Revisión de literatura sobre las técnicas de Machine Learning en la detección de fraudes bancarios

Bone Miño Mary Bella

20 de octubre de 2023

Resumen

Este artículo discute el aprendizaje automático o de máquinas, una subárea de la computación e informática estrechamente ligada a la inteligencia artificial, cuyo objetivo es lograr que los ordenadores aprendan para mejorar la experiencia. Se destaca su utilidad en el análisis de investigaciones y procesos que generan grandes cantidades de datos, y se realiza una revisión documental sobre los principales métodos de aprendizaje automático empleados para la detección de fraudes financieros en publicaciones y artículos de los últimos dos años.

1. INTRODUCCIÓN

La inteligencia artificial ha evolucionado con el tiempo, desarrollando diferentes metodologías de aprendizaje automático que se aplican a una amplia gama de áreas de la vida cotidiana. En la actualidad, con la gran cantidad de información disponible en línea, es esencial contar con herramientas tecnológicas que permitan a las personas obtener, procesar y comprender la información que necesitan para su formación profesional. Por esta razón, las técnicas de aprendizaje automático están experimentando un crecimiento sin precedentes en diversos ámbitos, tanto en el mundo académico como en el empresarial, lo que constituye una herramienta de transformación importante. [9] El aprendizaje automático es una herramienta poderosa que puede utilizarse para detectar fraudes financieros.

En este artículo, presenta un análisis documental de los principales métodos de aprendizaje automático que se utilizan para la detección temprana de fraudes financieros.

2. FUNDAMENTO TEÓRICO

Antes de proceder a la revisión teórica, es preciso considerar las investigaciones relativas al uso del Machine Learning en la detección de fraudes bancarios;

Los algoritmos KNN y Naive Bayes pueden identificar fraudes con tarjetas crediticias con una precisión del 98Porciento. [3]

Los algoritmos de aprendizaje automático para detectar fraudes con tarjetas de crédito deben utilizar información del entorno real para identificar variables significativas que pueden indicar un fraude. [17]

Los algoritmos de aprendizaje automático pueden identificar fraudes bancarios virtuales con una precisión del 95Porciento. [16]

Los algoritmos de aprendizaje automático Random Forest, SVM y regresión logística son efectivos para detectar fraudes con tarjetas de crédito y débito, tanto en transacciones virtuales como físicas. [12]

Emplearon Random Forest y Adaboost identificando que el primero presenta un mejor desempeño en la detección de fraudes en entidades bancarias por medio de transacciones virtuales. [1]

Los investigadores han demostrado que los fraudes bancarios son un problema creciente. Esto se debe a que los clientes cada vez realizan más operaciones bancarias por medios electrónicos, lo que los hace más vulnerables a los ataques de los hackers. Los fraudes bancarios pueden causar pérdidas económicas significativas para los bancos, así como dañar su imagen y la confianza de los clientes. Por esta razón, es importante que los bancos implementen medidas de prevención de fraudes.

3. Inteligencia artificial

La inteligencia artificial es la capacidad de las máquinas para realizar tareas que normalmente se consideran propias de los seres humanos, como el aprendizaje, el razonamiento y la toma de decisiones, está presente en muchos aspectos de nuestra vida, desde los juegos en línea hasta los automóviles autónomos.

Esta tiene como objetivo convertirse en una herramienta esencial en todos los ámbitos de la sociedad. Esto se lograría gracias al desarrollo de sistemas inteligentes, algoritmos y técnicas de aprendizaje automático. [4]

La inteligencia artificial utiliza el big data para recopilar y analizar grandes cantidades de datos. Estos datos pueden ser personales, empresariales o de cualquier otro tipo. El análisis de estos datos se realiza mediante algoritmos que permiten generar relaciones, parámetros y modelos. [13]

El aprendizaje profundo es un tipo de aprendizaje automático que utiliza redes neuronales artificiales para aprender de los datos. Estas redes neuronales están formadas por una serie de capas que se van conectando entre sí. Cada capa aprende un patrón diferente de los datos, y las capas más complejas son capaces de aprender patrones más complejos. [11]

El Deep Learning tiene gran acogida en diferentes áreas pero dos de éstas son parte de lastécnicas de aprendizaje en inteligencia artificial :

- Reconocimiento de voz e imágenes: El aprendizaje profundo es una herramienta que se utiliza tanto en el sector empresarial como académico. Se utiliza en aplicaciones como Skype y Siri para el reconocimiento de

patrones de voz. También se utiliza para generar subtítulos y detalles de imágenes de forma automática. [2]

- Sistemas de recomendación: Realizan las recomendaciones en base a las preferencias de los clientes [14]

4. Machine Learning

El machine learning es una rama de la inteligencia artificial que permite a las máquinas aprender de los datos sin ser programadas explícitamente. Esto se logra mediante el uso de algoritmos que permiten a las máquinas identificar patrones en los datos y utilizarlos para mejorar su rendimiento. [18]

El aprendizaje automático es una técnica que permite a las máquinas aprender de los datos sin ser programadas explícitamente. Se utiliza en una amplia gama de aplicaciones, desde el reconocimiento facial hasta las recomendaciones de productos.

5. Machine Learning en el sector bancario

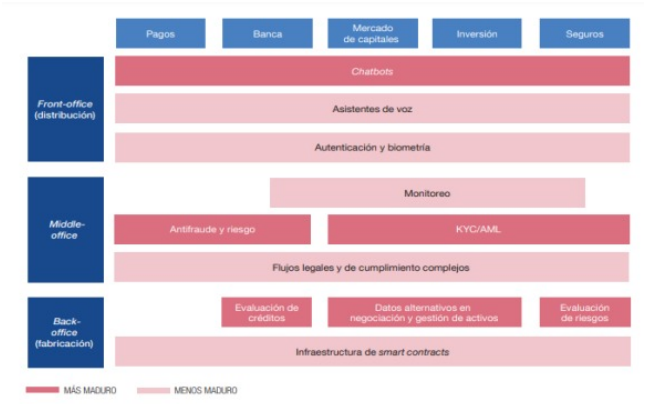

Figura 1: Funcionamiento del Machine Learning en el sector financiero [8]

La inteligencia artificial permite a las empresas financieras revisar grandes volúmenes de datos de forma rápida y precisa. Esto ayuda a las empresas a identificar tarjetas de crédito fraudulentas, conceder préstamos sin entrevistar al cliente y tomar otras decisiones importantes. [7]

6. PROCEDIMIENTOS METODOLOGICOS

Se empleó una revisión de literatura que comprende un análisis bibliográfico, la investigación documental es un proceso que permite la recuperación de información publicada sobre un tema en particular. Este proceso implica la selección, evaluación y síntesis de la documentación, de acuerdo con los objetivos del estudio que se lleva a cabo. [10]

Se revisaron 22 artículos sobre técnicas para detectar fraudes bancarios utilizando términos específicos en bibliotecas académicas como Google académico, Dialnet, Scielo y Crossref. Los artículos seleccionados corresponden al período entre 2018 y 2019, y se enfocan en identificar los algoritmos de Machine Learning que se utilizan para detectar fraudes financieros.

7. RESULTADOS Y DISCUSIÓN

En los 22 documentos analizados se evidenció una concordancia en cuanto al uso de las técnicas para detectar el fraude bancario. Así, se evidenciaron 5 técnicas principales para la detección de fraudes detalladas en la siguiente tabla:

Técnicas	Porcentaje de técnicas principales en la revisión de literatura
Redes neuronales	7 (32%)
Random forest	5 (23%)
Naive Bayes	4 (18%)
Maquinas vectoriales de soporte	4 (18%)
Modelos lineales generalizados (Modelo logit, probit, log-log)	2 (9%)
Total	**22 (100%)**

Figura 2: Técnicas de Machine Learning para detector el fraude

Según los resultados obtenidos se evidencia que la técnica aplicada de forma mayoritaria con un 32Porciento es la Red Neuronal, seguida, por Random Forest con un 23Porciento, de igual manera con un 18Porciento respectivamente se encuentra Naive Bayes y las máquinas vectoriales de soporte, por último con 9Porciento los modelos lineales generalizados.

En el caso de las redes neuronales, identificadas como las de mayor uso en la detección de fraudes, estas técnicas se basan en los procesos biológicos del cerebro humano, lo que implica que imitan la forma en que las neuronas aprenden, aunque solo se enfocan en sus funciones principales. Se trata de una

técnica de inteligencia artificial que se encarga de realizar análisis complejos de grandes cantidades de datos. [5]

Expusieron la importancia del uso de algoritmos de aprendizaje automático que hagan uso de datos reales con la intención de poder predecir y prevenir fraudes en transacciones electrónicas por medio del reconocimiento de variables destacadas en aquellas acciones irregulares que se detecten. [17]

Los autores sugirieron que los métodos de aprendizaje automático pueden ayudar a identificar transacciones fraudulentas en la banca virtual. Estos métodos funcionan de manera similar al cerebro humano, identificando patrones en los datos que pueden indicar actividad fraudulenta. La minería de datos se utiliza para identificar estos patrones, y la precisión de esta metodología puede alcanzar hasta un 95Porciento. [16]

Consideró que Random Forest posee una exactitud en la detección de fraudes del 97.7Porciento, es decir mayor a las redes neuronales. [12]

El algoritmo Naive Bayes se basa en la probabilidad de ocurrencia de los eventos. Es muy preciso cuando se trata de manejar grandes cantidades de datos. Según los casos que se ingresan como nuevas entradas, el algoritmo interpreta las variables para determinar la probabilidad de que un evento ocurra. [6]

Las máquinas vectoriales de soporte (SVM) se utilizan para clasificar y predecir datos. Son eficientes y precisas, pero su implementación es compleja. [15]

Los modelos lineales generalizados (GLM) son una técnica de aprendizaje automático que se utiliza para clasificar datos. Los GLM trabajan con medios aleatorios y variables independientes, y son capaces de identificar patrones complejos en los datos. Son útiles para la detección de fraudes porque pueden identificar datos que contienen mayor relevancia. Por ejemplo, si se introducen 30 términos de entrada a la realización, la evaluación mediante un modelo GLM solo arrojará las respuestas más significativas. [9]

8. Conclusiones

El artículo comienza con una revisión de los principales conceptos, definiciones y características del aprendizaje automático. Luego, identifica las principales técnicas de Machine Learning aplicadas a la seguridad y prevención de fraudes financieros.

Las redes neuronales son la técnica más popular, debido a su versatilidad y capacidad de estimar modelos no lineales. Esto es importante porque los fraudes financieros a menudo son complejos y no siguen patrones lineales.

Otras técnicas destacadas son Random Forest y Naive Bayes. Random Forest es un conjunto de árboles de decisión, lo que lo hace efectivo para manejar grandes cantidades de información. Naive Bayes es un algoritmo probabilístico simple, pero efectivo.

El estudio concluye que las técnicas de Machine Learning son una herramienta eficaz para la prevención de fraudes financieros. Sin embargo, presenta algunas limitaciones, como la falta de estudios a nivel de naciones y la antigüedad de las

publicaciones consultadas. Estas limitaciones podrían ser abordadas en futuras investigaciones.

Referencias

[1] Credit card fraud detection using machine learning. 2020.

[2] W. Arellano. El derecho a la transparencia algorítmica en big data e inteligencia artificial, 2019.

[3] J.and Adetunmbi A. Awoyemi and Oluwadare S. *Credit card fraud detection using machine learning techniques: A comparative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI).* IEEE, 2017.

[4] R. Bataller. La era de la inteligencia artificial. nuevas herramientas para los creadores, 2019.

[5] Bellido. Redes neuronales para predecir el comportamiento del conjunto de activos financieros más líquidos del mercado de valores peruano. *Revista Científica de la UCSA*, pages 49–64, 2019.

[6] González E. and Ortiz A. Detección de fraude en tarjetas de crédito mediante técnicas de mineria de datos, 2018.

[7] Frola, Chesñevar, Alvez, Etchart, Miranda, Ruiz, and Teze. Framework sdf machine learning en transacciones financieras y detección temprana de fraudes. 2019.

[8] Giraldo and Caimàn. Bigdata, análisis y tendencias en la economía digital. 2019.

[9] Calvo J. and Guzmán M.and Ramos D. *Machine Learning, una pieza clave en la transformación de los modelos de negocio.* Management Solutions, 2019.

[10] Hurtado J. *Metodología de la investigación. Guía para la compresión holística de la ciencia.* Quirón Ediciones, Caracas, cuarta edition, 2020.

[11] Kamlofsky J., Miana V., and Gonzalez E. Uso de técnicas de inteligencia artificial para el análisis del impacto de ambientes contaminantes en el índice de daño génetico. *Revista abierta de informática Aplicada (RAIA)*, pages 11–34, 2019.

[12] Campus K. Credit card fraud detection using machine learning models and collating machine learning models. *International Journal of Pure and Applied Mathematics*, 118(20):825–838, 2018.

[13] Hueso L. Riesgos e impactos del big data, la inteligencia artificial, y la robótica. enfoques, modelos y principios de la respuesta del derecho. *Revista general del derecho administrativo*, pages 50–17, 2019.

[14] Paràmo L. Inteligencia artificial:¿ más peligros que beneficios? *Revista Ideales*, pages 1–6, 2019.

[15] Morteza. Machine learning: A convergence of emerging technologies in computing. pages 181–192, 2018.

[16] Yee O., Sagadevan S., and Malim N. Credit card fraud detection using machine learning as data mining technique. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 10(1-4):23–27, 2018.

[17] Dhankhad S., Mohammed E., and Far B. Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. in 2018 ieee international conference on information reuse and integration (iri). *IEEE*, pages 122–125, 2018.

[18] Zepeda. Los big data: conceptos relacionados y algunas aplicaciones en pediatría. *Revista Chilena de Pediatría*, pages 376–383, 2019.