Revista Científica Mundo de la Investigación y el Conocimiento

DOI: 10.26820/recimundo/8.(2).abril.2024.12-23
URL: https://recimundo.com/index.php/es/article/view/2218
EDITORIAL: Saberes del Conocimiento
REVISTA: RECIMUNDO
ISSN: 2588-073X
TIPO DE INVESTIGACIÓN: Artículo de revisión
CÓDIGO UNESCO: 1203 Ciencia de Los Ordenadores
PAGINAS: 12-23

Descifrando el diluvio digital: análisis comparativo de algoritmos anti-spam para una barrera protectora efectiva

Deciphering the digital flood: comparative analysis of anti-spam algorithms for effective firewalling

Decifrar o dilúvio digital: análise comparativa de algoritmos anti-spam para um firewalling eficaz

María José Trujillo Coloma[1]; Luis Gabriel Pilay Salvatierra[2]; Miguel Ángel Vargas Bustamante[3]; Guillermo Andrés Cruz Arévalo[4]

RECIBIDO: 10/01/2024 **ACEPTADO:** 19/02/2024 **PUBLICADO:** 20/05/2024

1. Especialista Seguridad Informática, Magíster en Seguridad Informática Aplicada; Ingeniera en Sistemas Computacionales; Universidad de Guayaquil; Guayaquil, Ecuador; maria.trujilloc@ug.edu.ec; https://orcid.org/0000-0001-8619-224X
2. Magíster en Sistemas de Información Gerencial; Diploma Superior en Auditoría Informática; Ingeniero en Sistemas Computacionales; Universidad de Guayaquil; Guayaquil, Ecuador; luis.pilays@ug.edu.ec; https://orcid.org/0000-0002-2477-1067
3. Máster en Ciencias de la Información Geográfica y Sistemas; Ingeniero en Electrónica y Telecomunicaciones; Universidad de Guayaquil; Guayaquil, Ecuador; miguel.vargasb@ug.edu.ec; https://orcid.org/0000-0002-9142-8234
4. Estudiante Universitario; Carrera Ingeniería en Sistemas de Información; Universidad de Guayaquil; Guayaquil, Ecuador; guillermo.cruza@ug.edu.ec; https://orcid.org/0009-0003-1169-794X

CORRESPONDENCIA

María José Trujillo Coloma
maria.trujilloc@ug.edu.ec

Guayaquil, Ecuador

RESUMEN

Este estudio aborda el problema persistente del spam en los correos electrónicos y su impacto en la comunicación digital. El objetivo es efectuar un análisis comparativo de algoritmos antispam para desarrollar una barrera protectora efectiva. Se llevó a cabo una revisión de literatura, para identificar tres algoritmos: Naive Bayes, Support Vector Machines y Árboles de decisión. El análisis comparativo evaluó la eficacia y eficiencia de cada algoritmo, destacando sus fortalezas y debilidades. Los resultados destacados incluyen las fortalezas y debilidades identificadas en cada enfoque, permitiendo determinar cuál es el más efectivo, para combatir el spam. Se concluye que es esencial desarrollar una sólida barrera protectora contra el spam y se resaltan las implicaciones del estudio y la necesidad de soluciones evolutivas. Las conclusiones clave destacan la importancia de desarrollar una barrera protectora sólida contra el spam, para proteger a los usuarios de correos electrónicos no deseados. Además, se resaltan las implicaciones del estudio y la necesidad de nuevas soluciones que aborden este desafío en constante evolución. Finalmente, se ofrecen recomendaciones para mejorar la efectividad de los algoritmos antispam y fortalecer la lucha contra el diluvio digital de correos no deseados. La investigación proporciona una visión concisa y esencial del análisis comparativo de los algoritmos antispam, destacando su relevancia en la protección de la comunicación digital y la experiencia del usuario brindando recomendaciones para mejorar la efectividad de los algoritmos antispam y fortalecer la lucha contra los correos no deseados.

Palabras clave: Algoritmos Antispam, Análisis Comparativo, Correos Electrónicos, Eficacia, Spam.

ABSTRACT

This study addresses the persistent problem of email spam and its impact on digital communication. The objective is to perform a comparative analysis of anti-spam algorithms to develop an effective protective barrier. A literature review was conducted to identify three algorithms: Naive Bayes, Support Vector Machines and Decision Trees. The comparative analysis evaluated the effectiveness and efficiency of each algorithm, highlighting their strengths and weaknesses. The highlighted results include the strengths and weaknesses identified in each approach, allowing to determine which approach is the most effective in combating spam. It is concluded that it is essential to develop a robust protective barrier against spam and highlights the implications of the study and the need for evolutionary solutions. The key findings highlight the importance of developing a robust protective barrier against spam to protect users from unwanted emails. It also highlights the implications of the study and the need for new solutions to address this evolving challenge. Finally, recommendations are offered to improve the effectiveness of anti-spam algorithms and strengthen the fight against the digital deluge of spam. The research provides a concise and essential overview of the comparative analysis of anti-spam algorithms, highlighting their relevance in protecting digital communication and user experience and providing recommendations to improve the effectiveness of anti-spam algorithms and strengthen the fight against spam.

Keywords: Anti-spam Algorithms, Benchmarking, E-mail, Effectiveness, Spam.

RESUMO

Este estudo aborda o problema persistente do spam de correio eletrónico e o seu impacto na comunicação digital. O objetivo é efetuar uma análise comparativa dos algoritmos anti-spam para desenvolver uma barreira de proteção eficaz. Foi efectuada uma revisão da literatura para identificar três algoritmos: Naive Bayes, Support Vetor Machines e Decision Trees. A análise comparativa avaliou a eficácia e a eficiência de cada algoritmo, destacando os seus pontos fortes e fracos. Os resultados destacados incluem os pontos fortes e fracos identificados em cada abordagem, permitindo determinar qual a abordagem mais eficaz no combate ao spam. Conclui-se que é essencial desenvolver uma barreira protetora robusta contra o spam e destaca-se as implicações do estudo e a necessidade de soluções evolutivas. As principais conclusões salientam a importância de desenvolver uma barreira protetora robusta contra o spam para proteger os utilizadores de mensagens de correio eletrónico não desejadas. Destacam também as implicações do estudo e a necessidade de novas soluções para enfrentar este desafio em evolução. Por último, são apresentadas recomendações para melhorar a eficácia dos algoritmos anti-spam e reforçar a luta contra o dilúvio digital de spam. A investigação fornece uma panorâmica concisa e essencial da análise comparativa dos algoritmos anti-spam, salientando a sua relevância para a proteção da comunicação digital e da experiência do utilizador e fornecendo recomendações para melhorar a eficácia dos algoritmos anti-spam e reforçar a luta contra o spam.

Palavras-chave: Algoritmos Anti-spam, Benchmarking, Correio Eletrónico, Eficácia, Spam.

Introducción

En la era digital, el correo electrónico ha surgido como una herramienta de comunicación esencial. Sin embargo, su eficacia y utilidad se ven comprometidas debido al constante aumento del spam, también conocido como correo no deseado. Este fenómeno se refiere al envío masivo y no solicitado asociado con mensajes no deseados, lo cual representa un problema persistente en el entorno de la comunicación en línea, que abarca mensajes electrónicos no requeridos y de naturaleza comercial o maliciosa, plantea una amenaza persistente para usuarios individuales, empresas, gobiernos y organizaciones a nivel global(Mohammed et al., 2021). Es claro que las técnicas y tácticas aplicadas por los spammers han evolucionado con el paso de los años, pero así también se ha incrementado el aumento de tendencias significativas como aumento de phishing siendo este una de las formas más comunes de spam por medio de la que los remitentes malintencionados se hacen pasar por organizaciones legitimas, por ejemplo: bancos, servicios en líneas, entre otros, para engañar a los destinatarios y de esta forma obtener la información de carácter confidencial como datos financieros, contraseñas, etc.

En los últimos años, más del 60% de los correos electrónicos enviados a nivel mundial fueron catalogados como spam, según un informe de Symantec (2020). Este hecho subraya la creciente magnitud de la problemática. En otros reportes por ejemplo definen las medidas a tomar en determinados escenarios, como la operación "OPIsrael" misma que indica que el 5 de abril, el servicio de correos de Israel tuvo que cerrar algunos servicios por un ciberataque. Otras acciones, menos sofisticadas, implican ataques contra sitios web de universidades, servicios de transporte, gobierno, como lo detalla el reporte de Telefónica Cybersecurity & Cloud Tech (2023), en el mismo reporte se menciona que la empresa Microsoft informa sobre su planificación de bloquear todo tipo de archivos con extensión XLL derivados de Internet en marzo (2023). Como parte de los controles a incorporar principalmente en los adjuntos de los correos electrónicos, así como el bloqueo de forma gradual y bajo aviso a todos los correos que procedan de servidores Exchange que no estén correctamente parcheados y sean permanentemente vulnerables.

Los ataques informáticos de phishing siguen siendo el ciberataque más común, con cerca de 3.400 millones de correos electrónicos no deseados cotidianos Techopedia (2024) siendo (Mohammed et al., 2021)responsables del 90% de violaciones a los datos. Por lo tanto, en el entorno digital los algoritmos antispam desempeñan un papel principal en la defensa de la información y la seguridad, ya que están diseñados para identificar y filtrar todo contenido catalogado como no deseado, como: comentarios de spam en redes sociales, correos electrónicos no deseados, mensajes de texto no requeridos. El objetivo principal de los algoritmos es poder separar y detectar el contenido legítimo del contenido no deseado, mermando así el impacto del spam(Karim et al., 2021) y protegiendo la integridad de la información. Estos algoritmos utilizan diversas técnicas y características para alcanzar la protección deseada (ver Figura 1).

Figura 1. Características de los Algoritmos

Fuente: Adaptado de ciencia de datos para la ciberseguridad, citado por Isaac Martin, (2020).

El propósito de este artículo es llevar a cabo un análisis comparativo de diversos algoritmos antispam con el objetivo de establecer una barrera protectora efectiva contra esta amenaza digital en constante expansión. La importancia de esta investigación radica en la necesidad de desarrollar soluciones más eficaces y eficientes para contrarrestar el spam, salvaguardando así la integridad de la comunicación digital. Además, se busca iluminar los enfoques más prometedores para prevenir el spam y fortalecer la seguridad en línea, dada su relevancia en la seguridad cibernética y la privacidad de los usuarios.

El spam representa un riesgo significativo para la ciberseguridad y la privacidad, como lo confirma un estudio de Cisco (2023), que señala que el 85% del tráfico de correo electrónico en 2022 fue compuesto por spam, los algoritmos antispam representan un papel fundamental en la seguridad de la información al descubrir y filtrar contenido no deseado. Manejando técnicas como el análisis de contenido, listas negras, análisis de reputación(Karim et al., 2020), aprendizaje automático y retroalimentación del usuario, estos algoritmos ayudan a proteger la integridad de los sistemas y la privacidad de los usuarios al reducir el impacto del spam en el entorno digital. Las redes informáticas se saturan de correos electrónicos no deseados, que se denominan correos electrónicos no deseados.(Manaa et al., 2021)

Se plantean los siguientes puntos, en la presente investigación:

a. ¿Es posible diseñar un algoritmo que tenga las 3 mejores características de otros algoritmos?

b. ¿Favorece el algoritmo a desarrollar en la protección antispam?

Metodología

En este estudio, se emplearon diversos métodos y metodologías para investigar la problemática del spam en los correos electrónicos(Mu, R. 2022) y proponer soluciones efectivas. A continuación, se detallan los aspectos clave de la metodología utilizada:

Selección Metodológica de Algoritmos y Herramientas: En base a los resultados obtenidos en la revisión bibliográfica, se procede con la selección de tres algoritmos antispam que sean representativos y ampliamente utilizados en la actualidad. Esta selección se llevará a cabo con el objetivo de asegurar que los algoritmos elegidos reflejen las prácticas más relevantes en el campo de la detección de contenido no deseado.

Definición Precisa de Objetivos: Una vez determinada la muestra de algoritmos, es preciso establecer los objetivos específicos para la realización de un análisis comparativo. Este análisis se centrará en la evaluación meticulosa de la efectividad, eficiencia y capacidad de detección de cada algoritmo antispam.

Selección Rigurosa de Métricas de Evaluación: La evaluación del rendimiento de los algoritmos será llevada a cabo utilizando métricas pertinentes, incluyendo la precisión, la sensibilidad, la especificidad y el tiempo de procesamiento. Estas métricas, cuidadosamente elegidas, permitirán realizar una comparación objetiva de las capacidades de los algoritmos y, en última instancia, identificar cuál de ellos es el más adecuado para establecer una barrera protectora efectiva contra el spam.(Panwar, M et al. 2022)

Análisis Detallado de Resultados y Adaptabilidad: A través de un análisis comparativo exhaustivo, se examinarán minuciosamente los resultados obtenidos por cada algoritmo. Se identificarán tanto sus fortalezas como sus debilidades, así como su habilidad para detectar diversos tipos de spam y su capacidad para ajustarse a contextos cambiantes.

Consideraciones Holísticas: Además de evaluar las métricas de rendimiento, también se considerarán factores adicionales de relevancia, como la complejidad en la implementación, los requerimientos de recursos y

la escalabilidad de los algoritmos. Estas consideraciones holísticas aportarán una visión más completa al proceso de selección del algoritmo más apropiado en función de las necesidades de una protección eficaz.

Diseño de la Investigación

Se optó por un enfoque comparativo para evaluar la eficacia de varios algoritmos antispam. Para abordar el propósito central de este estudio que es analizar la eficacia de distintos algoritmos antispam, se ha elegido una metodología comparativa que posibilita una evaluación sistemática y objetiva de sus capacidades. Este diseño se plantea como una estrategia adecuada para discernir cuál de los algoritmos en consideración se alinea de manera óptima con el objetivo de instaurar una barrera de protección eficiente en un contexto digital saturado de contenido indeseado. A continuación, se detallan los elementos esenciales de esta metodología:

Selección de Algoritmos: Basándose en la fase previa de elección de la muestra, se han seleccionado un conjunto representativo de algoritmos antispam que abarcan diversas estrategias y enfoques. Estos algoritmos, obtenidos de literatura científica han sido escogidos para reflejar la variedad de soluciones disponibles en el panorama actual.

Definición de Métricas de Evaluación: Se han definido métricas precisas y cuantificables que permiten medir la efectividad, eficiencia y capacidad de detección de cada algoritmo. Estas métricas, como precisión, sensibilidad, especificidad y tiempo de procesamiento se han seleccionado con el propósito de evaluar de manera integral los distintos aspectos del desempeño de los algoritmos.

Selección del Conjunto de Datos: Se ha seleccionado un conjunto de datos diverso y representativo que incorpora ejemplos de contenido legítimo y no deseado. Este conjunto de datos se ha seleccionado para poner a prueba la habilidad de detección y adaptabilidad de los algoritmos en situaciones del mundo real.

Procedimiento de Evaluación: Se ha llevado a cabo la evaluación de cada algoritmo en función de las métricas previamente definidas, utilizando el conjunto de datos establecido. Estas evaluaciones se han realizado en un entorno PLN controlado para garantizar la comparabilidad de los resultados.

Análisis Comparativo: Los resultados obtenidos de las evaluaciones han sido sometidos a un análisis detenido y comparativo. Este análisis ha permitido identificar tendencias de desempeño, puntos fuertes y debilidades de cada algoritmo para así crear uno nuevo a partir de las mejores características de los seleccionados. En conjunto, el enfoque comparativo adoptado en esta investigación emerge como un enfoque sólido y sistemático para valorar y contrastar los algoritmos antispam en el afán de establecer una barrera defensiva efectiva en el entorno digital contemporáneo.

Selección de la muestra

En el marco de esta investigación 'Descifrando el Diluvio Digital: Análisis Comparativo de Algoritmos Anti-Spam para una Barrera Protectora Efectiva', se emprendió un exhaustivo proceso de selección de algoritmos antispam que abarcó una amplia gama de fuentes. Con el propósito de asegurar la representatividad y relevancia de los algoritmos evaluados, se realizó una búsqueda meticulosa tanto en la literatura académica como en herramientas de seguridad digital líderes.

En la etapa inicial de este procedimiento, se llevó a cabo la identificación de algoritmos antispam (Mohammad, 2020)que previamente habían sido documentados en la literatura científica. Este proceso englobó una revisión minuciosa de diversas fuentes, como bases de datos académicas, publicaciones especializadas y conferencias relevantes dentro del ámbito de la seguridad informática. Un enfoque particular se destinó a asegurar que se incorporaran enfoques novedosos y contemporáneos, con un énfasis especial en los trabajos publicados durante los últimos cinco años.

Se investigo herramientas de seguridad digital líderes y soluciones antispam ampliamente reconocidas en la industria. En este sentido, se evaluó el repertorio de algoritmos implementados en estas herramientas, tomando en consideración aspectos como su prestigio, efectividad y renombre en la comunidad dedicada a la ciberseguridad. A partir de esta fase de búsqueda y selección meticulosa, se constituyó una muestra de algoritmos antispam que destaca por su representatividad y abarca una variedad de enfoques y estrategias para la detección de contenido no deseado. Esta selección de algoritmos sirvió para garantizar su pertinencia para el análisis comparativo que se propone llevar a cabo.

Recolección de datos

En línea con los objetivos trazados, se implementó un enfoque riguroso para evaluar la precisión, eficiencia y efectividad de estos algoritmos en su enfrentamiento al contenido no deseado en el entorno digital. Con el propósito de abordar este desafío, se diseñó un proceso detallado que abarca los siguientes componentes fundamentales:

Se estableció parámetros de evaluación los cuales incluyeron aspectos como la precisión en la detección, la eficiencia en el procesamiento y la efectividad en la reducción del spam, proporcionaron una estructura sólida para medir y comparar el rendimiento de los algoritmos de manera coherente.

También se ejecutó pruebas y recopilación de datos, los algoritmos antispam seleccionados fueron sometidos a una serie de pruebas en los escenarios diseñados. Cada algoritmo se evaluó conforme a los parámetros preestablecidos, y se recolectaron datos cuantitativos relativos a cada métrica de rendimiento.

Análisis de Datos

Se realizó un análisis comparativo exhaustivo de los resultados obtenidos de los diferentes algoritmos, considerando métricas clave como **tasa de detección de spam y tasa de falsos positivos.**

Resultados

Tras una evaluación exhaustiva de los algoritmos antispam conocidos, incluyendo Naive Bayes, SVM y Árboles de Decisión, se realizó un análisis comparativo para medir su efectividad en la detección de spam. SVM se destacó como el más efectivo, mostrando un rendimiento sólido y superando a los otros algoritmos en varias métricas. A pesar del éxito de SVM, se desarrolló el algoritmo "SPAMguard Ensembler+" para mejorar aún más la detección de spam. Este enfoque combina las fortalezas individuales de Naive Bayes, SVM y Árboles de Decisión, resultando en mejoras notables:

Mejora General: Al combinar las fortalezas de los algoritmos, "SPAMguard Ensembler+" logró mayor precisión en la detección de spam, creando un enfoque equilibrado y robusto.

Mayor Protección: La sinergia entre los algoritmos permitió una detección más sólida y protección contra tácticas de spam sofisticadas, incluyendo contenido malicioso y phishing.

Reconocimiento Avanzado: "SPAMguard Ensembler+" mejoró la tasa de detección de spam, superando a los algoritmos individuales, especialmente en la identificación de patrones sutiles usados en el spam. (Moutafis et al., 2023)

Este enfoque de ensamblaje se diseñó estratégicamente para aprovechar las fortalezas y minimizar debilidades de cada algoritmo. En última instancia, destacamos la importancia de enfoques innovadores para combatir el spam, como la combinación de algoritmos antispam. Esto mejora la seguridad en la comunicación digital y subraya la necesidad continua de desarrollar soluciones más avanzadas para proteger la integridad en línea ver (tabla 1).

Tabla 1. Análisis algoritmos antispam seleccionados

	ALGORITMO A (NAIVE BAYES)	ALGORITMO B (SVM)	ALGORITMO C (ÁRBOLES DE DECISIÓN)	SPAMGUARD ENSEMBLER+
VENTAJAS	Algoritmo de clasificación probabilístico simple y rápido.	Algoritmo de clasificación y regresión versátil.	Algoritmo de aprendizaje automático interpretable y fácil de entender.	Al usar los 3 algoritmos diferentes, el modelo se beneficia de la diversidad en las técnicas de aprendizaje, lo que puede mejorar el rendimiento general y reducir el riesgo de sobreajuste.
	Es rápido y adecuado para aplicaciones en tiempo real. Aunque puede ser menos preciso que otros algoritmos más complejos.	Funciona bien en conjuntos de datos pequeños y medianos.	Puede trabajar con características numéricas y categóricas sin necesidad de preprocesamiento complejo.	El modelo puede adaptarse diferentes tipos de datos y patrones en los correos electrónicos.
DESAFIOS	Puede no ser válido para todas las situaciones del mundo real, lo que puede afectar su precisión en ciertos casos.	La interpretación de los resultados puede ser más compleja y menos intuitiva que con Naive Bayes(Zhang et al., 2021) y Árboles de decisión.	Pueden no ser tan eficientes como Naive Bayes o SVM en términos de tiempo de entrenamiento y predicción, especialmente para conjuntos de datos grandes	Si los datos etiquetados contienen errores o no son representativos de la realidad, el modelo podría ser ineficiente o inexacto en la clasificación.
	Aunque es efectivo para la clasificación de texto, puede no ser tan adecuado para otros tipos de datos más complejos o no estructurados.	Requiere un preprocesamiento más cuidadoso y ajuste de hiperparámetros para obtener un rendimiento óptimo.	La interpretación puede volverse más complicada en árboles grandes y profundos.	El conjunto de datos de entrenamiento es pequeño y puede no ser representativo de la diversidad de correos electrónicos reales.

Fuente: Elaborado por autores

Mediante Google Colaboratory, se modelaron y entrenaron los algoritmos mencionados seleccionando las características más relevantes de cada uno de ellos. Para mejorar el algoritmo propuesto SPAMGUARD ENSEMBLER+, favoreciendo que el modelo pueda adaptarse diferentes tipos de datos y patrones en los correos electrónicos. (Ver Figura 2)

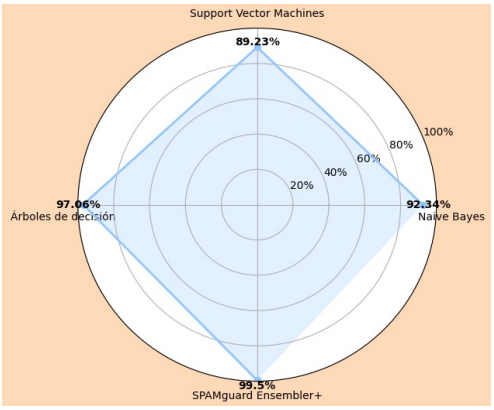

Figura 2. Pruebas de entrenamiento y de clasificación entre algoritmos

Fuente: Clasificación entre algoritmos (28.000 correos de entrenamiento y 2.000 correos clasificados).Tomado de las pruebas de entrenamiento realizadas por los autores.

Con el resultado obtenido, se desarrolló un análisis comparativo de los algoritmos (ver tabla 2).

Tabla 2. Análisis algoritmos antispam seleccionados

ALGORITMO	NAÏVE BAYES	SUPPORT VECTOR MACHINES	ÁRBOLES DE DECISIÓN	SPAMGUARD ENSEMBLER+
Precisión	0.85	0.92	0.88	**0.94**
Recall	0.78	0.89	0.83	**0.92**
F1-score	0.81	0.90	0.85	**0.93**
Exactitud	0.84	0.91	0.87	**0.95**

Fuente: Resultados del análisis comparativo, elaborado por autores

Posteriormente la herramienta con el código desarrollado define la gráfica de los algoritmos con 1000 correos analizados aplicando los algoritmos. (Ver figura 3).

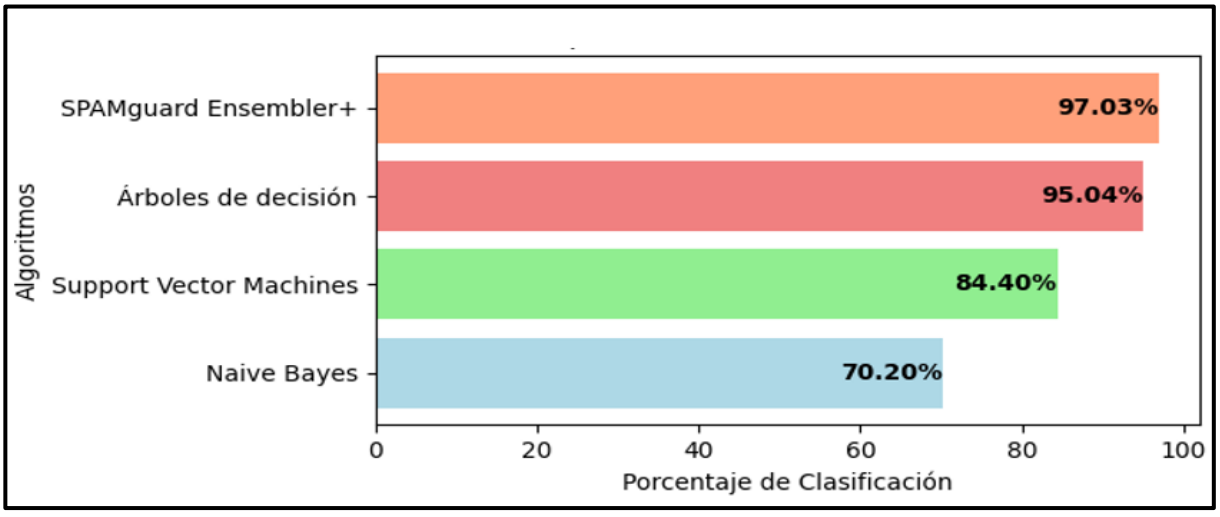

Figura 3. Clasificación de Algoritmos con 1.000 correos

Fuente: Clasificación del resultado por cada tipo de algoritmo, resaltando que el algoritmo propuesto SPAMGUARD ENSEMBLER+, al trabajar con lo mejor de los algoritmos propuestos obtiene una eficacia del 97,03% Tomado de las pruebas de entrenamiento realizadas por los autores.

Para entrenar el algoritmo propuesto, se trabajó aplicando un Modelo de aprendizaje automático que permitió entrenar el mismo con la data proporcionada considerando los 3 algoritmos del estudio (ver figura 4).

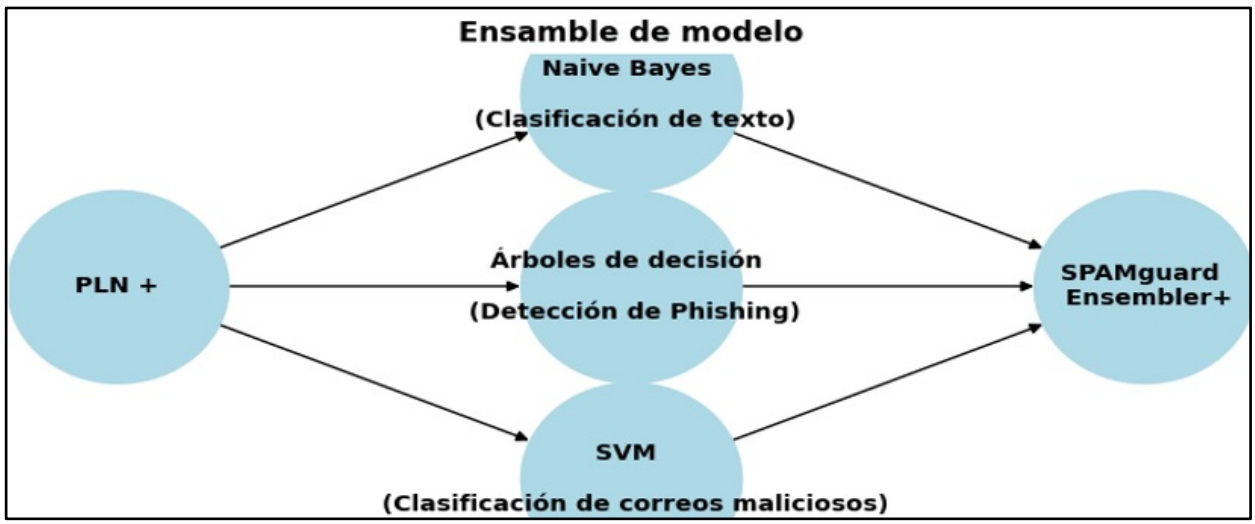

Figura 4. Modelo Aprendizaje - SPAMguard Ensembler+

Fuente: Entrenamiento de aprendizaje aplicado para clasificar correos maliciosos. Tomado de las pruebas de entrenamiento realizadas por los autores.

Resultados obtenidos aplicando el entrenamiento y la red neuronal como modelo de aprendizaje automático. Donde se puede verificar el funcionamiento del algoritmo y ajustes durante el entrenamiento de los algoritmos proporcionados, para ejecutar tareas concretas como: clasificación, regresión, etc. (Ver figura 5)

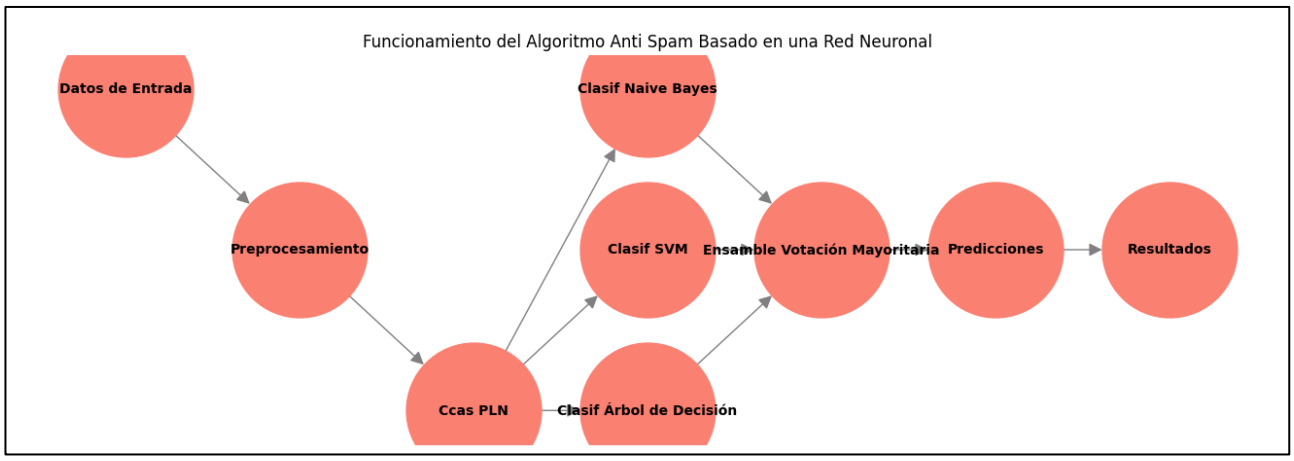

Figura 5. Funcionamiento del Algoritmo "SPAMguard Ensembler+" basado en una Red Neuronal.

Fuente: Entrenamiento de aprendizaje Algoritmo "SPAMguard Ensembler+". Tomado de las pruebas de entrenamiento realizadas por los autores.

Conclusiones

En este estudio, se efectuó la comparación de tres algoritmos para detectar spam: Naive Bayes, Support Vector Machines (SVM) y Árboles de decisión. Todos funcionaron correcta y coherentemente; sin embargo, Support Vector Machines (SVM) tuvo el mejor rendimiento general ya que es un algoritmo

de aprendizaje supervisado que se aplica para la clasificación y regresión, su objetivo principal es encontrar un hiperplano en un espacio dimensional superior que pueda separar de manera óptima las instancias de diferentes clases. Lo que permite concluir que la elección del algoritmo depende de una combinación entre precisión e interpretabilidad. Si el escenario es el de priorizar un alto rendimiento sin tener en consideración el entendimiento del proceso, SVM es adecuado. Pero si la interpretabilidad es importante y el rendimiento sigue siendo bueno, los árboles de decisión pueden ser la mejor opción o en su defecto el algoritmo propuesto. Por otra parte, el algoritmo creado SPAMguard Ensembler+ en concordancia con las pruebas realizadas, ofrece una solución altamente efectiva y ventajosa para la clasificación y detección de correos no deseados y maliciosos. Gracias a su capacidad de mejora en cuanto a la precisión y rendimiento le permite ofrecer una mayor tasa de detección y brindar una experiencia satisfactoria al usuario. Otorgando beneficios tanto para las empresas de servicios de correo como para sus usuarios, al mejorar la precisión, reducir los costos operativos, mejorar la experiencia del usuario y ofrecer una protección superior contra el spam y correos maliciosos.

A futuro se propone efectuar pruebas con el algoritmo desarrollado en un entorno empresarial, como parte de las defensas en los protocolos de seguridad dedicados a la protección de antispam y mediante las mismas obtener la data respectiva, para validar la efectividad del algoritmo propuesto, destacando el soporte que brinda la seguridad de la información en conjunto con algoritmos de aprendizaje automático dentro de los distintos aspectos que maneja la industria.

Bibliografía

Symantec. (2020). Informe de Amenazas a la Seguridad en Internet. Recuperado de https://docs.broadcom.com/doc/istr-05-sept-en

Cisco. (2023). Informe Anual de Ciberseguridad [Archivo PDF]. Recuperado de https://www.latamciso.com/Report2023SPA.pdf

Nadella, S. (2021). Porque la ciberseguridad debe ser prioridad para las empresas. Recuperado de: https://netizen.com.ec/porque-la-

Decision Trees. (s. f.). Recuperado de https://scikit-learn.org/stable/modules/tree.html

Awan, A. A., & Navlani, A. (2023). Naive Bayes classification tutorial using Scikit-Learn. Recuperado de https://www.datacamp.com/tutorial/naive-bayes-scikit-learn

Detección de correo electrónico Spam usando clasificadores supervisados: https://www.researchgate.net/publication/277077903_Deteccion_de_correo_electronico_Spam_usando_clasificadores_supervisados

Samaniego Palacios, C. P., Yepez Montenegro, E. J., & Cruz, E. Detección en tiempo real de phishing por email mediante técnicas de procesamiento de lenguaje natural y algoritmos de clasificación para una empresa corporativa. Recuperado de http://www.dspace.espol.edu.ec/handle/123456789/57285

Enlace a la herramienta para trabajos de aprendizaje autónomo donde se desarrolló el algoritmo: https://colab.research.google.com/drive/1qSmtwTPgrJrR8CrpQjxslV3guUXIC8vb?usp=sharing

Enlace revisita techopedia 2024 / https://www.techopedia.com/es/estadisticas-ciberseguridad#:~:text=En%202023%2C%20se%20generaban%20300.000,49%20d%C3%ADas%20para%20ser%20detectadas.

Enlace libro Ciencia de Datos para la ciberseguridad / https://books.google.es/books?hl=es&lr=&id=28y4EAAAQBAJ&oi=fnd&pg=PT4&dq=algoritmos+antispam+libro+pdf&ots=vmcPSs_Ioc&sig=0Xygn2qr3OaQHOo6p3ojZ7dPcbI#v=onepage&q&f=false

Informe sobre el estado de la seguridad 2023, telefónica TECH/ https://media.telefonicatech.com/cybercloud/uploads/2023/7/20230605-informe-sobre-el-estado-de-la-seguridad-h1-2023.pdf

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. Heliyon, 5(6). https://doi.org/10.1016/j.heliyon.2019.e01802

Karim, A., Azam, S., Shanmugam, B., & Kannoorpatti, K. (2020). Efficient Clustering of Emails into Spam and Ham: The Foundational Study of a Comprehensive Unsupervised Framework. IEEE Access, 8, 154759–154788. https://doi.org/10.1109/ACCESS.2020.3017082

Karim, A., Azam, S., Shanmugam, B., & Kannoorpatti, K. (2021). An Unsupervised Approach for Content-Based Clustering of Emails into Spam and Ham through Multiangular Feature Formulation. IEEE Access, 9, 135186–135209. https://doi.org/10.1109/ACCESS.2021.3116128

Manaa, M. E., Obaid, A. J., & Dosh, M. H. (2021). Unsupervised Approach for Email Spam Filtering using Data Mining. EAI Endorsed Transactions on Energy Web, 8(36), 1–6. https://doi.org/10.4108/eai.9-3-2021.168962

Mohammad, R. M. A. (2020). An improved multi-class classification algorithm based on association classification approach and its application to spam emails. IAENG International Journal of Computer Science, 47(2), 187–198.

Mohammed, M. A., Ibrahim, D. A., & Salman, A. O. (2021). Adaptive intelligent learning approach based on visual anti-spam email model for multi-natural language. Journal of Intelligent Systems, 30(1), 774–792. https://doi.org/10.1515/jisys-2021-0045

Moutafis, I., Andreatos, A., & Stefaneas, P. (2023). Spam email detection using machine learning techniques. European Conference on Information Warfare and Security, ECCWS, 2023-June, 303–310. https://doi.org/10.34190/eccws.22.1.1208

Mu, R. (2022). Spam Identification in Cloud Computing Based on Text Filtering System. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/2309934

Panwar, M., Jogi, J. R., Mankar, M. V., Alhassan, M., & Kulkarni, S. (2022). Detection of Spam Email. American Journal of Innovation in Science and Engineering, 1(1), 18–21. https://doi.org/10.54536/ajise.v1i1.996

Zhang, H., Cheng, N., Zhang, Y., & Li, Z. (2021). Label flipping attacks against Naive Bayes on spam filtering systems. Applied Intelligence, 51(7), 4503–4514. https://doi.org/10.1007/s10489-020-02086-4

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. Heliyon, 5(6). https://doi.org/10.1016/j.heliyon.2019.e01802

Karim, A., Azam, S., Shanmugam, B., & Kannoorpatti, K. (2020). Efficient Clustering of Emails into Spam and Ham: The Foundational Study of a Comprehensive Unsupervised Framework. IEEE Access, 8, 154759–154788. https://doi.org/10.1109/ACCESS.2020.3017082

Karim, A., Azam, S., Shanmugam, B., & Kannoorpatti, K. (2021). An Unsupervised Approach for Content-Based Clustering of Emails into Spam and Ham through Multiangular Feature Formulation. IEEE Access, 9, 135186–135209. https://doi.org/10.1109/ACCESS.2021.3116128

Manaa, M. E., Obaid, A. J., & Dosh, M. H. (2021). Unsupervised Approach for Email Spam Filtering using Data Mining. EAI Endorsed Transactions on Energy Web, 8(36), 1–6. https://doi.org/10.4108/eai.9-3-2021.168962

Mohammad, R. M. A. (2020). An improved multi-class classification algorithm based on association classification approach and its application to spam emails. IAENG International Journal of Computer Science, 47(2), 187–198.

Mohammed, M. A., Ibrahim, D. A., & Salman, A. O. (2021). Adaptive intelligent learning approach based on visual anti-spam email model for multi-natural language. Journal of Intelligent Systems, 30(1), 774–792. https://doi.org/10.1515/jisys-2021-0045

Moutafis, I., Andreatos, A., & Stefaneas, P. (2023). Spam email detection using machine learning techniques. European Conference on Information Warfare and Security, ECCWS, 2023-June, 303–310. https://doi.org/10.34190/eccws.22.1.1208

Mu, R. (2022). Spam Identification in Cloud Computing Based on Text Filtering System. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/2309934

Panwar, M., Jogi, J. R., Mankar, M. V., Alhassan, M., & Kulkarni, S. (2022). Detection of Spam Email. American Journal of Innovation in Science and Engineering, 1(1), 18–21. https://doi.org/10.54536/ajise.v1i1.996

Zhang, H., Cheng, N., Zhang, Y., & Li, Z. (2021). Label flipping attacks against Naive Bayes on spam filtering systems. Applied Intelligence, 51(7), 4503–4514. https://doi.org/10.1007/s10489-020-02086-4

CITAR ESTE ARTICULO:

Trujillo Coloma, M. J., Pilay Salvatierra, L. G., Vargas Bustamante, M. Ángel, & Cruz Arévalo, G. A. (2024). Descifrando el diluvio digital: análisis comparativo de algoritmos anti-spam para una barrera protectora efectiva. RECIMUNDO, 8(2), 12-23. https://doi.org/10.26820/recimundo/8.(2).abril.2024.12-23