

Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), mayo-junio 2025,
Volumen 9, Número 3.

https://doi.org/10.37811/cl_rcm.v9i1

**ESTUDIO DEL USO DE HERRAMIENTAS
DE IA PARA LA GESTIÓN DE PROYECTOS
DE SOFTWARE, COMO INSTRUMENTO
PARA MEJORAR LA SEGURIDAD DE
LAS APLICACIONES**

**STUDY OF THE USE OF AI TOOLS FOR SOFTWARE
PROJECT MANAGEMENT, AS AN INSTRUMENT
TO IMPROVE APPLICATION SECURITY**

Mtro. Mario Orea León

Universidad Tecnológica de Tecamachalco, Mexico

Mtro. Victor Manuel Bravo Romero

Universidad Tecnológica de Tecamachalco, Mexico

Mtro. David Arenas Hernández

Universidad Tecnológica de Tecamachalco, Mexico

Dr. Manuel González Pérez

Universidad Tecnológica de Tecamachalco, Mexico

DOI: https://doi.org/10.37811/cl_rcm.v9i3.18168

Estudio del Uso de Herramientas de IA para la Gestión de Proyectos de Software, como Instrumento para Mejorar la Seguridad de las Aplicaciones

Mtro. Mario Orea León¹mario.ol@personal.uttecam.edu.mx<https://orcid.org/0000-0003-2145-7408>Universidad Tecnológica de Tecamachalco
Mexico**Mtro. Victor Manuel Bravo Romero**victor.br@personal.uttecam.edu.mx<https://orcid.org/0009-0001-0394-2314>Universidad Tecnológica de Tecamachalco
Mexico**Mtro. David Arenas Hernández**david.ah@personal.uttecam.edu.mx<https://orcid.org/0009-0005-3868-8909>Universidad Tecnológica de Tecamachalco
Mexico**Dr. Manuel González Pérez**m.gonzalez.perez@personal.uttecam.edu.mx<http://orcid.org/0000-0001-8700-2866>Universidad Tecnológica de Tecamachalco
Mexico

RESUMEN

En la era de la transformación digital, la seguridad de las aplicaciones de software se ha convertido en un pilar fundamental para garantizar la confianza del usuario, la protección de datos y la continuidad operativa de las organizaciones en todos los sectores. Esta investigación tuvo como objetivo estudiar el uso de herramientas de inteligencia artificial (IA) para la gestión de proyectos de software para mejorar la seguridad de las aplicaciones. Se aplicó un cuestionario a 91 estudiantes de Tecnologías de la Información de la Universidad Tecnológica de Tecamachalco, Puebla. El cuestionario consta de quince preguntas diseñadas para ser aplicadas a la estadística inferencial, ya que se ordenaron de dos en dos para generar 225 hipótesis bivariadas. El diseño fue implementado con una escala Likert de 5 opciones, la cual se dicotomizó para validar las hipótesis bivariadas con una prueba de chi-cuadrado. El proceso de validación fue riguroso, con cuarenta hipótesis validadas en correlación lineal por coeficiente de Pearson > 0.6 y con una prueba de chi-cuadrado de dos grados de libertad con un límite de confianza del 95% y un error estadístico del 5%. De las 40 hipótesis validadas linealmente, solo nueve se tomaron por razones de espacio.

Palabras clave: inteligencia artificial, desarrollo de software, gestión de proyectos, seguridad de aplicaciones

¹ Autor principal.

Correspondencia: m.gonzalez.perez@personal.uttecam.edu.mx

Study of the Use of AI Tools for Software Project Management, as an Instrument to Improve Application Security

ABSTRACT

In the digital transformation era, software application security has become a critical pillar to ensure user trust, data protection, and the operational continuity of organizations across all sectors. This research aimed to study the use of artificial intelligence (AI) tools for software project management to improve application security. A questionnaire was administered to 91 Information Technology students at the Technological University of Tecamachalco, Puebla. The questionnaire consists of fifteen questions designed to be applied to inferential statistics, as they were ordered two by two to generate 225 bivariate hypotheses. The design was proprietary with a 5-option Likert scale, which was dichotomized to validate the bivariate hypotheses with a chi-square test. The validation process was rigorous, with forty hypotheses being validated in linear correlation by Pearson coefficient > 0.6 and with a two-degree-of-freedom chi-square test with a 95% confidence limit and a 5% statistical error. Of the 40 hypotheses validated linearly, only nine were taken for space reasons.

Keywords: artificial intelligence, software development, project management, application security

Artículo recibido 15 mayo 2025

Aceptado para publicación: 16 junio 2025



INTRODUCCIÓN

En la era de la transformación digital, la seguridad de las aplicaciones software se ha convertido en un pilar crítico para garantizar la confianza de los usuarios, la protección de datos y la continuidad operativa de organizaciones en todos los sectores (European Union Agency for Cybersecurity [ENISA], 2023). Sin embargo, el desarrollo de software enfrenta desafíos sin precedentes: ciclos de vida cada vez más cortos, requisitos de cumplimiento normativo más estrictos (como el Reglamento General de Protección de Datos de la UE) y amenazas cibernéticas en constante evolución (Open Web Application Security Project [OWASP], 2021).

Tradicionalmente, la gestión de proyectos de software ha priorizado aspectos como el cumplimiento de plazos, la asignación de recursos y el control de costos, relegando en ocasiones la seguridad a etapas tardías del proceso (McGraw, 2006). Esta desconexión ha demostrado ser insostenible, ya que vulnerabilidades no detectadas en fases iniciales pueden traducirse en brechas críticas, con impactos financieros devastadores (IBM Security, 2022).

En este contexto, las herramientas de inteligencia artificial (IA) emergen como un catalizador para transformar la gestión de proyectos, no solo optimizando la eficiencia operativa, sino también integrando la seguridad como un eje transversal desde el diseño hasta el despliegue (LeCun et al., 2015). La capacidad de los sistemas de IA para analizar grandes volúmenes de datos, predecir riesgos, automatizar tareas repetitivas y detectar patrones sutiles ofrece una oportunidad única para anticipar y mitigar vulnerabilidades de forma proactiva (Allamanis et al., 2018) (Casey y Perry, 2025) (Cao et al., 2025).

Por ejemplo, algoritmos de aprendizaje automático pueden identificar inconsistencias en el código fuente, modelos predictivos pueden evaluar el impacto de cambios en la arquitectura del software (Zhang et al., 2020) (Chai-Allah, 2025) (Vemulapalli, 2025), y sistemas de monitorización en tiempo real, basados en redes neuronales, pueden alertar sobre comportamientos anómalos durante la ejecución (Chowdhary et al., 2020).

A pesar de su potencial, la adopción de estas tecnologías en la gestión de proyectos de software aún enfrenta barreras técnicas, culturales y metodológicas (Amershi et al., 2019).



Este artículo explora cómo la integración estratégica de herramientas de IA en los flujos de trabajo de gestión no solo mejora la eficiencia, sino que también fortalece la seguridad de las aplicaciones. Se analiza el papel de la IA en la identificación temprana de riesgos, la priorización de tareas de seguridad y la creación de marcos colaborativos entre desarrolladores, gestores de proyectos y equipos de ciberseguridad (Forsgren et al., 2021).

La gestión tradicional de proyectos de software a menudo se ve obstaculizada por la dificultad de predecir y mitigar riesgos, la asignación ineficiente de recursos y la falta de visibilidad en el progreso del proyecto. Estas limitaciones pueden derivar en retrasos, sobrecostos y vulnerabilidades de seguridad que comprometen la calidad y la fiabilidad de las aplicaciones (Boehm, 1988; McConnell, 2006).

La IA ofrece un abanico de herramientas y técnicas que pueden abordar estos desafíos de manera efectiva. Los algoritmos de aprendizaje automático, por ejemplo, pueden analizar grandes volúmenes de datos para identificar patrones y tendencias, lo que permite a los gerentes de proyecto tomar decisiones más informadas y precisas (Russell & Norvig, 2016; Witten, Frank, Hall, & Pal, 2016). La IA también puede automatizar tareas repetitivas, como la generación de informes y el seguimiento del progreso, liberando tiempo valioso para que los equipos se concentren en actividades más estratégicas.

Además, la IA puede desempeñar un papel crucial en la mejora de la seguridad de las aplicaciones. Las herramientas de análisis de código impulsadas por IA pueden detectar vulnerabilidades y errores de seguridad en el código fuente, lo que permite a los desarrolladores corregirlos antes de que se conviertan en problemas graves (OWASP, 2021; Schach, 2010). La IA también puede ayudar a identificar y mitigar riesgos de seguridad durante todo el ciclo de vida del desarrollo de software, desde la fase de diseño hasta la implementación y el mantenimiento.

Por lo tanto, afirmamos que el dominio de herramientas de IA en el desarrollo de software representa un valor agregado significativo para los estudiantes de Tecnologías de la Información de la Universidad Tecnológica de Tecamachalco.

Este conocimiento no solo mejora la seguridad de las aplicaciones, sino que también prepara a los estudiantes para los desafíos y oportunidades del mercado laboral actual



METODOLOGÍA

Se aplicó un cuestionario a 91 estudiantes de Tecnologías de Información en la Universidad Tecnológica de Tecamachalco, Puebla. El cuestionario consta de quince preguntas, mismas que fueron diseñadas con la finalidad de llevarlas hasta estadística inferencial, ya que se ordenaron tomadas de dos en dos para generar 225 hipótesis bivariadas. El diseño fue propio con escala de Likert de 5 opciones que fueron dicotomizadas para validar las hipótesis bivariadas con Ji cuadrada. Este diseño fue realizado aplicando la metodología Cuántica-Hamiltoniana-Euleriana (CHE). La validación del cuestionario se llevó a cabo por expertos, aplicando 5 postulados de verificación y la correlación de Pearson, además de la prueba de bondad de ajuste Ji cuadrada (Hernández et al, 2021).

Las 225 inferencias bivariadas se convirtieron en hipótesis y se validaron por dos métodos: a) coeficiente de correlación de Pearson, para las correlaciones lineales y b) prueba de contraste Ji cuadrada para las asociaciones no lineales. La muestra fue aleatoria y correlacional, sin discriminación de género.

Cuestionario

1. Utilizo herramientas de IA para diseñar interfaces de usuario y experiencias de usuario
2. Utilizo herramientas de IA para generar código automáticamente
3. Utilizo herramientas de IA para realizar pruebas de software automatizadas.
4. Utilizo herramientas de IA para generar casos de prueba automáticamente
5. Utilizo herramientas de IA para gestionar y automatizar el ciclo de vida del desarrollo de software
6. Utilizo herramientas de IA para generar documentación técnica
7. Utilizo herramientas de IA para predecir y prevenir errores en el código
8. Utilizo herramientas de IA para optimizar el rendimiento del software.
9. Utilizo herramientas de IA para analizar y depurar código.
10. Utilizo herramientas de IA para la gestión de proyectos de software
11. Utilizo herramientas de IA para la seguridad del software, como la detección de vulnerabilidades
12. Estoy familiarizado con las herramientas de IA disponibles para el desarrollo de software
13. Considero que las herramientas de IA mejoran mi productividad en el desarrollo de software
14. Estoy interesado en aprender más sobre las herramientas de IA para el desarrollo de software



15. El uso de herramientas de IA en el desarrollo de software genera una ventaja competitiva en un Ingeniero en TI

Escala de Likert: 1 = menor medida, 5 = máxima medida.

RESULTADOS Y DISCUSIÓN

Validación de cuestionario.

Postulados de validación por expertos que revisaron si:

1. Las preguntas se repitieron. Resultado = No se encontraron preguntas repetidas.
2. Las preguntas están parafraseadas; el encuestado las tomó como repetidas. No hubo preguntas parafraseas.
3. La pregunta está parafraseada a propósito, se hicieron parafraseadas para cazar al encuestado en contradicción. No se encontraron preguntas parafraseadas a propósito.
4. Las preguntas se correlacionaron o asociaron por casualidad. No se encontraron preguntas correlacionadas por casualidad.
5. Las preguntas se correlacionaron o asociaron por su propia naturaleza. Si, se encontró que todas las correlaciones o asociaciones tanto lineales (coeficiente de Pearson) como no lineales (Chi cuadrada) fueron por la propia naturaleza de las preguntas.

Este cuestionario se aplicó y con los resultados. Las comparaciones fueron tomadas de una técnica de conteo, una ordenación tomada de dos en dos.

Ecuación 1

$$O = p^2 = 15^2 = 225$$

Donde:

O = al número de comparaciones bivariadas, que luego se convierten en inferencias, más adelante en hipótesis y luego en tesis (hipótesis comprobadas).

p = al número de preguntas o ítems.

En la tabla 1 se muestran los resultados de los coeficientes de Pearson para evaluar el cuestionario de las ordenaciones tomadas de dos en dos. Esta misma tabla servirá para evaluar las inferencias e hipótesis bivariadas.



Tabla 1. Resultado coeficiente de Pearson. Para validación de hipótesis bivariadas.

	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7	Item 8	Item 9	Item 10	Item 11	Item 12	Item 13	Item 14	Item 15
Item 1	1.000														
Item 2	-0.032	1.000													
Item 3	0.117	0.781	1.000												
Item 4	0.118	0.560	0.669	1.000											
Item 5	0.162	0.479	0.567	0.649	1.000										
Item 6	0.106	0.455	0.513	0.651	0.659	1.000									
Item 7	0.062	0.632	0.689	0.628	0.703	0.515	1.000								
Item 8	0.049	0.648	0.592	0.724	0.656	0.474	0.631	1.000							
Item 9	0.103	0.436	0.492	0.609	0.626	0.481	0.551	0.686	1.000						
Item 10	0.008	0.617	0.642	0.676	0.525	0.592	0.556	0.599	0.593	1.000					
Item 11	0.202	0.576	0.680	0.658	0.747	0.604	0.669	0.639	0.685	0.609	1.000				
Item 12	0.067	0.565	0.606	0.631	0.492	0.517	0.565	0.659	0.550	0.648	0.556	1.000			
Item 13	0.065	0.499	0.660	0.558	0.622	0.602	0.627	0.484	0.502	0.519	0.528	0.487	1.000		
Item 14	0.036	0.500	0.566	0.477	0.563	0.650	0.406	0.513	0.421	0.458	0.495	0.430	0.501	1.000	
Item 15	-0.003	0.320	0.422	0.331	0.536	0.459	0.402	0.436	0.332	0.401	0.432	0.348	0.537	0.505	1.000

En la tabla 2 se presentan las hipótesis validadas con el coeficiente de correlación de Pearson y Ji cuadrada para dos grados de libertad dicotomizada de la escala de Likert.

Tabla 2. Inferencias o hipótesis bivariadas validadas con Pearson y Ji cuadrada escogida por los autores.

Par	Inferencia o hipótesis bivariada	Pearson (0.6)	Ji Cuadrada (3.84)	Tesis
(10,11)	Si Utilizo herramientas de IA para la gestión de proyectos de software entonces Utilizo herramientas de IA para la seguridad del software, como la detección de vulnerabilidades	0.609	25.49	Utilizar herramientas de IA para la gestión de proyectos de software, permite mejorar la seguridad de las aplicaciones
(2,3)	Si Utilizo herramientas de IA para generar código automáticamente entonces Utilizo herramientas de IA para realizar pruebas de software automatizadas.	0.781	48.94	Utilizar herramientas de IA para generar código automáticamente se debe al buen uso de herramientas de IA para realizar pruebas de software automatizadas.
(2,7)	Si Utilizo herramientas de IA para generar código automáticamente entonces Utilizo herramientas de IA para predecir y prevenir errores en el código	0.632	33.15	El uso de IA en la generación de código, permite prevenir errores en el desarrollo de software
(2,8)	Si Utilizo herramientas de IA para generar código automáticamente entonces Utilizo herramientas de IA para optimizar el rendimiento del software.	0.648	25.06	El uso de IA en la generación de código, permite optimizar el rendimiento del software
(2,10)	Si Utilizo herramientas de IA para generar código automáticamente entonces Utilizo herramientas de IA para la gestión de proyectos de software	0.617	32.40	Utilizar herramientas de IA para generar código automáticamente, permite utilizar IA en la gestión de proyectos de Software



(3,2)	Si Utilizo herramientas de IA para realizar pruebas de software automatizadas. entonces Utilizo herramientas de IA para generar código automáticamente	0.781	48.948	Utilizar herramientas de IA para realizar pruebas de software automatizadas, generan código automáticamente
(3,4)	Si Utilizo herramientas de IA para realizar pruebas de software automatizadas. entonces Utilizo herramientas de IA para generar casos de prueba automáticamente	0.669	28.3782	Utilizar herramientas de IA para realizar pruebas de software automatizadas permite generar casos de prueba automáticamente
(3,7)	Si Utilizo herramientas de IA para realizar pruebas de software automatizadas. entonces Utilizo herramientas de IA para predecir y prevenir errores en el código	0.6887	43.651148	Utilizar herramientas de IA para realizar pruebas automatizadas, permite predecir y prevenir errores de código
(3,8)	Si Utilizo herramientas de IA para realizar pruebas de software automatizadas. entonces Utilizo herramientas de IA para optimizar el rendimiento del software.	0.592	27.744	Utilizar herramientas de IA para realizar pruebas de software automatizadas, permite optimizar el rendimiento del software

Argumentación de las tesis.

1. “Utilizar herramientas de IA para la gestión de proyectos de software, permite mejorar la seguridad de las aplicaciones”. Como el límite es de 3.84 y los jóvenes encuestados la toman 25.49, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.609.
2. “Utilizar herramientas de IA para generar código automáticamente se debe al buen uso de herramientas de IA para realizar pruebas de software automatizadas”. Como el límite es de 3.84 y los jóvenes encuestados la toman 48.94, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.781.
3. “El uso de IA en la generación de código, permite prevenir errores en el desarrollo de software”. Como el límite es de 3.84 y los jóvenes encuestados la toman 25.06, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.632.
4. “El uso de IA en la generación de código, permite optimizar el rendimiento del software”. Como el límite es de 3.84 y los jóvenes encuestados la toman 33.15, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.648.



5. “Utilizar herramientas de IA para generar código automáticamente, permite utilizar IA en la gestión de proyectos de Software”. Como el límite es de 3.84 y los jóvenes encuestados la toman 32.40, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.617.
6. “Utilizar herramientas de IA para realizar pruebas de software automatizadas, generan código automáticamente”. Como el límite es de 3.84 y los jóvenes encuestados la toman 48.94, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.781.
7. “Utilizar herramientas de IA para realizar pruebas de software automatizadas permite generar casos de prueba automáticamente”. Como el límite es de 3.84 y los jóvenes encuestados la toman 28.37, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.669.
8. “Utilizar herramientas de IA para realizar pruebas automatizadas, permite predecir y prevenir errores de código”. Como el límite es de 3.84 y los jóvenes encuestados la toman 43.65, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.688.
9. “Utilizar herramientas de IA para realizar pruebas de software automatizadas, permite optimizar el rendimiento del software”. Como el límite es de 3.84 y los jóvenes encuestados la toman 27.74, esto del 95% de confianza a un 99.9999. Además de tener una buena correlación lineal por el coeficiente de Pearson de 0.592.

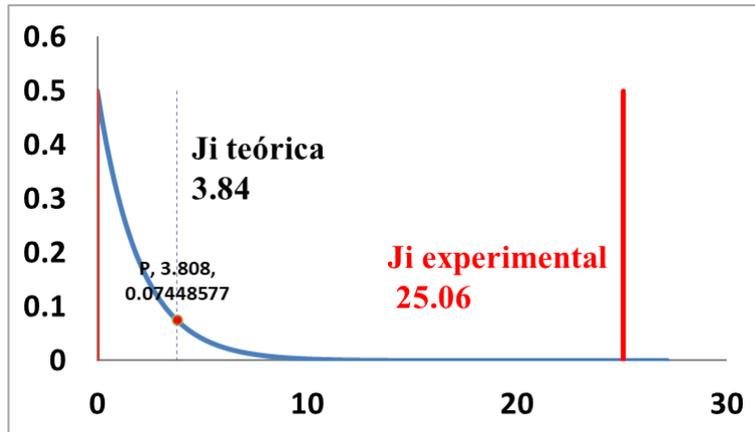
En la figura 1, se muestra la gráfica del par ordenado (2,8) (pregunta o ítem 2, con el 8).

Inferencia: “Si Utilizo herramientas de IA para generar código automáticamente entonces, utilizo herramientas de IA para optimizar el rendimiento del software. Pearson = 0.648; Ji cuadrada = 25.06.

Hipótesis comprobada o tesis: “El uso de IA en la generación de código, permite optimizar el rendimiento del software”



Figura 1. Gráfica del par ordenado de preguntas (2,8)



No se muestran las 40 tesis generadas, por razones de espacio.

CONCLUSIONES

La integración de herramientas de inteligencia artificial en la gestión de proyectos de software representa un avance paradigmático en la forma en que abordamos la seguridad de las aplicaciones. Los resultados analizados en este trabajo demuestran que la IA no solo optimiza procesos operativos, sino que redefine la seguridad como un componente intrínseco del ciclo de vida del desarrollo.

Objetivo

Usar herramientas de IA para la gestión de proyectos de software, como instrumento para mejorar la seguridad de las aplicaciones en la Universidad Tecnológica de Tecamachalco, se cumplió.

Tesis general

Utilizar herramientas de IA para la gestión de proyectos de software, si permite mejorar la seguridad de las aplicaciones.

REFERENCIAS BIBLIOGRAFICAS

- Allamanis, M., Barr, E. T., Devanbu, P., & Sutton, C. (2018). A survey of machine learning for big code and naturalness. *ACM Computing Surveys*, 51(4), 1–37. <https://doi.org/10.1145/3212695>
- Amershi, S., Begel, A., Bird, C., DeLine, R., Gall, H., Kamar, E., Nagappan, N., Nushi, B., & Zimmermann, T. (2019). Software engineering for machine learning: A case study. *Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice*, 291–300. <https://doi.org/10.1109/ICSE-SEIP.2019.00042>



- Cao, Y., Li, S., Liu, Y., Yan, Z., Dai, Y., Yu, P., & Sun, L. (2025). A survey of ai-generated content (aigc). *ACM Computing Surveys*, 57(5), 1-38.
- Casey, B., Santos, J. C., & Perry, G. (2025). A survey of source code representations for machine learning-based cybersecurity tasks. *ACM Computing Surveys*, 57(8), 1-41.
- Chai-allah, A., Hermes, J., De La Foye, A., Venter, Z. S., Joly, F., Brunschwig, G., ... & Fox, N. (2025). Assessing recreationists' preferences of the landscape and species using crowdsourced images and machine learning. *Landscape and Urban Planning*, 257, 105315.
- Chowdhary, K. R., Chowdhary, M., & Choo, K. K. R. (2020). Cybersecurity in the age of artificial intelligence. *IEEE Access*, 8, 223008–223037. <https://doi.org/10.1109/ACCESS.2020.3042274>
- European Union Agency for Cybersecurity. (2023). *Threat landscape for software supply chain attacks*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- Forsgren, N., Humble, J., & Kim, G. (2021). *Accelerate: The science of lean software and DevOps*. IT Revolution Press.
- IBM Security. (2022). *Cost of a data breach report*. <https://www.ibm.com/security/data-breach>
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
- McGraw, G. (2006). *Software security: Building security in*. Addison-Wesley Professional.
- National Institute of Standards and Technology. (2020). *Cybersecurity framework version 1.1*. <https://www.nist.gov/cyberframework>
- Open Web Application Security Project. (2021). *Top 10 application security risks*. <https://owasp.org/www-project-top-ten/>
- Vemulapalli, G. (2025). Charting the Ethical Horizon: A Deep Dive Into AI Ethics, Unraveling the Moral Threads in Machine Intelligence Development. In *Artificial Intelligence and Machine Learning for Sustainable Development* (pp. 209-220). CRC Press.
- Zhang, J. M., Harman, M., Ma, L., & Liu, Y. (2020). Machine learning testing: Survey, landscapes and horizons. *IEEE Transactions on Software Engineering*, 48(2), 1–25. <https://doi.org/10.1109/TSE.2019.2962027>

