

CAPÍTULO 20.

USO DE LA INTELIGENCIA ARTIFICIAL EN LA DETECCIÓN DE FRAUDES FINANCIEROS: LECCIONES DESDE LA EXPERIENCIA DE EMPRESAS AUDITADAS EN LIMA

Rubén Vellaneda Ambrosio
Josué Raúl Vásquez Orihuela¹
Chris Yosselin Colachagua Vivanco²

¹: Contador Público y Abogado.

 <https://orcid.org/0000-0003-2458-2132>

²: Abogada.

 <https://orcid.org/0000-0001-7555-994X>

RESUMEN

Este capítulo de revisión narrativa sintetiza, por primera vez para el Perú, las lecciones aprendidas sobre la implementación de inteligencia artificial (IA) para la detección de fraudes financieros en empresas auditadas en Lima durante 2018-2023. A partir de 68 fuentes académicas y grises, complementadas con evidencia de 15 compañías de retail, banca y servicios, se identificó que Random Forest, XGBoost, autoencoders e Isolation Forest son las técnicas más adoptadas, alcanzando F1-scores entre 0,82-0,91 y reduciendo el tiempo de detección en 35 %. El éxito depende críticamente de la calidad de datos (data quality score ≥ 80 %), de la conformación de equipos mixtos auditor-data scientist y de la existencia de gobernanza de modelos. Las principales barreras fueron datos fragmentarios, escasez de talento híbrido, resistencia cultural y ausencia de marcos regulatorios específicos. Se propone un comité de datos corporativo, pruebas de sesgo/explicabilidad en los planes de auditoría y un sandbox regulatorio para acelerar la adopción responsable de IA. El estudio extiende el Fraude Triangle al incorporar la “oportunidad data-driven” y ofrece un esquema replicable para otros países latinoamericanos.

Palabras clave: inteligencia artificial, fraude financiero, auditoría continua, gobernanza de datos, Perú.

INTRODUCCIÓN

El fraude financiero representa una de las amenazas más costosas para la estabilidad de los mercados. La Asociación de Examinadores de Fraude Certificados (ACFE, 2022) estima que las organizaciones pierden anualmente cerca del 5 % de sus ingresos por fraudes, lo que equivaldría a más de USD 4,7 billones a nivel global. Estas pérdidas no solo afectan la rentabilidad, sino que erosionan la confianza de inversores y consumidores, incrementan el costo de capital y generan externalidades negativas en el entorno económico (Kassem & Higson, 2022).

En el Perú, el panorama es igualmente preocupante. Entre 2018 y 2022, la Superintendencia de Banca, Seguros y AFP (SBS) reportó operaciones crediticias fraudulentas por USD 380 millones, mientras que el Registro de Denuncias de INDECOPI reveló un aumento del 42 % en reclamos por estafas corporativas (SBS, 2023; INDECOPI, 2023). La Comisión para el Mercado Financiero (CMF, ex CONASEV) advirtió que el 37 % de los errores materiales en estados financieros de empresas listadas tuvo un componente de intencionalidad (CMF, 2021). Estas cifras subrayan la urgencia de fortalecer los mecanismos de detección oportuna.

Los métodos tradicionales de auditoría —basados en muestreo estadístico y procedimientos de cumplimiento— han demostrado limitaciones para identificar fraudes sofisticados en entornos de alta volatilidad y volumen de transacciones (Alleyne & Howard, 2021). El enfoque de “auditoría basada en riesgos” suele depender de listas de verificación que pueden ignorar señales débiles o patrones no lineales característicos del fraude moderno (Yoon et al., 2019).

En este contexto, la inteligencia artificial (IA) surge como una alternativa complementaria capaz de procesar grandes volúmenes de datos en tiempo real, detectar anomalías complejas y adaptarse a nuevos esquemas de fraude

mediante aprendizaje continuo (Dilmegani, 2023). Técnicas como Random Forest, redes neuronales profundas y algoritmos de aislamiento (Isolation Forest) han mostrado precisiones superiores al 90 % en la identificación de transacciones sospechosas (Perols et al., 2022). Además, la integración de procesamiento de lenguaje natural (NLP) permite analizar notas de management y correos electrónicos en busca de “red flags” lingüísticas (Zhang et al., 2021).

No obstante, la mayoría de la evidencia proviene de mercados desarrollados, existiendo un vacío empírico sobre cómo estas tecnologías se adaptan a realidades institucionales, normativas y de gobernanza de mercados emergentes (Braun & Rodriguez, 2022). Lima, como centro financiero del Perú, concentra el 62 % de las empresas que cotizan en Bolsa y el 70 % de los activos del sistema bancario; sin embargo, no existen estudios que sistematicen las experiencias locales de implementación de IA para la detección de fraudes.

Con base en lo anterior, esta investigación se guía por la pregunta: ¿Qué lecciones clave sobre la implementación de IA para la detección de fraudes pueden extraerse de la experiencia de empresas auditadas en Lima durante el período 2018-2023? El objetivo general es sistematizar dichas lecciones, mientras que los objetivos específicos son: (a) identificar las técnicas de IA adoptadas, (b) describir los factores críticos de éxito y las barreras encontradas, y (c) proponer recomendaciones prácticas para auditores, directores de riesgo y reguladores peruanos.

Se espera que los resultados aporten una guía contextualizada que acelere la adopción responsable de IA en la auditoría local y sirvan de base para futuros estudios cuantitativos que evalúen el impacto de estas herramientas en la opinión de auditoría y en la reducción cuantificable del fraude.

METODOLOGÍA

Se realizó una revisión narrativa orientada a responder la pregunta de investigación: ¿qué lecciones clave sobre la implementación de inteligencia artificial (IA) para la detección de fraudes financieros pueden extraerse de la experiencia de empresas auditadas en Lima durante el período 2018-2023? El diseño narrativo se seleccionó porque permite integrar evidencia heterogénea —cuantitativa y cualitativa— y construir un relato comprehensivo útil para la toma de decisiones en contextos locales (Ferrari, 2015; Popay et al., 2020).

Búsqueda documental

Se exploraron cinco bases académicas —Scopus, Web of Science, IEEE Xplore, ScienceDirect y Redalyc— para cubrir literatura en inglés y español publicada entre enero 2010 y enero 2024. Para capturar experiencias de implementación no publicadas en revistas científicas, se incluyeron fuentes grises: informes anuales de las Big Four en Perú (PwC, EY, KPMG, Deloitte), memorias de la Superintendencia de Banca, Seguros y AFP (SBS) y del Banco Central de Reserva del Perú (BCRP), así como proceedings de conferencias de ISACA e Institute of Internal Auditors (IIA). Adicionalmente, se empleó Google Scholar con filtros de fecha y se revisaron tesis de maestría de dos repositorios nacionales (Pontificia Universidad Católica del Perú y Universidad del Pacífico) siguiendo las recomendaciones de Godin et al. (2021) para minimizar el sesgo de disponibilidad.

Estrategia de búsqueda

Se construyó un string ilustrativo combinando descriptores MeSH y términos libres: (“artificial intelligence” OR “machine learning” OR “data analytics” OR “deep learning”) AND (“fraud detection” OR “forensic accounting” OR “financial fraud”) AND (“audit” OR “auditing” OR “continuous auditing”) AND (“Peru” OR “Latin America” OR “emerging market”). La búsqueda se replicó en cada base adaptando la sintaxis (por ejemplo, TOPIC en Web of Science y

TITLE-ABS-KEY en Scopus). En fuentes grises se utilizó el operador SITE: para limitar dominios (.gob.pe, .org, .edu.pe) y se aplicó el método “snowball” sobre referencias de informes seleccionados (Wohlin, 2020).

Criterios de selección

Inclusión: (a) estudios empíricos o experiencias de implementación de IA para detección de fraudes financieros; (b) organizaciones auditadas o auditoras como unidad de análisis; (c) texto completo disponible en español o inglés; (d) publicación entre 2010-2024. Exclusión: fraudes no financieros, preprints sin revisión, artículos sin sección de metodología, estudios exclusivamente teóricos o de diseño de algoritmos sin aplicación organizacional. El proceso se documentó mediante un diagrama PRISMA adaptado (Page et al., 2021), registrando: identificación (n = 1.240), cribaje por título y resumen (n = 180), elegibilidad tras lectura de texto completo (n = 68) y conjunto final incluido (n = 52 artículos + 16 fuentes grises).

Análisis de contenido

Se empleó un enfoque inductivo- deductivo. Tras lectura abierta, dos investigadores codificaron fragmentos mediante el software ATLAS.ti 22, utilizando una lista inicial de cinco nodos: técnica IA, contexto organizacional, resultado cuantitativo, barrera y lección aprendida. La confiabilidad inter-codificadores ($\kappa = 0,81$) se resolvió por consenso y, cuando era necesario, se consultó a un tercer revisor (Nowell et al., 2022). Los temas emergentes se agruparon en matrices comparativas por sector y tamaño de empresa.

Casos de Lima

Complementariamente, se seleccionó intencionalmente una muestra de 15 empresas auditadas con sede principal en Lima, representando tres sectores de alta exposición a fraude: retail (4), banca y seguros (5) y servicios corporativos (6). La selección respondió a criterios de disponibilidad de información pública (informes de auditoría, notas a estados financieros) y acceso a actas de junta directiva que mencionan proyectos de analytics. Siete empresas aceptaron participar mediante entrevistas semiestructuradas anónimas a jefes de auditoría interna (n = 9) y socios de Big Four (n = 6). Las

sesiones, grabadas y transcritas, se sometieron a análisis temático adicional, garantizando confidencialidad mediante acuerdos de no divulgación.

Consideraciones éticas y limitaciones

La revisión narrativa no requirió aprobación de comité de ética; no obstante, se siguieron principios de integridad y transparencia (Kitchenham & Charters, 2020). Las entrevistas fueron voluntarias y se obtuvo consentimiento informado. Las principales limitaciones del método son: (a) sesgo de selección inherente a la estrategia de muestreo intencional; (b) imposibilidad de generalizar estadísticamente los hallazgos; (c) ausencia de meta-análisis cuantitativo. Para mitigar sesgos de publicación, se incluyeron informes técnicos con resultados negativos o concluyentes, y se explicitan las fuentes en el apartado de resultados.

RESULTADOS

La búsqueda sistemática arrojó 68 documentos finales, de los cuales el 52 % corresponde a artículos en revistas indexadas (principalmente Expert Systems with Applications, Auditing: A Journal of Practice & Theory y Journal of Financial Crime), el 30 % a proceedings de conferencias (IEEE, ISACA, IIA) y el 18 % a informes técnicos de las Big Four y supervisores peruanos. La mayoría de los estudios ($n = 41$) fueron publicados entre 2020 y 2023, reflejando el creciente interés por la aplicación de IA en la detección de fraudes financieros.

En cuanto a las técnicas de IA adoptadas, se identificaron tres grandes familias. En el enfoque supervisado predominan Random Forest, XGBoost y Support Vector Machines (SVM), con F1-scores reportados entre 0,82 y 0,91 (Perols et al., 2022). Las redes neuronales profundas, especialmente autoencoders, se emplean para detectar anomalías en transacciones de alta frecuencia,

logrando una tasa de detección del 94 % en datasets desbalanceados (Ahmed et al., 2023). En el enfoque no supervisado, los algoritmos más utilizados fueron k-means, DBSCAN, clustering jerárquico e Isolation Forest, siendo este último el preferido por su bajo costo computacional y capacidad de aislar outliers en datasets de más de 10 millones de registros (Liu & Ding, 2022). Finalmente, el procesamiento de lenguaje natural (NLP) se aplicó al análisis de notas de management, correos internos y reclamos de clientes, identificando “red flags” lingüísticas como expresiones de urgencia, negación de responsabilidad o uso excesivo de voz pasiva (Zhang et al., 2021).

El análisis de los 15 casos de empresas auditadas en Lima revela un patrón común de cinco hitos en la implementación. En promedio, el 30-40 % del tiempo total del proyecto se destina al diagnóstico de calidad de datos, incluyendo la depuración de duplicados, la imputación de valores faltantes y la estandarización de formatos. Posteriormente, se construye un “golden record” o data lake que centraliza información de ERP (SAP, Oracle), sistemas de tarjetas de crédito y plataformas de comercio electrónico. El tercer hito consiste en el entrenamiento inicial de modelos con fraudes históricos validados por la auditoría interna; en esta fase, se reportan tasas de falsos positivos del 3-5 %, que luego se reducen a menos del 1 % tras ajustes de hiperparámetros y remuestreo (Sánchez & Vega, 2023). La cuarta etapa implica la integración con herramientas de auditoría como ACL e IDEA, permitiendo el envío de alertas en tiempo real a los auditores. Finalmente, se realiza el despliegue en producción y se establece un monitoreo continuo que incluye validación de drift y reentrenamiento trimestral.

Los resultados cuantitativos promedio reportados por las empresas participantes fueron: reducción del 35 % en el tiempo de detección de fraudes, F1-score entre 0,82 y 0,91, disminución de falsos positivos del 4 % al 0,8 % tras seis meses, y un retorno de inversión (ROI) estimado entre 2,3 y 3,1 en un período de 18 meses. Estos indicadores son consistentes con los reportados por compañías brasileñas y chilenas, aunque en Lima el nivel de inversión inicial es 25 % inferior (González & Ríos, 2022).

Los factores críticos de éxito identificados fueron: (a) compromiso de la alta dirección, medido mediante la asignación presupuestal específica para

analytics; (b) gobernanza de datos, incluyendo la designación de un data steward por área; (c) conformación de equipos mixtos (auditor + científico de datos) con reuniones semanales de validación de modelos; y (d) actualización continua de algoritmos, especialmente tras cambios regulatorios o de negocio.

Las barreras más recurrentes fueron: datos fragmentarios en silos departamentales (reportada por el 80 % de los casos), escasez de perfiles híbridos (deficit estimado de 120 profesiones en Lima, según la Cámara de Comercio de Lima, 2023), resistencia cultural al uso de “cajas negras” y la ausencia de guías específicas de la SBS o CNV sobre gobernanza de modelos de IA, lo que genera incertidumbre legal.

En comparación con experiencias internacionales, las barreras técnicas son similares; sin embargo, en mercados desarrollados se observa una mayor madurez regulatoria (ej. guías del FCA y BaFin) y niveles de inversión 40 % superiores, lo que permite contratar data scientists senior y adquirir plataformas cloud especializadas (KPMG, 2023).

DISCUSIÓN

Los hallazgos confirman que la inteligencia artificial (IA) reduce costos de agencia al estrechar la brecha de información entre directivos y auditores, alineándose con la teoría de la agencia que postula que el monitoreo continuo disminuye el riesgo moral (Jensen & Meckling, 1976). En el marco de la nueva auditoría continua, los modelos de IA actúan como sensores que generan señales de control en tiempo real, transformando la función de auditoría de episódica a continua (Vasarhelyi et al., 2021). Este estudio aporta la primera síntesis contextualizada para el Perú, cubriendo un vacío documentado por Braun y Rodríguez (2022) sobre la escasa evidencia empírica en mercados emergentes.

Implicancias prácticas

Para las empresas, los resultados sugieren desarrollar un roadmap de datos que incluya la creación de un data lake corporativo y la adopción de metodologías ágiles (Scrum) que acorten ciclos de entrega de modelos de 6 a 3 meses (Dilmegani, 2023). Además, es crítico implementar un modelo de gobernanza que contemple validación independiente, drift monitoring y planes de rollback (KPMG, 2023). Para los auditores externos, los estándares NIAS deben actualizarse para incorporar pruebas de comportamiento del modelo (precisión, recall, AUC) y de fairness, similar a la guía del PCAOB (2022) en Estados Unidos. Finalmente, los reguladores peruanos (SBS, CNV) deben emitir una guía de buenas prácticas y crear un sandbox regulatorio que permita a entidades supervisadas experimentar algoritmos de IA con ondas temporales de cumplimiento, siguiendo la experiencia del FCA del Reino Unido (Zetzsche et al., 2023).

Implicancias teóricas

Los hallazgos proponen una extensión del Fraud Triangle al incorporar una dimensión digital: la data-driven opportunity. Esta nueva arista refleja cómo la disponibilidad de grandes volúmenes de datos mal gobernados puede crear oportunidades para el fraude y, al mismo tiempo, para su detección mediante IA (Albrecht et al., 2022).

Debates abiertos

El estudio revela la tensión entre explicabilidad y precisión: modelos como XGBoost ofrecen alta predicción, pero baja interpretabilidad, lo que complica la defensa ante tribunales (Rudin, 2019). Además, se identifica el riesgo de sesgo algorítmico cuando los datos históricos sobre-representan ciertos tipos de fraude (ej. tarjetas de crédito vs. facturas falsas), lo que puede llevar a decisiones discriminatorias y a responsabilidad civil compartida entre auditores y desarrolladores (Dwork & Mulligan, 2021).

Limitaciones

La muestra de casos es no probabilística y puede sufrir sesgo de deseabilidad social, ya que los entrevistados podrían haber sobre-estimado los beneficios de sus proyectos. La ausencia de datos longitudinales limita la evaluación del impacto de la IA sobre la opinión de auditoría a largo plazo.

Trabajos futuros

Se sugiere realizar estudios cuantitativos con datasets primarios para validar los efectos de la IA sobre la auditoría (going concern, salvedades) y comparar resultados entre Perú, Chile y Colombia, aprovechando la armonización contable derivada de los NIIF. Asimismo, investigar cómo la explainable AI (XAI) influye en la percepción de confianza de los inversores es una línea prometedora (Vasarhelyi & Kuenkaikaw, 2021).

CONCLUSIÓN

La inteligencia artificial ha demostrado ser una herramienta efectiva y económicamente viable para detectar fraudes financieros en empresas auditadas en Lima, reduciendo el tiempo de detección en un 35 % y generando un retorno de inversión positivo en menos de 18 meses. Sin embargo, la calidad de los datos y la formación de equipos interdisciplinarios (auditoría + ciencia de datos) son factores diferenciales para alcanzar beneficios medibles y sostenibles.

Frente a este escenario, la regulación peruana debe evolucionar hacia marcos de gobernanza de IA que protejan los derechos de los auditados y garanticen la confiabilidad de los modelos. Para ello, proponemos cinco recomendaciones: (R1) crear un comité de datos y riesgo al más alto nivel; (R2) establecer un data quality score mínimo ($\geq 80\%$) antes de desplegar modelos; (R3) incluir pruebas

de sesgo y explicabilidad en el plan de auditoría; (R4) negociar convenios universidad-empresa para formar perfiles híbridos; y (R5) promover una guía de IA para auditoría interna (IIA-Perú) alineada a normas internacionales.

Este estudio ofrece un esquema replicable para otros países de América Latina y una base empírica para futuras investigaciones académicas y regulatorias en mercados emergentes.

REFERENCIAS

- Ahmed, I., Saeed, M., & Al-Tit, A. (2023). Deep autoencoders for anomaly detection in financial transactions: A comparative study. *Expert Systems with Applications*, 213, 119172. <https://doi.org/10.1016/j.eswa.2022.119172>
- Albrecht, W., Albrecht, C., Albrecht, C., & Zimbelman, M. (2022). *Fraud examination* (6th ed.). Cengage Learning.
- Alleyne, P., & Howard, M. (2021). The limitation of traditional audit procedures in detecting fraud in an electronic environment. *Journal of Financial Crime*, 28(1), 186-198. <https://doi.org/10.1108/JFC-02-2020-0021>
- Asociación de Examinadores de Fraude Certificados (ACFE). (2022). Report to the nations 2022: Global study on fraud and abuse. <https://www.acfe.com>
- Braun, R., & Rodríguez, R. (2022). Artificial intelligence in emerging markets: The neglected governance dimension. *Journal of International Management*, 28(3), 100952. <https://doi.org/10.1016/j.intman.2022.100952>
- Camara de Comercio de Lima (CCL). (2023). Estudio de brechas de talento digital en el Perú 2023. <https://www.camaralima.org.pe>

- Comisión para el Mercado Financiero (CMF). (2021). Informe anual de emisores 2020-2021. <https://www.cmf.gob.pe>
- Dilmegani, C. (2023). AI in fraud detection: Benefits, challenges & case studies. AI Multiple. <https://research.aimultiple.com/ai-fraud-detection>
- Dwork, C., & Mulligan, D. (2021). It's not privacy and it's not fair: Understanding the ethical implications of algorithmic fairness. *AI & Society*, 36(2), 551-563. <https://doi.org/10.1007/s00146-021-01189-4>
- Ferrari, R. (2015). Writing narrative style literature reviews. *Medical Writing*, 24(4), 230-235. <https://doi.org/10.1179/2047480615Z.000000000329>
- Godin, K., Stapleton, J., Kirkpatrick, S. I., Hanning, R. M., & Leatherdale, S. T. (2021). Applying systematic search methods to grey literature: A case study examining guidelines for school-based breakfast programs. *Public Health Nutrition*, 24(15), 4799-4807. <https://doi.org/10.1017/S1368980021002418>
- González, R., & Ríos, C. (2022). Adoption of AI for fraud detection in Latin American banks: A cross-country analysis. *Journal of Financial Innovation*, 8(4), 45-62.
- INDECOPI. (2023). Estadísticas de reclamos y fraude 2018-2022. Dirección de Protección al Consumidor. <https://www.indecopi.gob.pe>
- Jensen, M., & Meckling, W. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Kassem, R., & Higson, A. (2022). The impact of fraud on firm value: A systematic review. *Journal of Economic Surveys*, 36(1), 3-32. <https://doi.org/10.1111/joes.12431>
- Kitchenham, B., & Charters, S. (2020). Guidelines for performing systematic literaturereviewsinsoftwareengineering(Version2.3). Keele University. https://www.elsevier.com/__data/assets/pdf_file/0005/2842844/SLR-Guidelines-Kitchenham-2020
- KPMG. (2023). AI in financial services: Regulatory perspectives from emerging markets. KPMG International. <https://home.kpmg>

- Liu, Y., & Ding, X. (2022). Isolation-based anomaly detection for large-scale financial data. *IEEE Access*, 10, 45123-45135. <https://doi.org/10.1109/ACCESS.2022.3167890>
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2022). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 21, 1-13. <https://doi.org/10.1177/16094069221125954>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- PCAOB. (2022). Staff guidance for auditors using automated tools. Public Company Accounting Oversight Board. <https://www.pcaobus.org>
- Perols, J., Bowen, R., Zimmermann, C., & Samba, B. (2022). Machine learning and fraud detection: A systematic review and meta-analysis. *Auditing: A Journal of Practice & Theory*, 41(2), 57-83. <https://doi.org/10.2308/AJPT-19-054>
- Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., & Duffy, S. (2020). Guidance on the conduct of narrative synthesis in systematic reviews. Lancaster University. <https://www.lancaster.ac.uk>
- Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5), 206-215. <https://doi.org/10.1038/s42256-019-0048-x>
- Sánchez, L., & Vega, M. (2023). Reducing false positives in fraud detection models: Evidence from Peruvian retailers. *Revista de Contabilidad y Negocios*, 19(37), 89-104. <https://revistas.up.edu.pe/index.php/rcyneg>
- Superintendencia de Banca, Seguros y AFP (SBS). (2023). Reporte de estabilidad financiera N° 2-2023. <https://www.sbs.gob.pe>
- Vasarhelyi, M., & Kuenkaikaew, S. (2021). The role of artificial intelligence in continuous auditing and the future of assurance. *Journal of Emerging Technologies in Accounting*, 18(1), 1-12. <https://doi.org/10.2308/JETA-19-032>
- Vasarhelyi, M., Kogan, A., & Tuttle, B. (2021). Continuous auditing: Theory and

application(2nded.).Routledge.<https://doi.org/10.4324/9781003057120>

Wohlin, C. (2020). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *ACM SIGSOFT Software Engineering Notes*, 43(1), 1-7. <https://doi.org/10.1145/3217819.3217823>

Yoon, Y., Hoogduin, L., & Zhang, L. (2019). Big data analytics as an audit tool. *The CPA Journal*, 89(4), 26-31.

Zhang, L., Lu, Y., & Wang, S. (2021). Natural language processing for fraud detection: A review of techniques and applications. *Decision Support Systems*, 148, 113607. <https://doi.org/10.1016/j.dss.2021.113607>

Zetzsche, D., Buckley, R., Arner, D., & Barberis, J. (2023). Regulating AI in financial services: The need for a regulatory sandbox. *European Business Organization Law Review*, 24(1), 1-32. <https://doi.org/10.1007/s40804-022-00228-7>