Revista Ciencia & Tecnología

No. 33, 31 de enero de 2022
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Análisis de las técnicas de machine learning aplicadas en la detección de fraudes bancarios

Analysis of machine learning techniques applied in the detection of bank fraud

Msc. Carlos Vicente Jones- Ortiz[1]
carlos.jones@unae.edu.ec
ORCID: https://orcid.org/0000-0002-3132-7765

Jomar Elizabeth Guzmán – Seraquive[2]
jomar.guzman@educacion.gob.ec
ORCID: https://orcid.org/0000-0002-8387-8921

Recibido: 28/6/2021, Aceptado: 28/9/2021

RESUMEN
Se considera al aprendizaje automático o de máquinas (machine learning en inglés), como una subárea en el campo de la computación e informática, además de estar estrechamente ligada a la inteligencia artificial; el objetivo de esta técnica es lograr que los ordenadores aprendan, siendo un agente que mejore la experiencia; ha sido muy útil sobre todo para el análisis de investigaciones y procesos que generan grandes cantidades de datos; para el presente artículo se realiza una revisión documental sobre el estado del arte de los principales métodos de aprendizaje automáticos, basados en publicaciones y artículos de hace no más de dos año. Busca eliminar las necesidades de contar con conocimiento experto en el análisis de datos, sin embargo, la intuición del ser humano sigue siendo pieza clave y no puede ser reemplazada en su totalidad. El objetivo del artículo es analizar las técnicas de machine learning más utilizadas en la detección de fraudes bancarios conociendo, las métricas empleadas.

Palabras clave: Machine learning, inteligencia artificial, análisis de datos, fraudes bancarios

ABSTRACT
Machine learning or machine learning is considered a subarea in the field of computing and informatics, in addition to being closely linked to artificial intelligence; The objective of this technique is to make computers learn, being an agent that improves the experience; It has been very useful especially for the analysis of investigations and processes that generate large amounts of data; For this article, a documentary review is carried out on the state of the art of the main automatic learning methods, based on publications and articles

[1] Universidad Nacional de Educación
[2] Unidad educativa General Antonio Elizalde

No. 33, 31 de enero de 2022
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

from no more than two years ago. It seeks to eliminate the need for expert knowledge in data analysis, however, human intuition remains a key element and cannot be replaced in its entirety. The objective of the article is to analyze the most used machine learning techniques in the detection of bank fraud, knowing the metrics used.

Introducción

Con el pasar de los años, la inteligencia artificial ha evolucionado al punto de presentar diferentes metodologías de aprendizaje automático aplicadas a un sinnúmero de áreas en la vida cotidiana; actualmente, con la gran cantidad de documentos que se producen y publican en la web, es fundamental contar con herramientas tecnológicas que permita a las personas obtener, procesar y discernir información que le resulte de utilidad en su formación profesional. "Las técnicas de aprendizaje automático están experimentando un auge sin precedentes en diversos ámbitos, tanto en el mundo académico como en el empresarial, constituyendo una palanca de transformación relevante" (Calvo, Guzmán, & Ramos, 2018, p. 5). Con el desarrollo tecnológico que se evidencia, en el área de educación, empresarial, y con mucha presencia en los últimos años en temas de seguridad, el aprendizaje automático o de máquina, ha tomado principal relevancia con el objetivo de alcanzar un mayor y mejor entendimiento de toda la información que reposa en la nube.

Al ser esta una tecnología basada en patrones, es capaz de aprender relaciones y tendencias de manera automática, permitiendo integrar técnicas de gran capacidad de analítica como el machine learning, es posible entre otras cosas monitorear y configurar parámetros que colaboren en la detección de acciones que antes eran más difícil de prevenir. En la actualidad, diferentes empresas, sobre todo del área financiera, optan por esta alternativa para evaluar escenarios donde se evalúen clientes con perfiles riesgosos e inclusive determinar operaciones que signifiquen fraudes.

El objetivo del artículo es analizar las técnicas de machine learning mas utilizadas para la detección de fraude bancaria mediante una revisión de literatura generando conocimiento relacionado a las métricas empleadas.

Materiales y métodos

Se empleó una revisión de literatura con el fin de evidenciar las técnicas empleadas para la detección de fraudes bancarios, se revisaron artículos desde diferentes fuentes bibliográficas publicado en los años 2018 al 2020 con la finalidad de recabar información lo más actualizada posible. El objetivo es analizar la popularidad, características y eficiencia de las principales técnicas de minería de datos y machine learning desde el punto de vista que los investigadores exponen en función de la detección de fraudes bancarios.

Para garantizar la calidad y veracidad de la información consultada se aplican estrategias de búsqueda que garanticen un adecuado proceso de selección, se utilizaron bases de datos como Scopus, Scielo, Web of Science o IEEE Xplore; la selección se limita en función del título, palabras clave y el resumen que presenta cada artículo. Se evalúa el nivel de detalle que cada artículo ofrece,

ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

para ello se plantean preguntas que permiten identificar escenarios positivos y relevantes para la investigación como:
¿El artículo está enfocado en la detección de fraudes en entidades bancarias?
¿En el artículo se analizan y desarrollan una o más técnicas de machine learning?
¿Los autores utilizan métricas para la evaluación de la técnica utilizada?

En su mayoría las propuestas analizadas cumplen con las necesidades planteadas al detallar los procesos de detección de fraudes y la manera en que es posible evaluar su rendimiento.

Resultados y discusiones

Machine Learning en el sector bancario

El Machine Learning es una metodología para el análisis de datos que facilita el desarrollo de modelos analíticos. Hueso (2019) indica que "se refiere a la capacidad que tienen los ordenadores de aprender a partir de los datos, mediante el uso de algoritmos que permiten a la máquina cambiar su comportamiento" (pág. 20). Es una rama de la inteligencia artificial fundamentada en la idea que un sistema puede aprender de datos para así identificar patrones y tomar decisiones con una mínima intervención del agente humano.

Siddhant, Anish, Namita, & Arvind (2020) mencionan que esta disciplina se encuentra estrechamente ligada a la inteligencia artificial, la misma se plantea con la finalidad de abordar sistemas capaces de aprender automáticamente en un contexto de identificar patrones y conductas en una amplia base de datos.

El surgimiento del interés en el aprendizaje automático y el constante desarrollo de las tecnologías de la información y computación ha permitido que esta técnica evolucione a un contexto iterativo, ya que a medida que los modelos son expuestos a nuevos datos, éstos pueden aprender y adaptarse de forma independiente a través de cálculos previos, emitiendo resultados confiables.

Las entidades bancarias persiguen como meta primordial la maximización de utilidades y reducción de costos; para ello se enfocan en solventar factores ligados a aspectos sociales, políticos, económicos y tecnológicos (Fernández, 2019). En este último punto es común encontrar que, si bien los recursos tecnológicos significan un aporte en el desarrollo y mejora en la gestión de bienes y servicios hacia el cliente, son susceptibles también a generar formas de cometer delitos, principalmente lo que se conoce como fraude.
Dichos actos ilícitos desembarcan en pérdidas para los clientes y las entidades bancarias que además pierde credibilidad afectando a la larga su reputación y posicionamiento como empresa (Giraldo & Caimàn, 2019). El Machine Learning ha permitido el desarrollo e integración constante de alternativas que permite monitorear y controlar dichos ataques como por ejemplo sistemas de verificación de dirección, verificación de tarjeta.
Las herramientas con las que cuentan la inteligencia artificial hacen posible que, en el sector empresarial de forma específica en entidades financieras, se pueda elaborar una revisión de gran volumen de datos y de forma rápida (Henderson & Richard, 2020).

No. 33, 31 de enero de 2022
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Esto conlleva a una precisión en la identificación de las tarjetas de crédito, evitando que ingresen datos fraudulentos, conceder préstamos por medio de revisión automática sin tener previa entrevista con el cliente, entre otros.

Para Bataller (2019) el concepto propio del Machine Learning o aprendizaje automático hace referencia a la detección sistemática de conductas y patrones significativos en un grupo de datos. Por su parte Guillén (2019) indica que lo vuelve una herramienta fundamental para cualquier tarea de extracción de información en grandes volúmenes de datos.
Diferentes algoritmos de Machine Learning han presentado grandes resultados en diversas tareas, sobre todo al tratarse de visión por computadora, clasificación de documentos, conducción automática, reconocimiento biométrico (Suntaxi, Ordoñez, & Pesantes, 2018). Permitiendo que a partir de la información obtenida se genere un análisis exhaustivo de acciones y patrones imperceptibles para el humano.

Menese (2018) indican que aspectos como la computación en la nube y la evolución constante de tecnologías como el internet de las cosas han permitido el desarrollo y posicionamiento de diversas técnicas de minería de datos y aprendizaje automático. Ramírez, Jenkins, Martínez, & Quesada López (2020) mencionan que la regresión lineal simple o múltiple, redes neuronales artificiales, análisis de discriminante lineal, máquinas de soporte vectorial, árboles de decisión o Naive Bayes; se determinan como las principales técnicas utilizadas para la detección de fraudes en entidades bancarias.
Diferentes trabajos se han enfocado en determinar la eficiencia de estas en función de métricas que evalúan su rendimiento, simplicidad y comportamiento, por ellos partiendo de la revisión bibliográfica se mencionan las más utilizadas.

Redes neuronales

Para Sadgali, Sael, & Benannou (2019) mencionan que estas redes están basadas en la biología humana, esto significa que imitan el comportamiento de las neuronas en cuanto al aprendizaje se refiere. Para Bellido (2019) naturalmente esto únicamente en sus funcionalidades primarias, son una técnica de la inteligencia artificial que se encargan de realizar regresiones complejas sobre grandes volúmenes de datos.

Singh & Jain (2019) refieren que las características principales son: Aprendizaje desde la experiencia, sistematizan de ejemplos previos para la generación de nuevos y abstracción de los datos de entrada.

Esta técnica de detección según lo mencionado por los autores tiene su base en el aprendizaje automática de la máquina, de allí toma la información de entrada y la procesa las veces que sea necesaria, hasta establecer si contiene algún error.

Revista Ciencia & Tecnología
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Random forest
Se le denomina como clasificador capaz de discernir grandes cantidades de datos, trabajan con valores aleatorios semejando su funcionamiento a los árboles de decisión (Borja Robalino, Monleón Getino, & Rodellar, 2020). En la detección de fraudes utiliza la selección al azar de usuarios creando así nuevas entradas que a su vez permiten aprender el comportamiento pasado.

Naive bayes
Se enfoca en la probabilidad de ocurrencia, es muy preciso cuando se trata de manejar grandes cantidades de información (González & Ortiz, 2018). Según los casos que se ingresan como nuevas entradas realiza la interpretación de cada variable.

Máquinas vectoriales de soporte
Emplea un conjunto de datos que han sido introducidos previamente por el ente humano, estos son resultados de las observaciones de un entendido en el tema, a su vez sirven para el entrenamiento del sistema de aprendizaje (Bonsón & Ortega, 2019). Es importante mencionar que no siempre un individuo debe estar revisando los resultados obtenidos.

Modelos lineales generalizados logit, probit, log log
Trabaja con medios aleatorios y variables independientes, a su vez emplea el método de clasificación para el reconocimiento de patrones en usuarios que registren datos fraudulentos (Singla & Baliyan, 2019). Muestra datos que contienen mayor relevancia por ejemplo si se introducen 30 términos de entradas al realización la evaluación mediante este modelo solo arroja las respuestas más significativas.

En los documentos analizados se evidenció una concordancia en cuanto al uso de las técnicas para detectar el fraude bancario. Se evidenciaron 5 técnicas principales para la detección de fraudes detalladas en la siguiente tabla:

Tabla 1. Técnicas de Machine Learning para detectar el fraude

Técnicas	Porcentaje de técnicas principales en la revisión de literatura
Redes neuronales	(36%)
Random forest	(20%)
Naive Bayes	(16%)
Maquinas vectoriales de soporte	(16%)

Revista Ciencia & Tecnología

No. 33, 31 de enero de 2022
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Modelos lineales generalizados (Modelo logit, probit, log, log)	(12%)
Total	(100%)

Fuente: Elaboración de los autores

Según los resultados obtenidos se evidencia que la técnica aplicada de forma mayoritaria con un 36% es las red neuronal, seguida, por Random Forest con un 20%, de igual manera con un 16% respectivamente se encuentra Naive Bayes y las maquinas vectoriales de soporte, por último, con 12% los modelos lineales generalizados.

Una vez definida la popularidad de las técnicas de machine learning entre los autores, se analizan las métricas que los mismos utilizan para (Frola, y otros, 2019) evaluar la eficiencia de estas, para las métricas juegan un rol fundamental en problemas de clasificación donde se busca analizar algoritmos Machine y Deep Learning, facilitando así la elección del mejor algoritmo en función de un objetivo concreto.

Los autores mencionan diferentes métricas como accuracy, tabla de confusión, recall o curva ROC, para diferentes investigadores, la primera de estas es la más utilizada gracias a su comprensión para la evaluación general de un algoritmo y las facilidades de cálculo que presentan, por su parte recall o sensibilidad es una medida que permite establecer una proporción de casos positivos debidamente clasificados.

En cuanto a la eficiencia se encuentran referencias sobe otras métricas enfocadas al desempeño computacional de las plataformas y herramientas machine learning, estas son speed, scalability y execution time.

Tabla 2. Métricas utilizadas para la evaluación de técnicas machine learning

Métrica	Descripción	Porcentaje
Accurary	Clasificaciones predichas de manera correcta en función del total de incidencias	(58%)
Recall	Porcentaje de casos positivos debidamente clasificados	(20%)

Revista Ciencia & Tecnología
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

False positive rate	Precisión de una prueba de diagnóstico o aprendizaje	(10%)
Specificity	Porcentaje de casos positivos debidamente clasificados	(6%)
Índice kappa	K=Po-Pe/1-Pe -> donde Po es la proporción de accuarary observado por lo tanto Po = accurary	(6%)
Total		(100%)

Fuente: Elaboración de los autores

Si bien esta metodología no es del todo nueva, ha tomado nuevos propósitos y rutas basada en algoritmos de aprendizaje de máquina aplicados en diferentes contextos del mundo real como por ejemplo cálculos matemáticos complejos de Big data o simplemente ofertas y recomendaciones en línea.

Conclusiones

La revisión documental realizada permitió profundizar en los principales conceptos, definiciones y características del aprendizaje automático o de máquina (machine learning) y sus aplicaciones en cuanto a la seguridad y prevención de fraudes financieros; se pudo identificar las principales técnicas de machine learning expuestas por los autores de los artículos consultados de los años (2018 y 2019) donde se observa una tendencia alineada a la metodología de redes neuronales donde se especifican las ventajas debido a su capacidad de estimar modelos no lineales, que sirven sobre todo para la cuantificación del riesgo de crédito.

Otras técnicas destacadas son Random Forest y Naive bayes, mismas que se enfocan en la probabilidad de que ocurra un hecho aislado, manejando grandes cantidades de información, trabajando con valores aleatorios que semejan el funcionamiento de un árbol de decisión.

Se concluye mediante el estudio realizado que existen diferentes técnicas capaces de establecer herramientas eficientes que reduzcan el riesgo de fraude financiero en este tipo de instituciones, además que, las redes neuronales son las que mayor aceptación y predilección representa entre los autores, que se explica en el sentido en que cuenta con gran versatilidad para diferentes aplicaciones.

No. 33, 31 de enero de 2022
ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

Por su parte, la técnica Naive Bayes es simplista, y presenta una semántica sencilla que usa y genera conocimiento a través de análisis probabilísticos lo que la vuelve también una metodología popular entre los autores.

La exactitud o accurary es la métrica de mayor utilización, los principales valores de exactitud expuestos están entre el 70 y 99% en las diferentes implementaciones y técnicas de clasificación sobre todo en redes neuronales, convolucionales y máquinas vectoriales de soporte. Estas se enfocan en el tiempo que le toma al algoritmo arrojar resultados, por su parte alguna de ella se enfoca en el costo computacional.

Referencias

Bataller, R. (2019). *La era de la inteligencia artificial. Nuevas herramientas para los creadores .* San Juan : Unversidad Nacional de San Juan .

Bellido. (2019). Redes neuronales para predecir el comportamiento del conjunto de activos financieros más líquidos del mercado de valores peruano. *Revista Científica de la UCSA,*, 49-64. Retrieved from https://ucsa.edu.py/yeah/wp-content/uploads/2019/04/4_A0._Bellido-B.-Redes-neuronales-para-predecir-el-comportamiento_49-64.pdf

Bonsón, E., & Ortega, M. (2019). Big data, Iteligencia Artificial y Data Analitics (BIDA). *Dialnet*, 11-13.

Borja Robalino, R., Monleón Getino, A., & Rodellar, J. (2020). Estandarización de métricas de rendimiento para clasificadores Machine y Deep Learning. *Revista Ibérica de Sistemas e Tecnologias de Informação, 30*, 184-196. Obtenido de https://www.researchgate.net/profile/Antonio_Monleon-Getino/publication/342009715_Estandarizacion_de_metricas_de_rendimiento_para_clasificadores_Machine_y_Deep_Learning/links/5ede3d0392851cf13869078e/Estandarizacion-de-metricas-de-rendimiento-para-clasifi

Calvo, J., Guzmán, M., & Ramos, D. (2018). Machine Learning, una pieza clave en la transformación de los modelos de negocio. *Management Solutions*, 1 - 42. Retrieved from https://www.managementsolutions.com/sites/default/files/publicaciones/esp/machine-learning.pdf

Fernández, A. (2019). Inteligencia artificial en los servicios financieros. *Boletín Económico*, 1-10.

Frola, Chesñevar, Alvez, Etchart, Miranda, Ruiz, & Teze. (2019). *Framework SDF Machine Learning en transacciones financieras y detección temprana de fraudes.* In XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan)..

Giraldo, & Caimàn. (2019). Bigdata, Análisis Y Tendencias En La Economía Digital. *Eventos imteggrados*, 1-522.

ISSN impreso: 1390 - 6321
ISSN online: 2661 - 6734

González, E., & Ortiz, A. (2018). *Detección de Fraude en Tarjetas de Crédito mediante técnicas de mineria de datos .* Universidad Santo Tomás .

Guillén, R. (2019). *Sistemas para detectar fraude en medios de pago.* Madrid: Universidad Politécnica de Madrid.

Henderson, & Richard. (2020). Using graph databases to detect financial fraud. *Computer Fraud & Security*, 6-10. doi:10.1016/S1361-3723(20)30073-7

Hueso, L. (2019). Riesgos e impato del Big Data, la inteligencia artificla, y la róbotica. Enfoque modelos y principios de la respuesta del derecho. *Revista general del derecho administrativo*, 2-37.

Meneses, M. (2018). Grandes datos, grandes desafíos para las ciencias sociales. *Revista Mexicana de Sociología*, 415-444. Obtenido de http://www.scielo.org.mx/pdf/rms/v80n2/0188-2503-rms-80-02-415.pdf

Ramírez, A., J. M., Martínez, A., & Quesada López, C. (2020). Uso de técnicas de minería de datos y aprendizaje automático para la detección de fraudes en estados financieros: un mapeo sistemático de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 97 - 109.

Sadgali, Sael, & Benannou. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science*, 45-54.

Siddhant, B., Anish, G., Namita, G., & Arvind, G. (2020). Credit Card Fraud Detection using Pipeling and Ensemble Learning. *Procedia Computer Science, 173*, 104-112. doi:10.1016/j.procs.2020.06.014

Singh, A., & Jain, A. (2019). Adaptive Credit Card Fraud Detection Techniques Based on Feature Selection Method. *Advances in Computer Communication and Computational Sciences* (págs. 167-178). Singapore: Springer.

Singla, S., & Baliyan, N. (2019). Space Shuttle Landing Control Using Supervised Machine Learning. *Book Chapter published 2019 in Advances in Intelligent Systems and Computing*, 349-356. doi:doi.org/10.1007/978-981-13-1822-1_32

Suntaxi, M., Ordoñez, P., & Pesantes, M. (2018). Applications of Deep Learning in Financial Intermediation: A Systematic Literature Review. *KnE Engineering*, 47-60. doi:10.18502/keg.v3i9.3645