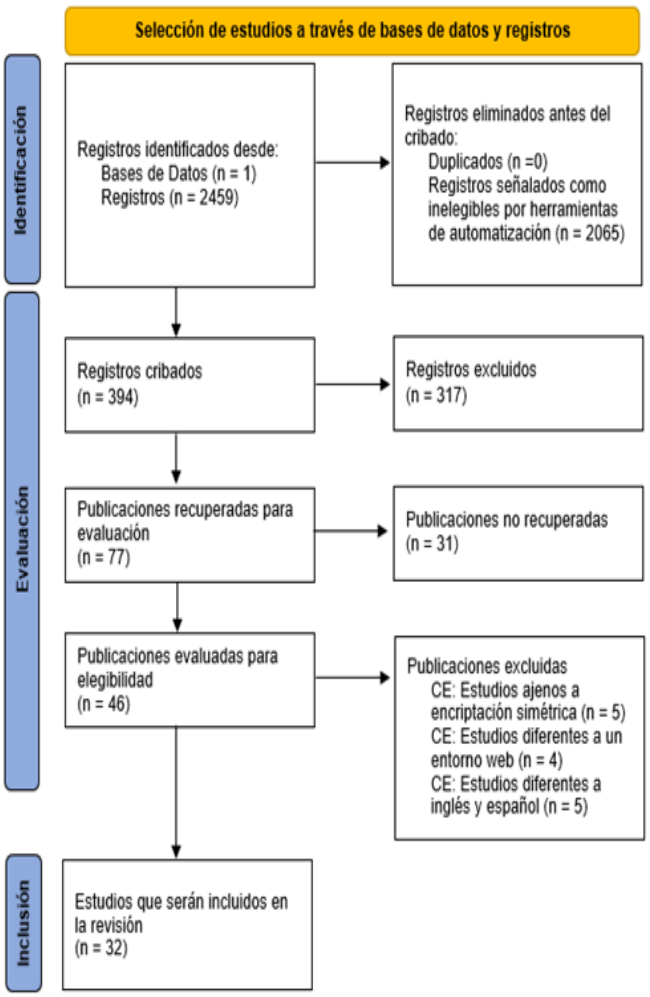

Fig. 2 Diagrama de flujo PRISMA

II. Resultados

En esta sección, se exponen los datos recopilados y se proporcionan análisis estadísticos o cualitativos, según la naturaleza del estudio. La información se presenta de manera organizada, a menudo utilizando tablas, gráficos o descripciones narrativas, con el propósito de responder a la pregunta de investigación.

Tras finalizar la selección de información con el Diagrama de flujo Prisma, se muestra en la Tabla II la especificación de estudios retirados por criterios de exclusión, que se analizaron 394 estudios aplicando el primer criterio de exclusión con el objetivo de acortar el tamaño de estudios analizados.

Una vez obtenido esa cantidad se procedió a revisar cada documento en base a su título y contenido relacionado con el tema de investigación y se descartan así un total de 362 estudios luego de su análisis respectivo.

En efecto, se logra obtener 32 estudios selectos para la revisión sistemática, con el fin de mantener una relación con los objetivos propuestos.

En consecuencia, se menciona los ítems que son de ayuda para la extracción de datos pertenecientes a la pregunta PICO del trabajo de investigación. A continuación, en la Tabla III se detalla los ítems respecto a cada elemento PICO:

TABLA II
Especificaciones de Estudios Retirados por Criterios de Exclusión

	PICO	Paso
	SCOPUS	
Identificación	2459	Toda la literatura
	394	1er criterio de exclusión
	394	Duplicados filtrados
Selección	77	2do criterio de exclusión
	46	3er criterio de exclusión
Elegibilidad	32	4to criterio de exclusión

TABLA III
Ítems para la Extracción de Datos

RQ - PICO	ÍTEMS
RQ1 (Problema): ¿Cuál es el impacto de un ataque de fuerza bruta hacia la seguridad de claves y canales de comunicación?	- Descripción del problema abordado. - Definición de un ataque de fuerza bruta. - Seguridad y tipos de claves.
RQ2 (Intervención): ¿Qué algoritmos de encriptación simétrica serán utilizados?	- Detalle de algoritmos aplicados - Equipos que fueron utilizados - Métodos aplicados al diseño - Duración de las pruebas - Tipo de almacén de datos utilizado - Entorno de desarrollo integrado (IDE) - Lenguaje de programación utilizado - Lógica aplicada al desarrollo
RQ3 (Comparación): ¿La aplicación de algoritmos en los canales de comunicación mejoraron la seguridad de claves de encriptación de los que no la tienen?	- Respuesta de seguridad con algoritmos implementados - Excepciones de canales con el modelo utilizado
RQ4 (Resultados): ¿Cuáles son las apreciaciones tras la optimización en seguridad de claves y canales de comunicación?	- Datos (cuantitativos) según cuestionarios, formularios, mesa de ayuda, caja de comentarios - Muestra de desempeño de los algoritmos en las investigaciones - Reseña de usuarios tras pruebas de claves simétricas encriptadas.
RQ5 (Contexto): ¿Cuáles son los sitios web donde se presencia una mayor consulta masiva hacia los canales de comunicación?	- Tipos de páginas web relacionadas al tema de investigación - Recuento de encuestas y evidencias de otras páginas - Enfoque hacia la venta por internet (E-commerce).

Los ítems fueron definidos según el componente PICO, esto para especificar el entorno de estudio y su debido contenido para el formulario de extracción de datos.

Luego, para contar con la información utilizada hace falta una organización de los datos más relevantes insertados en un formulario de diseño específico, como encabezado se cuenta con las categorías de DOI, Título del Artículo, los autores que lo desarrollaron, el Año de publicación, Título de la Revista, Editorial, País de Origen, Contexto de Aplicación y el tipo de estudio (experimento, simulaciones, estudio de caso, estudio con encuestas, investigación-acción).

Asimismo, el formulario también contiene un apartado donde se coloca información más específica según los

componentes PICO. Además, preguntas como la definición de encriptación, los algoritmos que fueron discutidos, los factores en torno a seguridad de claves, la muestra de desempeño de los algoritmos planteados, métodos aplicados, soluciones propuestas, entre otros.

Una vez detallada la información y análisis respectivo se resumen que en 17 artículos [2], [4], [6], [7], [9], [11], [14], [15], [16], [19], [21], [22] [23], [25], [27], [29], [32] que presentan proyectos a través de experimento, es decir, la presentación y aplicación de un método. Asimismo, se catalogaron 11 artículos [3], [8], [10], [13], [17], [18], [24], [26], [28], [30], [31] donde se realizaron un estudio de caso. Un total de 4 artículos [1], [5], [12], [20] que presentan un estudio de tipo investigación – acción. Estos estudios abarcan temas como la detección de ataques DDoS [15], [16], [18], [20], [22], [23], [31], la aplicación de algoritmos de aprendizaje automático [2], [5], [7], [17], [27], aplicación de TLS (Seguridad de la capa transporte) [1], [12], [16], [29], establecen un enfoque en el cifrado de datos [4], [9], [10], [17], [21], [24], [26], la gestión de tráfico en la red [16], [18], [28], [32], la seguridad de claves [17], [24], [29], entre otros temas.

A continuación, se explican los resultados extraídos de toda la información, y así comprender el enfoque de estos.

En la Fig. 3 se puede apreciar la distribución de estudios según sea cualitativo o cuantitativo. En este caso, los estudios de tipo cualitativo abarcan el 84.4% del total de estudios seleccionados. Cabe enfatizar el tema que trataban la mayoría de los artículos como la aplicación de un algoritmo de privacidad, la detección de ataques distribuidos, la implementación de SOA en el comercio electrónico, aplicación de la estenografía, implementación y uso de TLS 1.3, cifrado de datos. Mientras que los 5 artículos de tipo cuantitativo [1], [2]. [3]. [4], [5] se concentran en la evaluación de mecanismos de procesamiento de datos, la protección del despliegue DoH y ECH, algoritmos de corrección de errores y detección de DDoS.

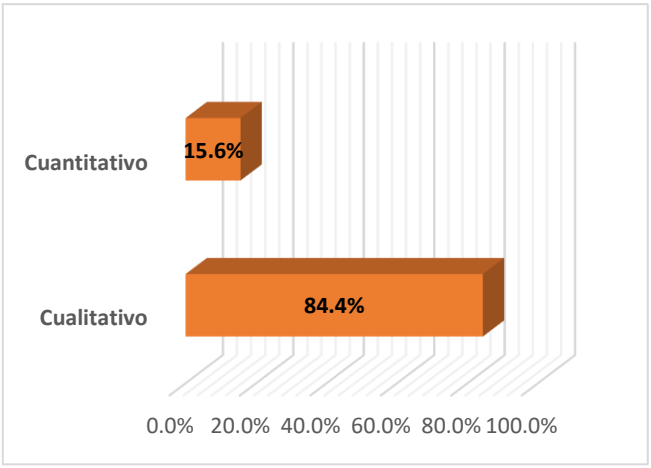

Fig. 3 Cantidad de tipos de estudios

En la Tabla IV se puede deducir que la mayor presencia de estudios se encuentra en el año 2022 con 16 artículos. Entre los temas abordados están la inserción de esteganografía [11], el uso de TLS 1.3 [13], la implementación de un diseño de protección de claves privadas [31] y detección de ataques DDoS [22].

Mientras que la menor cantidad presenciada se encuentra en el año 2021, cuenta con 4 estudios que abarcan la detección temprana de ataques distribuidos [9], la implementación de SOA en E-commerce [10], análisis y rendimiento de algoritmos utilizados para el cifrado de datos [3] y un modelo de privacidad con su algoritmo de implementación [8].

En el año 2023 contiene 12 estudios publicados, los documentos muestran la comparación de modelos en función a su efectividad al momento de detectar ataques DDoS [5], el límite de alcance para medir la protección del despliegue DoH y ECH [2], autenticación de usuarios de internet para evitar actos maliciosos [27], análisis de técnicas de cifrado y protección de datos [29], análisis de la gestión de contraseñas en el sistema web con el objetivo de detectar fallas e inseguridad [25].

TABLA IV
PUBLICACIÓN RESPECTO AL AÑO

Autores	2021	2022	2023
David J, Thomas C. [9]	1		
Kumar K, Gupta H. [10]	1		
Wu Z, Shen S, Zhou H, Li H, Lu C, Zou D. [8]	1		
Pronika, Tyagi S.S. [3]	1		
Poniszewska-Maranda, A. Pradzynski, K. [4]		1	
Almalki K.A, Mohammed R. [11]		1	
Canavese D, Regano L, Basile C, Ciravegna G, Lioy A. [12]		1	
Guan Y, Gou G, Wang B, Fu P, Li Z. [13]		1	
Nirmalraj T, Jebathangam J. [14]		1	
Song B, Sun L, Qin Z. [16]		1	
Agrawal A, Singh R, Khari M, Vimal S, Lim S. [17]		1	
He G, Wei Q, Wang J, Zhu H, Xu B. [18]		1	
Lingamgunta N.M, Gubbal, S.G.N.A. [19]		1	
Snigdho M.A, Chowdhury S, Jahan N. [20]		1	
Ullah M, Khan R.U, Khan I.U, Aslam N, Aljameel S.S, Ul Haq M.I, Islam M.A [21]		1	
Bhargava R, Pal Singh Y, Narawade N.S. [22]		1	
Vishnoi A, Aggarwal A, Prasad A, Prateek M, Aggarwal S. [23]		1	
Akshara Vemuri S, Krishna Chaitanya G. [24]		1	
Guan, Y. Li, Z. Xiong, G. [28]		1	
Galal, H. Mannan, M. Youssef, A. [31]		1	
Chanu, U.S. Singh, K.J. Chanu, Y.J. [1]			1
Trevisan, M. Soro, F. Mellia, M. Drago, I. Morla, R. [2]			1
Geluvaraj, B. Santhosh Krishna, B.V. Umesh, M. Vishnu Girish, G. Yaqoob, Y. [5]			1
Kim, M. Lee, I. [6]			1
Shanker, R. Aggrawal, P. Singh, A. Bhatt, M.W. [7]			1
Pandare, P. Uniyal, S. Vani, R. Mali, S. Rumao, P. [15]			1
Ramesh, A. Haris, R. Arora, S. [25]			1
Althamir, M. Alabdulhay, A. Yasin, M.M. [26]			1
Iskhakov, A.Y. Mamchenko, M.V. Khripunov, S.P. [27]			1
Ling, Y. Li, X. Bin, D. Yang, C. Lu, J. [29]			1
Vankadara, A. Myneni, V. Pendyala, H. Vadlamudi, D. [30]			1
Singh, S. Gupta, M. Sharma, D.K. [32]			1
Sumatoria	4	16	12
Total			32

En la Fig. 4 se muestra en un gráfico de barras los modelos utilizados en los estudios seleccionados, donde la mayor frecuencia visualizada está en Procesamiento de datos y Aprendizaje automático. Se destaca esta cantidad por ser la más representativa a comparación de los demás modelos, cabe aclarar que la frecuencia de los modelos no califica su efectividad.

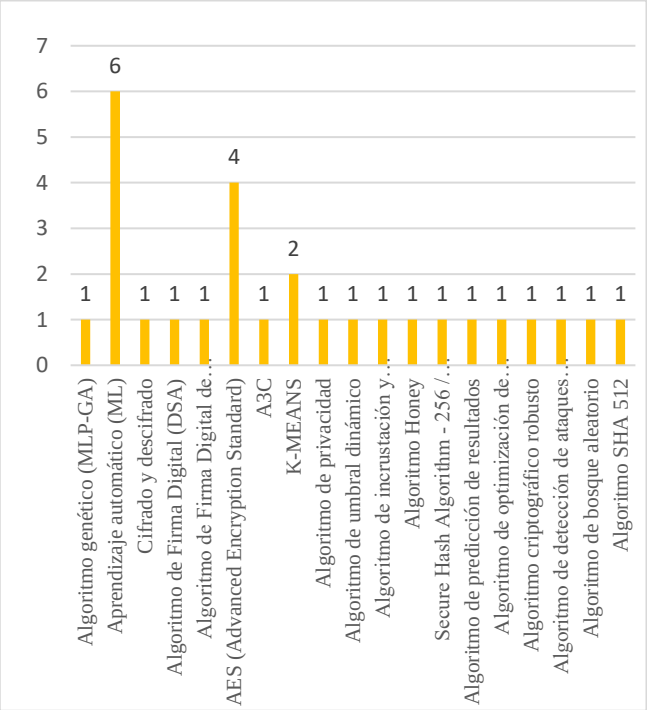

Fig. 4 Métodos utilizados

La Fig. 5 muestra los tipos de estudios que se hallaron en la revisión. A través de un gráfico de barras de doble entrada se aprecia que 17 estudios pertenecen al tipo de estudio experimento, esta cantidad representa una mayor frecuencia a comparación que estudios de caso e investigación – acción.

Fig. 5 Tipos de estudios recopilados

Posteriormente, se observa en la Tabla V la cantidad de tipos de documentos analizados. Para esta revisión sistemática hay Conference Proceedings y Journal como documentos, con una frecuencia de 19 y 13 estudios respectivamente. La temática que predomina dentro de Conference Proceedings es la comparación de varios modelos para separar por categorías los ataques en función de su efectividad para la detección de DDoS, enfatiza la seguridad TLS/SSL, la flexibilidad del cifrado Honey frente a un ataque de fuerza bruta.

Por otro lado, hay 13 documentos de tipo Journal dentro de la revisión. Los temas que predominan son el despliegue DoH y ECH para la protección de sitios web, optimización en la búsqueda de web privada

TABLA V
DISTRIBUCIÓN DE TIPO DE DOCUMENTOS Y SUS AUTORES

Autores	Cantidad	Tipo de Documentos
Poniszewska-Maranda, A. Pradzynski, K. [4] Geluvaraj, B. Santhosh Krishna, B.V. Umesh, M. Vishnu Girish, G. Yaqoob, Y. [5] Kumar K, Gupta H. [10] Almalki K.A, Mohammed R. [11] Guan Y, Gou G, Wang B, Fu P, Li Z. [13] Nirmalraj T, Jebathangam J. [14] Pandare, P. Uniyal, S. Vani, R. Mali, S. Rumao, P. [15] He G, Wei Q, Wang J, Zhu H, Xu B. [18] Snigdho M.A, Chowdhury S, Jahan N. [20] Bhargava R, Pal Singh Y, Narawade N.S. [22] Vishnoi A, Aggarwal A, Prasad A, Prateek M, Aggarwal S. [23] Akshara Vemuri S, Krishna Chaitanya G. [24] Ramesh, A. Haris, R. Arora, S. [25] Althamir, M. Alabdulhay, A. Yasin, M.M. [26] Iskhakov, A.Y. Mamchenko, M.V. Khripunov, S.P. [27] Guan, Y. Li, Z. Xiong, G. [28] Ling, Y. Li, X. Bin, D. Yang, C. Lu, J. [29] Vankadara, A. Myneni, V. Pendyala, H. Vadlamudi, D. [30] Singh, S. Gupta, M. Sharma, D.K. [32]	19	Conference Proceedings
Chanu, U.S. Singh, K.J. Chanu, Y.J. [1] Trevisan, M. Soro, F. Mellia, M. Drago, I. Morla, R. [2] Pronika, Tyagi S.S. [3] Kim, M. Lee, I. [6] Shanker, R. Aggrawal, P. Singh, A. Bhatt, M.W. [7] Wu Z, Shen S, Zhou H, Li H, Lu C, Zou D. [8] David J, Thomas C. [9] Canavese D, Regano L, Basile C, Ciravegna G, Lioy A. [12] Song B, Sun L, Qin Z. [16] Agrawal A, Singh R, Khari M, Vimal S, Lim S. [17] Lingamgunta N.M, Gubbal, S.G.N.A. [19] Ullah M, Khan R.U, Khan I.U, Aslam N, Aljameel S.S, Ul Haq M.I, Islam M.A. [21] Galal, H. Mannan, M. Youssef, A. [31]	13	Journal

La Fig. 6 muestra una comparación de los algoritmos utilizados en los diferentes estudios. Siendo el algoritmo de aprendizaje automático usado con mayor frecuencia, a comparación del algoritmo AES que muestra un total de 4 en artículos analizados [6, 13, 26, 29] con un enfoque hacia el cifrado de datos, el análisis de datos que se envían entre remitente y receptor, y su importancia en la seguridad de la capa transporte. Además, el algoritmo K-MEANS es utilizado en 2 ocasiones [7, 21] donde presenta una temática de encontrar similitud entre el perfil del usuario y el grupo seleccionado, también se aplica para analizar patrones de comportamiento de usuarios al utilizar los canales de comunicación.

Por último, son 16 algoritmos que son utilizados con menor frecuencia a comparación con los demás, esta característica muestra una variedad en cuestión de algoritmos respecto al tipo de estudio.

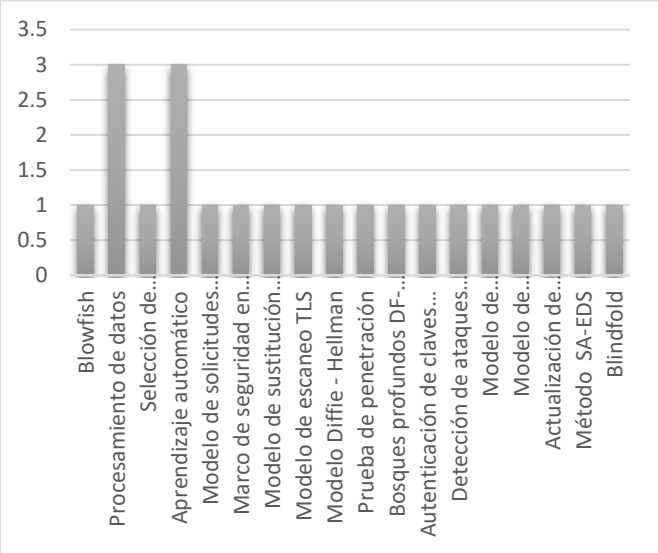

Fig. 6 Algoritmos utilizados en los estudios

Tras enfatizar los algoritmos utilizados de las investigaciones, también es importante mencionar la cantidad de citas que contiene cada estudio. Por ello, en la Fig. 7 se muestra el total de citas que tuvo dicha investigación en la base de datos Scopus, guiado por su ID extraído del formulario. A través de un gráfico de barras se obtuvo que la mayor frecuencia de citas fue en el estudio [8] con un total de 125, donde se muestra un modelo de privacidad y su algoritmo de implementación para evaluar los comportamientos de visualización por parte de los usuarios. Asu vez, los estudios [3], [9], [17], [21] se mantienen entre 5 a 8 citas, es decir, una cantidad estándar y aceptable.

Por otro lado, se aprecia que los estudios [2], [4], [5]. [6], [7], [10], [11], [13]. [14], [15], [16], [20], [22], [25], [26], [27], [28]. [29], [30], [32] no presentan frecuencia en cuestión de citados a comparación del resto, lo cual genera una ligera preocupación por no lograr un impacto oportuno en el área de investigación. Asimismo, existen 5 estudios [1], [19], [23], [24], [31] que al menos contienen una cita dentro del conteo.

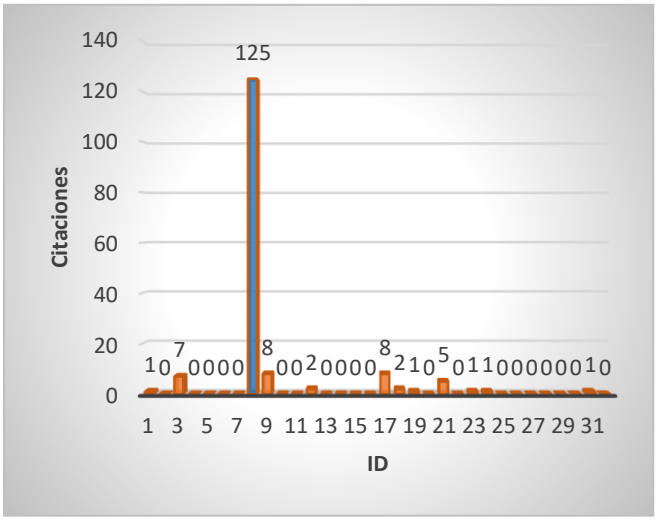

Fig. 7 Cantidad de citas por investigación

En la Fig. 8 se analiza mediante un gráfico de barras el origen de los estudios y la cantidad según su país. Los que más frecuentes son India, Italia, Polonia, Corea del Sur, China, Arabia Saudita, Bangladesh, Rusia y Egipto. Se identifica que el país de origen más recurrente es India con un total de 15 estudios [1], [3], [5], [7], [9], [10], [14], [15], [19], [22], [23], [24], [25], [30], [32], esto representa el 46.8% de los estudios tienen como país de origen a India.

También es importante destacar a China por contener 6 estudios, es decir el 18.7% del total. Además, de Italia, Corea del Sur, Arabia Saudita que se mantienen en un 6.25%.

Por último, están los países con menor recurrencia como Polonia, Bangladesh, Rusia, Egipto presentando un 3% de estudios publicados.

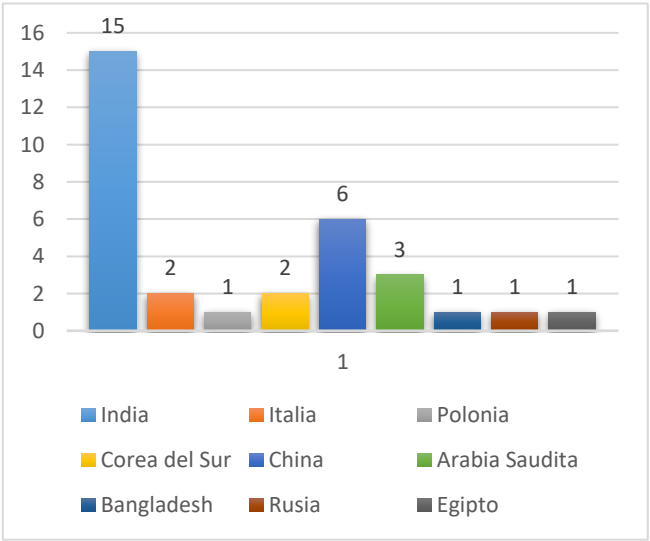

Fig. 8 Origen de estudios analizados

Luego, se tiene las Tablas VI y VII mostrando el resultado más representativo propuesto por los autores de cada investigación. Asimismo, para representar de una forma más compresible se añade el ID de su respectiva posición.

TABLA VI
RESULTADOS OBTENIDOS POR CADA INVESTIGACIÓN

RESULTADOS
La selección de características híbridas, junto con la verificación cruzada del análisis de correlación, proporciona detalles relacionados para la clasificación. [1]
La metodología aplicada explota las características de flujo y las características a nivel paquete, lo que permite que el modelo ML alcance un alto rendimiento cuando hay suficientes datos de entrenamiento disponibles. [2]
El examen de varios cálculos muestra que la naturaleza del modelo depende de la organización de claves, el tipo de criptografía y la cantidad de claves. Después del cifrado se puede decir que el algoritmo DES es más adecuado para cifrar 1KB de archivo y ARC4 para cifrar 1MB. [3]
Los códigos polares se han utilizado recientemente en las comunicaciones 5G, lo que los convierte en una mejor opción entre varios códigos de corrección de errores. [4]
Análisis y comparación de varios modelos para categorizar ataques en función de su efectividad para la detección de DDoS. [5]
Mejorar las soluciones PWS (búsqueda de web privada) criptográficas para reducir su complejidad de O(1) rondas. [6]
La aplicación del método K-Means para investigar la transmisión y su implementación utilizando Python y el conjunto de datos KDDcup99. [7]
Modelo de privacidad y su algoritmo de implementación para los comportamientos de visualización de productos del usuario. [8]
Detección temprana y eficiente de ataques distribuidos de denegación de servicio y su discriminación de flash crown, con el parámetro de tamaño de paquete y la dirección IP. [9]
Implementación de SOA en el comercio electrónico bajo los criterios y tecnologías de seguridad como TLS/SSL, XML. [10]
Análisis en sistemas existentes y aplicar la esteganografía de imagen (IS) basada en sustitución dinámica con una clave secreta. [11]
Monitoreo de seguridad que plantea la adopción generalizada de comunicaciones cifradas. [12]
Implementación y uso de TLS 1.3 desde su estandarización por parte del IETF. [13]
Revisión de cifrado Honey cuyo sistema garantiza flexibilidad frente al ataque de fuerza. [14]
Análisis del estado actual de la gestión de contraseñas de la aplicación web con el objetivo de detectar fallas e inseguridad en el sitio. [15]

TABLA VII
RESULTADOS OBTENIDOS POR CADA INVESTIGACIÓN

RESULTADOS
Implementación de un diseño de sistema de pruebas de penetración de seguridad web. [16]
Detectar ataques tipo DDoS se utiliza una red neuronal de creencia profunda para detectar con precisión DDoS desde la red. [17]
Método de detección basado en bosques profundos llamado DF-IDS, con el fin de descubrir tráfico malicioso cifrado con SSL/TLS. [18]
Protocolo de acuerdo de claves con EC-Diffie Hellman en el entorno SET para mejorar la seguridad. [19]
Técnica de red neuronal convucional (CNN) para detectar y clasificar el tráfico DDoS. [20]
Protocolo de preservación de la privacidad de búsqueda web de Profile Aware ObScure Logging (PaOsLo). [21]
Método para la detección de ataques DDoS en la computación en la nube. [22]
Método para la transformación homomórfica para hacerlo más exclusivo y adecuado para el cifrado de texto. [23]
Protocolo de autenticación para ataques internos basado en un algoritmo criptográfico robusto, ECC. [24]
Algoritmo de detección de ataques DDoS que utiliza una selección de características integrada heterogénea. [25]
Análisis de las diferencias entre las claves simétricas y asimétricas en el proceso de cifrado y descifrado. [26]
Espacio Web puede contener información necesaria para identificar y autenticar a los usuarios en internet. [27]
Análisis del método de gestión del tráfico que combina “punto final” y “tubería”. [28]
Análisis de diferentes técnicas de cifrado y protección de datos existentes basadas en los parámetros comunes. [29]
Diseño de un diagrama de flujo y un diseño conceptual de un mecanismo de llamada a una función hash. [30]
Diseño de Blindfold para proteger claves privadas en infraestructuras HTTPS/TLS. [31]
Descubrimiento de ataques en el aprendizaje automático a partir de datos de tráfico [32]

Posteriormente, la Fig. 9 muestra la frecuencia de palabras claves según su pertenencia a la revisión sistemática. La detección de ataques DDoS representa la mayor recurrencia en investigaciones enfocadas en la seguridad de datos con un total de 8, mientras que la criptografía es la segunda palabra clave más utilizada [7].

Si se compara estadísticamente, la detección de ataques DDoS representan el 16.6%, mientras que la criptografía muestra el 14.5% del total de palabras claves utilizadas.

Fig.9 Palabras claves más utilizadas

III. Discusión

En esta sección, se presenta un análisis exhaustivo de los resultados obtenidos en el presente estudio, con el objetivo de comprender su relevancia en el contexto de la investigación. Los datos recopilados y los análisis realizados nos ofrecen una visión detallada de la implementación de algoritmos simétricos estándar para la protección de datos y la discusión subsiguiente buscará interpretar estos resultados a la luz de los objetivos iniciales. Además, se exploran cómo estos hallazgos se alinean con la literatura existente, identificando similitudes, diferencias y contribuciones novedosas. A lo largo de este proceso, se destacarán las implicaciones prácticas y teóricas de los resultados, así como las limitaciones del estudio que deben tenerse en cuenta.

En este estudio de revisión, la optimización en los algoritmos de clasificación destinados a la anticipación de ataques de denegación de servicio distribuido (DDoS), como el refinamiento de variables críticas mejoró significativamente la precisión y eficiencia de los modelos de clasificación, fortaleciendo la capacidad predictiva del sistema según estudios [5] en comparación con el análisis hacia las características de los paquetes, el Algoritmo de Umbral dinámico detecta ataques DDoS explorando la IP destino y el tamaño del paquete, en este se calculan utilizando el valor medio de los atributos de red para detectar el ataque [9]. La diferencia entre estos dos estudios radica en la metodología aplicada, por un lado, se utiliza el procesamiento de datos a través de bibliotecas, mientras que en el segundo se evalúa atributos de red. La segunda aplicación resultó más eficiente tras expresar exactitud, precisión y sensibilidad. Con el método DARPA 98 se obtiene un 94,4% de detección y 99,5% de exactitud [9].

Por consiguiente, se introdujo una mejora significativa en la seguridad web, específicamente en la gestión de contraseñas basada en la nube, mediante la implementación de algoritmos criptográficos robustos como SHA-256 y Diffie-Hellman (DH) [15]. Con relación a este hallazgo, la técnica NKAP-ECDH-SET aprovecha el método de intercambio de claves Elliptic Curve Diffie-Hellman (ECDH) para garantizar una comunicación segura y confidencial entre los usuarios y el sistema. La inclusión de Secure Electronic Transaction (SET) refuerza aún más la seguridad, asegurando que las transacciones electrónicas y la autenticación del usuario se realicen de manera íntegra y protegida contra posibles amenazas [19]. Estos desarrollos representan una respuesta proactiva a las crecientes preocupaciones de seguridad en entornos digitales, incorporando tecnologías avanzadas para salvaguardar la integridad y confidencialidad de la información, así como para proteger las transacciones electrónicas y la autenticación de usuarios.

IV. Conclusiones

Se identificaron los algoritmos de encriptación estándar más utilizados y eficientes según su análisis. Se tiene AES, su utilización recalca la aplicación de escaneos TLS con el fin de obtener un enlace TLS para cada dominio alojado en su IP. El algoritmo de intercambio de claves Diffie- Hellman, obtuvo una mejora en la gestión de claves basadas en la nube con SHA-256 y DH. A su vez, el algoritmo criptográfico robusto señala la participación de tres entidades como la administración de contraseñas, proveedor de servicios y PC cliente. Los más eficientes al momento de ponerlos aprueba son el algoritmo criptográfico robusto, mostrando un 75% de efectividad en su diseño frente a ataques de seguridad. Un dato del algoritmo AES, resalta en su alta complejidad computacional, ya que se utilizan dos métodos criptográficos llevando así una mayor precisión.

El algoritmo de optimización de chimpancé (ChOA) detecta y alerta al usuario si se presenta un ataque. Los datos se suministran a un codificador automático, un codificador y un decodificador una vez que el conjunto de datos está libre de ataques o dificultades.

La utilización del aprendizaje automático enfocado en la detección de DDoS, en éste se extrae los conjuntos de datos CICIDS 2017 y CICDDoS 2019, luego pasa por un procesamiento de datos a través de los conjuntos. Después se aplica las técnicas de aprendizaje automático para la clasificación de ataques.

A futuros trabajos, se recomienda analizar la importancia y eficiencia de algoritmos simétricos estándar para la encriptación de datos debido a su alta variedad.

Para realizar el enfoque sobre el algoritmo a priori, se recomienda realizar una comparación entre la eficiencia y sus resultados post-implementación para determinar el más factible.

V. Agradecimiento

Expreso el sincero agradecimiento a todos aquellos que contribuyeron de manera significativa a la realización de esta revisión sistemática sobre la implementación de encriptación simétrica y tener la oportunidad de explorar y analizar los

desafíos de seguridad que enfrenta en el entorno digital. También agradecer a la Universidad Tecnológica del Perú a los profesores y asesores, cuya orientación y conocimientos han sido invaluables en la comprensión y aplicación de los conceptos relacionados con la encriptación de datos. Espero que este estudio contribuya al conocimiento en seguridad de la información y, a su vez, beneficie a empresas que buscan fortalecer su seguridad en el mundo digital.

REFERENCIAS

[1] U.S. Chanu, K.J. Singh and Y.J. Chanu, "A dynamic feature selection technique to detect DDoS attack", *Journal of Information Security and Applications*, vol. 74, March 2023.

[2] M. Trevisan, F. Soro, M. Mellia, I. Drago and R. Morla, "Attacking DoH and ECH: Does Server Name Encryption Protect Users' Privacy?", *ACM Transactions on Internet Technology*, vol. 23, no. 1, pp. 1-22, February 2023.

[3] S.S. Pronika, "Performance analysis of encryption and decryption algorithm", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 2, pp. 1030-1038, August 2021.

[4] A. Poniszewska-Maranda and K. Pradzynski, "Code-based encryption algorithms for generating and verifying digital signature" IEEE 21st International Conference on Trust, Security and Privacy in Computing and Communications, pp. 465-472, 2022.

[5] B. Geluvaraj, B.V. Santhosh, M. Umesh, G. Vishnu and Y. Yaqoob, "DDoS Attack Detection and Analytics" *International Conference for Advancement in Technology*, ICONAT 2023.

[6] M. Kim and I. Lee, "Taming the round efficiency of cryptographic protocols for private web search schemes", *Information Sciences*, vol. 621, pp. 1-21, April 2023.

[7] R. Shanker, P. Aggrawal, A. Singh and M. Bhatt, "Framework for identifying network attacks through packet inspection using machine learning", *Nonlinear Engineering*, vol. 12, no. 1, 2023.

[8] Z. Wu, S. Shen, H. Zhou, H. Li, C. Lu and D. Zou, "An effective approach for the protection of user commodity viewing privacy in e-commerce website", *Knowledge-Based Systems*, vol. 220, 2021

[9] J. David and C., Thomas, "Discriminating flash crowds from DDoS attacks using efficient thresholding algorithm", *Journal of Parallel and Distributed Computing*, vol. 152, pp. 79-87, 2021.

[10] K. Kumar and H. Gupta, "Designing a Security Framework for Enhancement of Electronic Transactions" [9th *International Conference on Reliability*, Infocom Technologies and Optimization, ICRITO 2021].

[11] K.A. Almalki., R. A. "Mohammed, Novel Steganography Approach to Embed Secret Information into a Legitimate URL" Proceedings of 2022 [2nd International Conference on Computing and Information Technology, ICCIT 2022, pp. 180-185].

[12] D. Canavese, L. Regano, C. Basile, G. Ciravegna and A. Lioy, "Encryption-agnostic classifiers of traffic originators and their application to anomaly detection", *Computers and Electrical Engineering*, vol. 97, 2022.

[13] Y. Guan, G. Gou, B. Wang, P. Fu and Z. Li, "A Large-Scale Privacy Measurement of Novel TLS 1.3 Protocol", *IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers*, [IPEC, pp. 867-872, 2022].

[14] T. Nirmalraj and J. Jebathangam, "A Novel Password Secure Mechanism using Reformation based Optimized Honey Encryption and Decryption Technique" Proceedings - 2022 [6th International Conference on Intelligent Computing and Control Systems, ICICCS 2022, pp. 877-880].

[15] P. Pandare, S. Uniyal, R. Vani, S. Mali and P. Rumao, "Enhanced Password Manager using Hybrid Approach" [6th International Conference on Inventive Computation Technologies, ICICT 2023, Proceedings, pp. 1793-1798]

[16] B. Song, L. Sun and Z. Qin "Design of Web Security Penetration Test System Based on Attack and Defense Game" Scientific Programming, 2022.

[17] A. Agrawal, R. Singh, M. Khari, S. Vimal and S. Lim, "Autoencoder for Design of Mitigation Model for DDOS Attacks via M-DBNN" *Wireless Communications and Mobile Computing*, 2022.

[18] G. He, Q. Wei, J. Wang, H. Zhu and B. Xu, "One-Shot Detection of Malicious TLS Traffic" [IEEE 25th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2022, pp. 145-150].

[19] N.M. Lingamgunta, S.G.N.A. Gubbala, "New Key Agreement Protocol and Cryptosystem over ECC under SET Protocol Environment in E-Commerce" *International Journal of Intelligent Engineering and Systems*, vol. 15 no. 4, pp. 319-328, 2022.

[20] M. A. Snigdho, S. Chowdhury and N. Jahan, "Real-Time DDoS Attack Prediction using Supervised Algorithms and CNN" [7th International Conference on Communication and Electronics Systems, ICCES 2022 - Proceedings, pp. 1342-1348].

[21] M. Ullah, R.U. Khan, I.U. Khan, N. Aslam, S.S. Aljameel, M.I. Haq and M.A. Islam, "Profile Aware ObScure Logging (PaOSLo): A Web Search Privacy-Preserving Protocol to Mitigate Digital Traces" Security and Communication Networks, 2022.

[22] R. Bhargava, Y. Pal and N.S. Narawade, "Implementation of Machine Learning Based DDOS Attack Detection System" [3rd International Conference for Emerging Technology, INCET 2022].

[23] A. Vishnoi, A. Aggarwal, A. Prasad, M. Prateek, S. Aggarwal, "Text encryption for lower bandwidth channels: Design and implementation", Proceedings of the 2022 [3rd International Conference on Intelligent Computing, Instrumentation and Control Technologies: Computational Intelligence for Smart Systems, ICICICT 2022, pp. 1460-1464].

[24] S. Akshara and G. Krishna, "Insider Attack Detection and Prevention using Server Authentication using Elgamal Encryption" [5th International *Conference on Inventive Computation Technologies*, ICICT 2022 - Proceedings, pp. 967-972].

[25] A. Ramesh, R. Haris, S. Arora, "ML based D3R: Detecting DDoS using Random Forest" Proceedings [23rd IEEE/ACM *International Symposium on Cluster, Cloud and Internet Computing Workshops*, CCGridW 2023, pp. 141-146, 2023].

[26] M. Althamir, A. Alabdulhay, M. M. Yasin, "A Systematic Literature Review on Symmetric and Asymmetric Encryption Comparison Key Size" Proceedings [3rd *International Conference on Smart Data Intelligence*, ICSMDI 2023, pp. 110-117].

[27] A.Y. Iskhakov, M.V. Mamchenko and S.P. Khripunov, "Enhanced User Authentication Algorithm Based on Behavioral Analytics in Web-Based Cyberphysical Systems" *International Russian Smart Industry Conference, Smart Industry Con*, pp. 253-258, 2023

[28] Y. Guan, Li and G. Xiong, "Research on Novel TLS Protocol Network Traffic Management and Monitoring Method" *ACM International Conference Proceeding Series*, pp. 89-94.

[29] Y. Ling, X. Li, D. Bin, C. Yang and J. Lu, J. "Web Random Token Generation Technology Based on Asymmetric Encryption Technology" [IEEE 2nd *International Conference on Electrical Engineering, Big Data and Algorithms*, EEBDA 2023, pp. 804-808, 2023].

[30] A. Vankadara, V. Myneni, H. Pendyala, and D. Vadlamudi, "Enhancing Encryption Mechanisms using SHA-512 for user Authentication through Password & Face Recognition" [6th *International Conference on Inventive Computation Technologies*, ICICT 2023 - Proceedings, pp. 1086-1095].

[31] H. Galal, M. Mannan and A. Youssef, "Blindfold: Keeping private keys in PKIs and CDNs out of sight" *Computers and Security*, vol. 118, 2023.

[32] S. Singh, M. Gupta and D. K. Sharma, "DDOS Attack Detection with Machine Learning: A Systematic Mapping of Literature" Proceedings - 5th International Conference on Smart Systems and Inventive Technology, pp. 939-945, 2023.