CAPTCHA en la Era de la Inteligencia Artificial

Joel Ibaceta, Vicky Huilca, Willmer Contreras, Aldair Quispe, Thomy Villanueva
Universidad Nacional de Ingeniería, Lima, Perú
Correo electrónico: {joel.ibaceta.c, vicky.huilca, w.contreras.q, tvillanuevaq}@uni.edu.pe

***Resumen*— Este informe analiza la evolución y eficacia de los CAPTCHA en la era de la inteligencia artificial. A medida que los bots automatizados y las técnicas de aprendizaje profundo avanzan, el enfoque tradicional enfrenta desafíos significativos en su capacidad para diferenciar entre humanos y máquinas. Se revisan los diferentes tipos, evaluando su confiabilidad y las limitaciones que presentan frente a las tecnologías emergentes. Además, se exploran tendencias futuras y alternativas propuestas para mejorar la seguridad y usabilidad de estos sistemas. Las conclusiones destacan la necesidad de enfoques innovadores y adaptativos que equilibren la seguridad con la experiencia del usuario, considerando las implicaciones éticas y de privacidad.**

***Index Terms*—CAPTCHA, Inteligencia Artificial, Seguridad Web, Aprendizaje Automático, Reconocimiento de Patrones**

I. Introducción

La interacción entre humanos y sistemas informáticos es constante y cada vez más sofisticada. Sin embargo, esta interacción se ve amenazada por la proliferación de bots automatizados que pueden comprometer la seguridad y funcionalidad de los servicios en línea [1], [2]. Para mitigar este problema, se han desarrollado los CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), que actúan como una barrera para diferenciar entre usuarios humanos y sistemas automatizados [3].

El concepto de distinguir entre humanos y máquinas tiene sus raíces en el Test de Turing, propuesto por Alan Turing en 1950 como una forma de evaluar la capacidad de una máquina para exhibir un comportamiento indistinguible del de un humano [4]. Los CAPTCHA pueden considerarse como una implementación práctica de este concepto, donde se invierte el rol: en lugar de que una máquina intente parecer humana, se busca que los sistemas identifiquen a los usuarios humanos para prevenir accesos no autorizados y actividades maliciosas [3].

Funcionan presentando desafíos que son fáciles de resolver para los humanos pero difíciles para las máquinas. Estos explotan las habilidades cognitivas humanas en reconocimiento de patrones y percepción, áreas en las que las máquinas tradicionalmente han tenido dificultades. No obstante, con el avance de la inteligencia artificial y, en particular, de las técnicas de aprendizaje profundo, los sistemas automatizados han mejorado significativamente en tareas de reconocimiento y análisis, poniendo en entredicho la eficacia de los metodos tradicionales [2], [5], [6]. Esto plantea nuevos desafíos en la seguridad web y la necesidad de desarrollar métodos más robustos para asegurar que detrás de cada interacción en línea hay un humano legítimo [7].

Este informe analiza la evolución de los CAPTCHA frente al avance de la inteligencia artificial, explorando investigaciones recientes y los retos actuales sobre su confiabilidad para cumplir su proposito con eficacia.

II. Antecedentes

La necesidad de diferenciar entre humanos y máquinas en entornos digitales surgió con el aumento de actividades maliciosas automatizadas en la web, como el envío masivo de spam y los ataques de denegación de servicio [8]. Para mitigar estos problemas, en el año 2000, von Ahn et al. introdujeron el concepto de CAPTCHA [8].

Los primeros eran principalmente basados en texto, donde se presentaban caracteres distorsionados y superpuestos que los humanos podían leer pero que eran difíciles de interpretar por máquinas, aprovechando las limitaciones de los algoritmos de reconocimiento óptico de caracteres (OCR) de la época [6]. Este método se convirtió en un estándar para la verificación humana en sitios web y servicios en línea.

Con el avance de las técnicas de OCR y el aprendizaje automático, los programas automatizados comenzaron a resolverlos con mayor precisión [9]. Investigaciones como la de Mori y Malik [6] demostraron que los CAPTCHA basados en texto podían ser vulnerables a ataques automatizados.

En respuesta a ello, se desarrollaron nuevos tipos, incluyendo versiones basadas en imágenes y audio, los cuales requieren capacidades cognitivas humanas avanzados en reconocimiento visual o auditivo [10], siguiendo esta tendencia posteriormente han desarrollado otros tipos adicionales: Basados en audio, video, comportamiento, preguntas lógicas o matemáticas, entre otros. [11]–[13].

II-A. Desafíos debido al Avance de la Inteligencia Artificial

El surgimiento del aprendizaje profundo y las redes neuronales convolucionales mejoró significativamente la capacidad de las máquinas para reconocer objetos en imágenes y patrones [14]. Esto incrementó la vulnerabilidad de los CAPTCHA tradicionales, ya que los algoritmos podían ser entrenados para resolverlos con altas tasas de éxito [15].

Estudios han demostrado que los desafios basados en texto e imágenes pueden ser resueltos utilizando técnicas de aprendizaje profundo. Por ejemplo, Kovács y Tajti [5] utilizaron algoritmos de *machine learning* para reconocer y resolver diferentes tipos con eficacia.

Como respuesta se han propuesto nuevos enfoques en el diseño de los CAPTCHA, como aquellos que requieren interacciones más complejas que van más allá del reconocimiento visual simple [11]. Además, se han explorado métodos que incorporan elementos de interacción humana y comportamiento, difíciles de replicar por máquinas [16].

Ante el creciente poder de los algoritmos de inteligencia artificial, algunos investigadores han explorado tambien el uso de IA para crear CAPTCHAs que sean difíciles de resolver incluso para otras IA. Una de las técnicas más prominentes en este ámbito es el uso de Redes Generativas Antagónicas (GAN, por sus siglas en inglés).

Actualmente la comunidad cientifica aun se encuentra en la busqueda de nuevos enfoques y soluciones para garantizar la eficacia de los CAPTCHA en la era de la inteligencia artificial. [17]

III. Tipologia

Los CAPTCHA han evolucionado considerablemente desde su introducción, dando lugar a diversos tipos diseñados para aprovechar diversas habilidades cognitivas humanas que son difíciles de replicar por máquinas. Según Kumar et al. [2], los principales tipos son:

III-A. Basados en Texto

Este es el tipo más tradicional, donde se presentan caracteres alfanuméricos distorsionados que el usuario debe identificar y transcribir [8]. Comúnmente se aplican varios tipos de transformaciones, desorden, ruido, combinaciones de colores, entre otros, al primer plano y/o al fondo para hacer que la imagen resultante sea más desafiante. [18]

III-B. Basados en Imágenes

Estos requieren que el usuario identifique imágenes que cumplen cierta condición, como seleccionar todas las imágenes que contienen un objeto específico [10]. Aprovechan la capacidad humana para el reconocimiento de patrones y objetos en imágenes complejas.

III-C. Basados en Audio

Diseñados para usuarios con discapacidades visuales, estos presentan clips de audio con palabras, números distorsionados que deben ser transcritos [19], en el trabajo de Bursztein et al. [7] se menciona que en un estudio sobre Ebay hasta el 0.77

III-D. Basados en Video

Estos presentan videos cortos y solicitan al usuario que responda preguntas sobre el contenido [12]. Buscan aprovechar la capacidad humana para comprender secuencias temporales y contextos visuales complejos.

III-E. Basados en Comportamiento

Analizan patrones de interacción del usuario con el dispositivo, como movimientos del ratón, dinámicas de tecleo o gestos táctiles [13]. Se basan en la biometría de comportamiento, que es difícil de replicar por bots.

III-F. Basados en Preguntas Lógicas o Matemáticas

Plantean problemas simples de lógica o matemáticas que requieren comprensión y razonamiento, como resolver una suma o identificar el resultado de una operación [11]. Existen tambien variantes más complejas que involucran problemas cognitivos avanzados que implican comprensión semántica y contextual, como resolucion de acertijos, analogias, interpretacion semantica, etc. [18]

IV. Análisis de la Eficacia de los CAPTCHA

En esta sección se analiza la eficacia de los distintos tipos de CAPTCHA, citando estudios que los introdujeron o evaluaron su efectividad, así como trabajos que señalan sus limitaciones.

IV-A. Eficacia de los CAPTCHA Basados en Texto

Estos fueron introducidos por von Ahn et al. [8] y demostraron ser efectivos inicialmente al aprovechar las limitaciones de los algoritmos de reconocimiento óptico de caracteres (OCR) de la época. Sin embargo, estudios posteriores mostraron vulnerabilidades. Mori y Malik [6] lograron romper estos CAPTCHA utilizando técnicas de visión por computadora. Además, Goodfellow et al. [15] demostraron que las redes neuronales profundas pueden reconocer caracteres distorsionados con alta precisión.

IV-B. Eficacia de los CAPTCHA Basados en Imágenes

Introducidos para superar las limitaciones de las versiones de texto, estos planteaban problemas basados en la interpretacion de imágenes, los cuales fueron considerados más seguros [10]. Sin embargo, Sivakorn et al. [20] demostraron que es posible superar sistemas como reCAPTCHA de Google utilizando técnicas de aprendizaje profundo e incluso desafios como reconocer rostros humanos reales vs avatars, pueden ser resueltos [16], poniendo en duda su eficacia.

IV-C. Eficacia de los CAPTCHA Basados en Audio

Aunque ofrecen accesibilidad para usuarios con discapacidades visuales, las versiones de audio también presentan vulnerabilidades. Patel y Tam, [19], [21] mostraron que mediante el procesamiento de señales de audio, es posible filtrar el ruido y reconocer el contenido, reduciendo su eficacia como medida de seguridad.

IV-D. Eficacia de los CAPTCHA Basados en Video

Usar video permite aprovechar la complejidad de procesar secuencias visuales y contextos temporales. Kluever y Zanibbi [12] evaluaron su eficacia y encontraron que son más resistentes a ataques automatizados, aunque su uso suele estar limitado por la complejidad de implementación y la demanda de recursos que estos requieren.

IV-E. Eficacia de los CAPTCHA Basados en Comportamiento

La biometria de comportamiento ofrece una mayor resistencia a los bots debido a la dificultad de replicar patrones humanos complejos [13]. Sin embargo, Borges et al. [22] demostraron que con suficientes datos, es posible entrenar modelos que emulen comportamientos humanos, poniendo en duda su infalibilidad.

IV-F. Eficacia de los CAPTCHA Basados en Preguntas Lógicas o Matemáticas

Estos requieren comprensión y razonamiento, lo que inicialmente los hizo efectivos contra bots simples [11]. No obstante, avances en procesamiento del lenguaje natural y sistemas de inteligencia artificial capaces de resolver problemas matemáticos han reducido su eficacia [23].

IV-G. Limitaciones

Bursztein et al. [7] realizaron una amplia evaluación de diversos tipos de CAPTCHA, concluyendo que muchos presentan problemas de usabilidad, accesibilidad y seguridad. Yan y El Ahmad [9] destacaron que la complejidad excesiva puede frustrar a usuarios legítimos sin ofrecer una seguridad significativamente mayor.

Tambien es importante considerar tal como lo sugieren Bursztein y Chellapilla que tan buenos somos los humanos resolviendo CAPTCHA, ya que si estos son muy dificiles de resolver para nosotros, no cumplirian su proposito. [7], [24]

V. Evaluación de la Efectividad

La efectividad de implementar CAPTCHA en comparación con no utilizarlos ha sido objeto de estudio en diversas investigaciones.

Su confiabilidad como herramienta de seguridad es cada vez más cuestionada. Si bien siguen siendo una barrera útil contra bots simples, su eficacia contra ataques más sofisticados es limitada. La dependencia en desafíos que pueden ser resueltos por inteligencia artificial reduce su valor como medida de seguridad.

Bursztein et al. [7] evaluaron su efectividad en entornos reales y encontraron que, aunque pueden disuadir a bots simples, los atacantes más sofisticados pueden superarlos utilizando técnicas avanzadas, uso de la inteligencia artificial o servicios de resolución humana de CAPTCHAs.

Motoyama et al. [25] investigaron el mercado de servicios de resolución humana y demostraron que los atacantes pueden subcontratar a bajo costo, poniendo en duda la real efectividad de estos sistemas incluso con implementaciones confiables. Esto sugiere que, en algunos casos, tener un CAPTCHA puede no ofrecer una protección sustancial real en comparación con no tenerlo.

Por otro lado Gafni y Pavel [26] propusieron un modelo para evaluar el costo-beneficio de implementar CAPTCHA en sitios web comerciales. Su estudio concluyó que, si bien su uso puede reducir la actividad maliciosa, también pueden disminuir la participación del usuario, lo que en algunos casos puede superar los beneficios de seguridad proporcionados.

VI. Tendencias Futuras para mejorar la confiabilidad

El avance acelerado de la inteligencia artificial plantea desafíos significativos para mantener la eficacia en el tiempo de los CAPTCHA. En esta sección, exploramos brevemente los trabajos recientes y tendencias emergentes que abordan el futuro de esta tecnología, su viabilidad y alternativas propuestas.

Los avances en aprendizaje profundo y redes neuronales han mejorado la capacidad de las máquinas para resolver desafíos que antes eran exclusivos de los humanos [15]. Esto ha llevado a cuestionar la viabilidad a largo plazo de los CAPTCHA tradicionales. Bursztein et al. [27] demostraron que es posible romper múltiples sistemas de CAPTCHA basados en texto utilizando técnicas automatizadas, sugiriendo que los métodos actuales pueden volverse obsoletos eventualmente.

Hay varios investigadores que son pesimistas sobre la sostenibilidad de los CAPTCHA. Nguyen et al. [28] argumentan que, dada la rápida evolución de la IA, los CAPTCHA basados en desafíos cognitivos pueden no ser viables en el futuro cercano.

Pero por otro lado, otros tambien son más optimistas y confian en que los CAPTCHA pueden evolucionar para incorporar elementos más complejos y adaptativos [29].

VI-A. Alternativas Propuestas

Ante las limitaciones de los CAPTCHA tradicionales, se han propuesto alternativas que buscan mejorar la seguridad y la experiencia del usuario.

VI-A1. Autenticación Basada en Biometría de Comportamiento: La biometría de comportamiento analiza patrones únicos en el comportamiento del usuario, como la dinámica de tecleo, el movimiento del ratón y los gestos táctiles [30]. Estos métodos son más difíciles de replicar por bots y ofrecen una autenticación continua sin interrumpir la experiencia del usuario [13].

VI-A2. Análisis de Riesgo y Aprendizaje Automático: Los sistemas de análisis de riesgo evalúan múltiples factores, como la dirección IP, el historial de navegación y el comportamiento en el sitio, para determinar la probabilidad de que un usuario sea un bot [31]. Google reCAPTCHA v3 implementa este enfoque, proporcionando una puntuación de riesgo sin presentar desafíos al usuario [32].

VI-A3. Pruebas Cognitivas y Emocionales: Se ha propuesto tambien el uso de desafíos que requieren comprensión semántica profunda o respuestas emocionales, que son difíciles de emular por máquinas [33]. Estos incluyen pruebas que involucran humor, ironía o comprensión de contexto cultural.

VI-A4. CAPTCHA Generados mediante GAN: Goodfellow et al. [34] introdujeron las GAN, que consisten en dos redes neuronales que compiten entre sí: una generadora y una discriminadora. Esta arquitectura ha sido utilizada para generar

imágenes sintéticas que son difíciles de distinguir de imágenes reales.

Sajjad et al. [35] propusieron el uso de GAN para generar CAPTCHA más complejos y difíciles de resolver por sistemas automatizados. Al entrenar una red generadora para producir CAPTCHAs que engañen a una red discriminadora (simulando un sistema de reconocimiento automático), se pueden obtener desafíos que son intrínsecamente difíciles para las IA actuales.

VI-A5. Enfoque en Problemas de IA No Resueltos: Shirali-Shahreza y Shirali-Shahreza [17] propusieron el uso de problemas de inteligencia artificial que aún no han sido resueltos por máquinas, como la comprensión del lenguaje natural en contextos complejos, para diseñar CAPTCHA más resistentes. Estos desafíos requieren que el usuario interprete y responda a preguntas que involucran sentido común y conocimiento contextual.

VI-B. Consideraciones Éticas y Privacidad

A medida que se incorporan técnicas más avanzadas, es crucial considerar las implicaciones éticas y de privacidad. Por ejemplo, en el uso de biometría de comportamiento y análisis de datos personales este debe realizarse de manera responsable, garantizando la protección de la información del usuario y cumpliendo con regulaciones de privacidad [13].

VI-C. Evaluación Continua y Adaptabilidad

Finalmente, es importante que los sistemas CAPTCHA sean evaluados y actualizados continuamente para responder a las nuevas técnicas de ataque que emergen con el avance de la inteligencia artificial. La adaptabilidad y la capacidad de evolución serán características clave para mantener la eficacia de estos sistemas en el futuro

VII. Conclusiones

La evolución de la inteligencia artificial ha planteado desafíos significativos para la confiabilidad y eficacia de los CAPTCHA como herramienta de seguridad en línea. Inicialmente, los CAPTCHA basados en texto y otros métodos tradicionales ofrecían una barrera efectiva contra bots y actividades maliciosas. Sin embargo, con los avances en aprendizaje profundo y técnicas de reconocimiento, muchos de estos métodos han demostrado ser vulnerables.

El análisis de los diferentes tipos de CAPTCHA revela que, aunque algunos ofrecen mayor resistencia a ataques automatizados, ninguno es completamente infalible. Los CAPTCHA basados en imágenes, audio, video y comportamiento han sido comprometidos mediante técnicas avanzadas de inteligencia artificial o por medio de servicios de resolución humana de CAPTCHA a bajo costo [20], [25].

Además, la implementación de CAPTCHA puede afectar negativamente la experiencia del usuario, generando frustración y potencialmente disminuyendo la participación en sitios web [9], [26]. Esto plantea dudas sobre si los beneficios de seguridad superan los costos asociados con su uso.

Las tendencias futuras sugieren que la confiabilidad de los CAPTCHA dependerá de la capacidad para innovar y adaptarse a las nuevas tecnologías. El uso de inteligencia artificial para generar desafíos más complejos, la integración de biometría de comportamiento y el análisis de riesgo representan direcciones prometedoras [13], [35]. Sin embargo, también es crucial abordar consideraciones éticas y de privacidad al implementar estas soluciones.

En conclusión, aunque los CAPTCHA siguen siendo una herramienta útil en la seguridad en línea, su eficacia y confiabilidad están en constante desafío debido al avance de la inteligencia artificial. Es esencial que la comunidad académica y la industria colaboren en el desarrollo de métodos más robustos y adaptativos, equilibrando la seguridad con la usabilidad y la privacidad del usuario. Solo a través de una evolución continua y una evaluación constante se podrá mantener la relevancia y efectividad de los CAPTCHA en el futuro.

Referencias

[1] J. Hidalgo and G. Álvarez, "Captchas," vol. 83, pp. 109–181, 2011.

[2] M. Kumar, M. Jindal, and M. Kumar, "A systematic survey on captcha recognition: Types, creation and breaking techniques," *Archives of Computational Methods in Engineering*, vol. 29, no. 2, pp. 1107–1136, Mar 2022.

[3] L. von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," *Communications of the ACM*, vol. 47, no. 2, pp. 56–60, 2004.

[4] A. Turing, "Computing machinery and intelligence," *Mind*, vol. 59, no. 236, pp. 433–460, 1950.

[5] Kovács and T. Tajti, "Captcha recognition using machine learning algorithms with various techniques," *Annales Mathematicae et Informaticae*, vol. 58, pp. 81–91, 2023.

[6] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: Breaking a visual captcha," in *Proceedings of the 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 1. IEEE, 2003, pp. I–I.

[7] E. Bursztein, S. Bethard, C. Fabry, J. Mitchell, and D. Jurafsky, "How good are humans at solving captchas? a large scale evaluation," in *2010 IEEE Symposium on Security and Privacy*, 2011, pp. 399–413.

[8] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard ai problems for security," in *Advances in Cryptology—EUROCRYPT 2003*. Springer, 2003, pp. 294–311.

[9] J. Yan and A. S. El Ahmad, "A low-cost attack on a microsoft captcha," *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pp. 543–554, 2008.

[10] R. Gossweiler, M. Kamvar, and S. Baluja, "What's up captcha?: A captcha based on image orientation," in *Proceedings of the 18th International Conference on World Wide Web*, 2009, pp. 841–850.

[11] J. C. Hernandez-Castro and A. Ribagorda, "Pitfalls in captcha design and implementation: The math captcha, a case study," in *2010 International Conference on Availability, Reliability and Security*. IEEE, 2010, pp. 161–168.

[12] K. A. Kluever and R. Zanibbi, "Balancing usability and security in a video captcha," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009, p. 14.

[13] S. J. Murdoch, "Beyond captcha: Detecting silent, human-like malicious interactions using behavioral biometrics," *Communications of the ACM*, vol. 63, no. 6, pp. 42–44, 2020.

[14] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in Neural Information Processing Systems*, vol. 25, 2012, pp. 1097–1105.

[15] I. J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud, and V. Shet, "Multi-digit number recognition from street view imagery using deep convolutional neural networks," *arXiv preprint arXiv:1312.6082*, 2014.

[16] B. B. Zhu, J. Yan, G. Bao, M. Yang, and N. Xu, "Attacks and design of image recognition captchas," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 2010, pp. 187–200.

[17] M. Shirali-Shahreza and S. M. Shirali-Shahreza, "Using ai-hard problems for captcha design," in *2018 4th International Conference on Web Research (ICWR)*. IEEE, 2018, pp. 142–147.

[18] A. Algwil, "A survey on captcha: Origin, applications and classification," vol. 36, pp. 1 – 37, 06 2023.

[19] K. Y. W. Tam, J. Simsa, L. von Ahn, and M. Blum, "Breaking audio captchas," in *Advances in Neural Information Processing Systems*, vol. 20, 2008, pp. 1–8.

[20] S. Sivakorn, I. Polakis, and A. Keromytis, "I am robot: (deep) learning to break semantic image captchas," in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2016, pp. 388–403.

[21] M. Patel and A. Nath, "Breaking audio captchas," *International Journal of Computer Applications*, vol. 139, no. 12, pp. 5–8, 2016.

[22] P. V. Borges and A. Conci, "Biometric continuous authentication: A review of recent advances and recommendations for future research," *Computers & Security*, vol. 88, p. 101640, 2019.

[23] H. J. Levesque, E. Davis, and L. Morgenstern, "The winograd schema challenge," in *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Law*, 2011, pp. 211–215.

[24] K. Chellapilla, K. Larson, P. Y. Simard, and M. Czerwinski, "Designing human friendly human interaction proofs (hips)," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2005, pp. 711–720.

[25] M. Motoyama, K. Levchenko, D. McCoy, S. Savage, and G. M. Voelker, "Re: Captchas—understanding captcha-solving services in an economic context," in *USENIX Security Symposium*, 2010, pp. 435–462.

[26] R. Gafni and T. Pavel, "Examining user experience and security in captcha systems: A cost-benefit perspective," *Online Journal of Applied Knowledge Management*, vol. 7, no. 1, pp. 1–14, 2019.

[27] E. Bursztein, J. Aigrain, A. Moscicki, and J. C. Mitchell, "The end is nigh: Generic solving of text-based captchas," in *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, 2014.

[28] T. T. Nguyen, M.-T. Tran, N. Le *et al.*, "Captcha design: A review of trends and techniques," *IEEE Access*, vol. 8, pp. 145 749–145 766, 2020.

[29] P.-Y. Huang, C.-H. Chen *et al.*, "A survey of captcha technologies and their applications," *Computers & Security*, vol. 77, pp. 101–117, 2018.

[30] P. L. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," *The Scientific World Journal*, vol. 2013, p. 408280, 2013.

[31] R. Kumar, R. K. Singh, and M. Kumar, "Anomaly detection in web applications using machine learning," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2019, pp. 227–232.

[32] Google, "Google recaptcha," Consultado en septiembre de 2024, 2018, disponible en https://developers.google.com/recaptcha/.

[33] C. y. o. Vázquez, "Understanding captcha robustness: A survey," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–36, 2018.

[34] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in Neural Information Processing Systems*, vol. 27, 2014, pp. 2672–2680.

[35] M. Sajjad, S. U. R. Khan, I. Ullah, S. Choi, and S. W. Baik, "Captcha generation and security using generative adversarial networks," *Computers & Security*, vol. 85, pp. 218–231, 2019.