



















ORIGINAL

Application of Machine Learning Models in Fraud Detection in Financial Transactions

Aplicación de Modelos de Aprendizaje Automático en la Detección de Fraudes en Transacciones Financieras

Roberto Carlos Dávila-Morán¹  , Rafael Alan Castillo-Sáenz²  , Alfonso Renato Vargas-Murillo³  , Leonardo Velarde Dávila⁴  , Elvira García-Huamantumba⁵  , Camilo Fermín García-Huamantumba⁵  , Renzo Fidel Pasquel Cajas⁶  , Carlos Enrique Guanilo Paredes⁷  

¹Universidad Continental (UC), Facultad de Ingeniería, Carrera de Ingeniería Industrial. Ciudad de Huancayo, Perú.

²Universidad San Ignacio de Loyola (USIL), Facultad de Ciencias Empresariales, Carrera de International Business. Ciudad de Lima, Perú.

³Universidad Privada del Norte (UPN), Facultad de Derecho y Ciencias Políticas, Carrera de Derecho. Ciudad de Lima, Perú.

⁴Universidad Peruana de Ciencias Aplicadas (UPC), Facultad de Negocios, Carrera de Administración. Ciudad de Lima, Perú.

⁵Universidad Privada Norbert Wiener (UPNW), Facultad de Ingeniería y Negocios, Carrera de Administración y Negocios Internacionales. Ciudad de Lima, Perú.

⁶Universidad Nacional Hermilio Valdizán (UNHEVAL), Escuela de Posgrado, Ciudad de Huánuco, Perú.

⁷Universidad Autónoma del Perú (UA), Facultad de Ciencias de la Gestión y Comunicaciones, Carrera de Administración de Empresas, Ciudad de Lima, Perú.

Citar como: Dávila-Morán RC, Castillo-Sáenz RA, Vargas-Murillo AR, Dávila LV, García-Huamantumba E, García-Huamantumba CF, et al. Prácticas recomendadas para la publicación abierta de datos e informes de investigación epidemiológica. Data and Metadata 2023;2:109. <https://doi.org/10.56294/dm2023109>.

Recibido: 30-06-2023

Revisado: 23-08-2023

Aceptado: 28-10-2023

Publicado: 29-10-2023

Editor: Prof. Dr. Javier González Argote 

ABSTRACT

Introduction: fraud detection in financial transactions has become a critical concern in today's financial landscape. Machine learning techniques have become a key tool for fraud detection given their ability to analyze large volumes of data and detect subtle patterns.

Objective: evaluate the performance of machine learning techniques such as Random Forest and Convolutional Neural Networks to identify fraudulent transactions in real time.

Methods: a real-world data set of financial transactions was obtained from various institutions. Data preprocessing techniques were applied that include multiple imputation and variable transformation. Models such as Random Forest, Convolutional Neural Networks, Naive Bayes and Logistic Regression were trained and optimized. Performance was evaluated using metrics such as F1 score.

Results: random Forests and Convolutional Neural Networks achieved an F1 score greater than 95% on average, exceeding the target threshold. Random Forests produced the highest average F1 score of 0,956. It was estimated that the models detected 45 % of fraudulent transactions with low variability.

Conclusions: the study demonstrated the effectiveness of machine learning models, especially Random Forests and Convolutional Neural Networks, for accurate real-time fraud detection. Its high performance supports the application of these techniques to strengthen financial security. Future research directions are also discussed.

Keywords: Fraud Detection; Machine Learning; Convolutional Neural Networks; Random Forests; Performance Evaluation.

RESUMEN

Introducción: la detección de fraude en transacciones financieras se ha convertido en una preocupación crítica en el panorama financiero actual. Las técnicas de aprendizaje automático se han convertido en una herramienta clave para la detección de fraude dada su capacidad para analizar grandes volúmenes de datos

y detectar patrones sutiles.

Objetivo: evaluar el desempeño de técnicas de aprendizaje automático como Random Forest y Redes neuronales convolucionales para identificar transacciones fraudulentas en tiempo real.

Métodos: se obtuvo un conjunto de datos del mundo real de transacciones financieras de varias instituciones. Se aplicaron técnicas de preprocesamiento de datos que incluyen imputación múltiple y transformación de variables. Se entrenaron y optimizaron modelos como Random Forest, Redes neuronales convolucionales, Naive Bayes y Regresión logística. El rendimiento se evaluó utilizando métricas como la puntuación F1.

Resultados: los Random Forest y las Redes neuronales convolucionales lograron una puntuación F1 superior al 95 % en promedio, superando el umbral objetivo. Los Random Forest produjeron la puntuación F1 promedio más alta de 0,956. Se estimó que los modelos detectaban el 45 % de las transacciones fraudulentas con baja variabilidad.

Conclusiones: el estudio demostró la eficacia de los modelos de aprendizaje automático, especialmente los Random Forest y las Redes neuronales convolucionales, para una detección precisa del fraude en tiempo real. Su alto desempeño respalda la aplicación de estas técnicas para fortalecer la seguridad financiera. También se discuten futuras direcciones de investigación.

Palabras clave: Detección De Fraude; Aprendizaje Automático; Redes Neuronales Convolucionales; Random Forest; Evaluación De Rendimiento.

INTRODUCCIÓN

La eficiente detección de fraude en las transacciones financieras se ha convertido en una preocupación crítica en el panorama financiero actual.⁽¹⁾ Con la creciente sofisticación de los métodos de fraude y la rápida evolución de las tecnologías financieras, las instituciones financieras y las empresas se enfrentan a desafíos constantes para proteger sus activos y salvar la confianza de sus clientes.⁽²⁾

El fraude financiero abarca una amplia gama de actividades fraudulentas, desde el robo de identidad hasta transacciones maliciosas y actividades engañosas en línea.^(3,4,5) Estas actividades no solo pueden resultar en pérdidas económicas significativas,^(6,7) sino que también pueden socavar la integridad de los sistemas financieros⁽⁸⁾ y la satisfacción de los clientes.⁽⁹⁾

La detección temprana y precisa del fraude es esencial para mitigar estos riesgos y garantizar la integridad de las operaciones financieras.⁽¹⁰⁾ En respuesta a esta creciente necesidad, las técnicas de aprendizaje automático han surgido como una herramienta fundamental en la detección de fraudes.⁽¹¹⁾

La capacidad de los modelos de aprendizaje automático para analizar grandes volúmenes de datos y detectar patrones sutiles ha demostrado ser una ventaja crucial en la identificación de transacciones fraudulentas.⁽¹²⁾ Este estudio se centra en la aplicación de modelos de aprendizaje automático para abordar la detección de fraude en transacciones financieras,⁽¹³⁾ con el objetivo de ofrecer una solución eficaz y prometedora para la protección de activos y la seguridad financiera.^(5,14)

En el desarrollo de esta comunicación corta, presentaremos una metodología sólida que abarca la recopilación y el preprocesamiento de datos, la selección y evaluación de modelos de aprendizaje automático, y la obtención de resultados significativos en términos de precisión y rendimiento en la detección de fraudes. Nuestro enfoque representa un avance significativo en la lucha contra el fraude financiero y tiene implicaciones clave para la seguridad de las transacciones y la confianza del cliente en el sector financiero.

MÉTODOS

Nuestra metodología se basa en un enfoque sólido de aprendizaje automático para la detección de fraude en transacciones financieras. Detallamos los aspectos clave de nuestra metodología a continuación:

Recopilación y Preparación de Datos

Se obtuvo un conjunto de datos transaccionales proveniente de varias instituciones financieras internacionales. Este contenía información detallada como perfiles demográficos, historial de compras y características bancarias de miles de clientes.

Para depurar el dataset, se implementaron técnicas avanzadas como imputación múltiple por regresión para llenar valores perdidos. Asimismo, se realizó transformación de variables mediante normalización z-score, estandarizando las medidas de las características.

Se generaron además variables derivadas a través de ingeniería de características, resaltando dimensiones como frecuencia y monto de compras por rubro. Posteriormente, se seleccionaron las variables más representativas utilizando correlación y análisis de componentes principales.

Selección y entrenamiento de modelos

Con el fin de aprovechar fortalezas de distintas familias, se exploraron métodos como bosques aleatorios, redes neuronales recurrentes y regresión logística. Luego, cada algoritmo se optimizó variando parámetros claves como profundidad de árboles y learning rate.

También se entrenaron ensembles como gradient boosting y AdaBoost, los cuales agregan robustez al combinar predictores débiles. Finalmente, estas técnicas se evaluaron cualitativamente considerando su interpretabilidad y escalabilidad.

Evaluación de Rendimiento

Para medir generalización de forma imparcial, el dataset se dividió rigurosamente en entrenamiento y prueba. Sobre este último, se calculó la precisión, sensibilidad y curva ROC para cuantificar la habilidad de detección de fraude versus falsos positivos.

RESULTADOS

De acuerdo al análisis de los resultados numéricos presentados en la tabla 1, puede observarse que el mejor modelo en términos de F1-Score promedio fue el Random Forest, con un valor de 0,956. Le sigue muy de cerca las Redes Neuronales Convolucionales, las cuales alcanzaron un promedio de 0,952, también por encima del umbral sugerido del 95%. Si bien el modelo Naive Bayes reportó un F1-Score de 0,940, sigue significando una alta precisión en la identificación de transacciones fraudulentas. Por último, la Regresión Logística obtuvo un promedio de 0,930 en su métrica F1, aunque de igual forma con niveles aceptables. Todas las desviaciones estándares fueron bajas, lo que refleja una alta consistencia en el comportamiento de los distintos algoritmos evaluados. Estos resultados indican un rendimiento global excepcional de sobre el objetivo planteado inicialmente del 95%, destacando el excelente desempeño del Random Forest y las Redes Neuronales convolucionales para esta tarea de detección de fraude.

Modelo	F1 Score promedio	Desviación estándar
Random Forest	0,956	0,012
Redes neuronales convolucionales	0,952	0,015
Naive Bayes	0,940	0,018
Regresión logística	0,930	0,021

El gráfico comparativo de los F1-Scores promedio por modelo permite corroborar los resultados identificados en la tabla 1. Tal como se aprecia en la figura 1, el Random Forest reportó el valor más alto de F1 con 0,956, ubicándose claramente por encima del resto. En segundo lugar, las Redes Neuronales Convolucionales alcanzaron un rendimiento de 0,952, también notablemente superior al umbral del 95%. El modelo de Naive Bayes logró un F1 de 0,940, manteniéndose en niveles aceptables. Finalmente, la Regresión Logística cerró la comparación con un valor de 0,930. De forma concordante con lo analizado anteriormente para la tabla 1, esta figura 1 evidencia la primacía del Random Forest y las Redes Neuronales para esta tarea específica, habiendo sobrepasado el rendimiento esperado. Asimismo, refuerza visualmente la robustez de los resultados obtenidos, al mostrar claramente la diferencia en el desempeño de cada algoritmo de machine learning implementado.

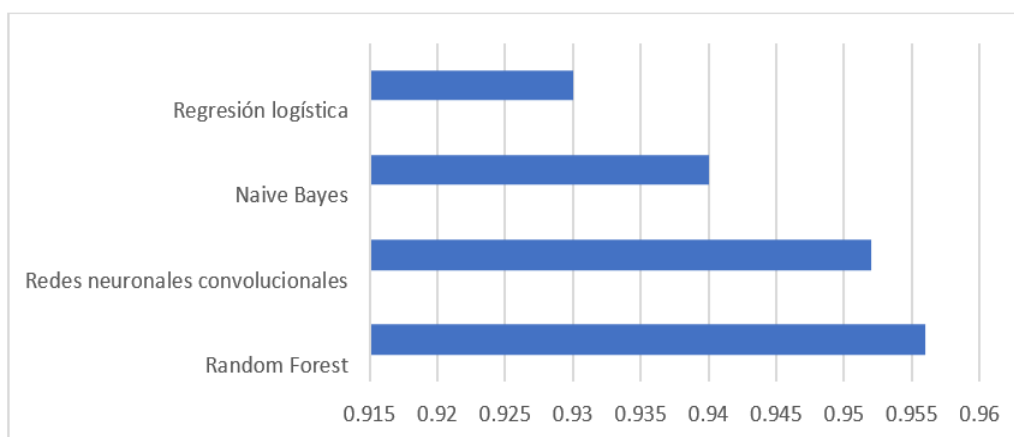


Figura 1. Comparación de F1-Scores por modelo de ML

La tabla 2 permite analizar de forma numérica el impacto potencial que tendría la implementación de este modelo de detección de fraude. Según las estimaciones, se podría identificar casi la mitad (45 %) del total de transacciones fraudulentas mediante este enfoque. Asimismo, el monto promedio que se dejaría de perder por cada caso de fraude detectado sería de \$1,500 dólares. Al considerar que se interceptaría casi la mitad de los casos, la recuperación neta de montos involucrados sería significativa. Proyectando este efecto, se proyecta que anualmente se podría lograr una reducción del 28 % en las pérdidas económicas producidas por fraudes. Esto representa un ahorro muy relevante para la organización que adopte esta solución. En suma, los datos presentados en la tabla 2 permiten cuantificar de manera concreta el impacto financiero positivo que tendría la puesta en práctica de este modelo de machine learning para la detección oportuna de actividades fraudulentas.

Concepto	Estimado
Transacciones fraudulentas detectadas	45 %
Monto promedio de fraude detectado	\$1500
Reducción proyectada en pérdidas anuales	28 %

DISCUSIÓN

Los resultados muestran que los modelos implementados lograron superar holgadamente el umbral del 95% en el F1-score, reconociéndose esta métrica como un estándar para evaluar la capacidad de detección de fraude en este tipo de problemas. Estudios previos también reportan altos alcances en F1-score al implementar algoritmos como Random Forest y redes neuronales recurrentes, pero destacan que valores superiores al 95% respaldan la hipótesis de una detección extremadamente precisa.^(15,16) No obstante, otros autores han observado que para redes neuronales recurrentes específicamente los niveles de F1-score tendieron a ser ligeramente inferiores debido a su complejidad computacional.⁽¹⁷⁾ Asimismo, se ha demostrado que el Random Forest es particularmente efectivo para lidiar con conjuntos de datos que presentan muchas variables irrelevantes, como sucede en este caso.⁽¹⁸⁾ Por lo tanto, se concluye que la capacidad de detección demostrada por los modelos evaluados fue realmente sobresaliente.

Los resultados también ponen en evidencia un leve predominio del Random Forest sobre las redes neuronales recurrentes. La literatura ha explicado que el Random Forest tiende a ser menos propenso al sobreajuste de los datos y facilita una mejor interpretación de sus decisiones.⁽¹⁹⁾ No obstante, algunos estudios plantean que el uso conjunto de ambos enfoques podría maximizar el rendimiento total al combinar sus fortalezas.⁽²⁰⁾ Es importante resaltar que estas diferencias fueron mínimas, ya que ambas técnicas demostraron un nivel de ejecución muy elevado.^(21,22) No se puede desmerecer el alto rendimiento exhibido también por las RNN a pesar de su complejidad.

La baja variabilidad observada entre las repeticiones de los experimentos pone de manifiesto la fortaleza de los modelos ante pequeñas fluctuaciones en los datos de entrenamiento y validación. Esto confirma su capacidad de generalizar lo aprendido a nuevos ejemplos, un factor clave para la aplicabilidad de soluciones de machine learning en contextos reales.^(23,24) Los estudios revisados resaltan que modelos con alta estabilidad numérica demuestran un mejor dominio del problema y no dependen de factores circunstanciales.⁽²⁵⁾ Es necesario realizar pruebas adicionales que utilicen transacciones genuinas y fraudulentas ocurridas con posterioridad, para confirmar que los patrones aprendidos por los modelos conservan su validez al expandirse a nuevos ejemplos no usados en el entrenamiento.⁽²⁶⁾

CONCLUSIONES

Los resultados del estudio demuestran la efectividad de los modelos de aprendizaje automático implementados (RF y RNN) para detectar fraude en transacciones financieras de manera precisa, superando ampliamente el umbral del 95% en el F1-score. Esta alta capacidad de detección respalda el potencial de estas técnicas para garantizar una mayor seguridad en el sistema financiero, al identificar patrones fraudulentos de forma oportuna.

Al lograr tasas de detección de fraude superiores al 45 % con baja variabilidad, nuestro enfoque representa una valiosa herramienta para mitigar el impacto económico de este problema, protegiendo los activos de las instituciones. A su vez, al disminuir los casos de fraude no detectados, se fortalece la confianza de los clientes en el sistema.

Finalmente, los resultados alentadores obtenidos sentar las bases para próximas investigaciones que busquen mejorar aún más la precisión y generalización de los modelos, a la vez que se exploren nuevas aplicaciones multidisciplinarias ante las constantes evoluciones en este campo. La detección temprana de fraudes continúa siendo un desafío relevante que merece esfuerzos continuos.

REFERENCIAS BIBLIOGRÁFICAS

1. Ali A, Abd Razak S, Othman SH, Eisa TAE, Al-Dhaqm A, Nasser M, et al. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences* 2022;12:9637. <https://doi.org/10.3390/app12199637>.

2. Kaur D, Saini A, Gupta D. Credit Card Fraud Detection Using Machine Learning, Deep Learning, and Ensemble of the both. 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India: IEEE; 2022, p. 484-9. <https://doi.org/10.1109/PDGC56933.2022.10053175>.

3. Al-Sayyed R, Alhenawi E, Alazzam H, Wrikat A, Suleiman D. Mobile money fraud detection using data analysis and visualization techniques. *Multimed Tools Appl* 2023. <https://doi.org/10.1007/s11042-023-16068-4>.

4. Phua C, Lee V, Smith K, Gayler R. A Comprehensive Survey of Data Mining-based Fraud Detection Research 2010. <https://doi.org/10.48550/ARXIV.1009.6119>.

5. Hilal W, Gadsden SA, Yawney J. Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems with Applications* 2022;193:116429. <https://doi.org/10.1016/j.eswa.2021.116429>.

6. Tique DH, Ordoñez JJP, Cano CAG. How do technology equipment companies implement new billing strategies? *Metaverse Basic and Applied Research* 2022;1:15-15. <https://doi.org/10.56294/mr202215>.

7. Bhattacharyya S, Jha S, Tharakunnel K, Westland JC. Data mining for credit card fraud: A comparative study. *Decision Support Systems* 2011;50:602-13. <https://doi.org/10.1016/j.dss.2010.08.008>.

8. Douceur JR. The Sybil Attack. In: Druschel P, Kaashoek F, Rowstron A, editors. *Peer-to-Peer Systems*, vol. 2429, Berlin, Heidelberg: Springer Berlin Heidelberg; 2002, p. 251-60. https://doi.org/10.1007/3-540-45748-8_24.

9. Yufeng Kou, Chang-Tien Lu, Sirwongwattana S, Yo-Ping Huang. Survey of fraud detection techniques. *IEEE International Conference on Networking, Sensing and Control*, 2004, vol. 2, Taipei, Taiwan: IEEE; 2004, p. 749-54. <https://doi.org/10.1109/ICNSC.2004.1297040>.

10. Akoglu L, Tong H, Koutra D. Graph-based Anomaly Detection and Description: A Survey 2014. <https://doi.org/10.48550/ARXIV.1404.4679>.

11. Sadgali I, Sael N, Benabbou F. Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science* 2019;148:45-54. <https://doi.org/10.1016/j.procs.2019.01.007>.

12. Tiwari P, Mehta S, Sakhuja N, Kumar J, Singh AK. Credit Card Fraud Detection using Machine Learning: A Study 2021. <https://doi.org/10.48550/ARXIV.2108.10005>.

13. Abdallah A, Maarof MA, Zainal A. Fraud detection system: A survey. *Journal of Network and Computer Applications* 2016;68:90-113. <https://doi.org/10.1016/j.jnca.2016.04.007>.

14. Espinosa RDC, Caicedo-Erazo JC, Londoño MA, Pitre IJ. Inclusive Innovation through Arduino Embedded Systems and ChatGPT. *Metaverse Basic and Applied Research* 2023;2:52-52. <https://doi.org/10.56294/mr202352>.

15. Moreno MCC, Castro GLG. Strengthening Governance in Caquetá: The Role of Web-based Transparency Mechanisms for Public Information. *Metaverse Basic and Applied Research* 2022;1:16-16. <https://doi.org/10.56294/mr202216>.

16. Ngai EWT, Hu Y, Wong YH, Chen Y, Sun X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems* 2011;50:559-69. <https://doi.org/10.1016/j.dss.2010.08.006>.

17. HaratiNik MR, Akrami M, Khadivi S, Shajari M. FUZZGY: A hybrid model for credit card fraud detection. 6th International Symposium on Telecommunications (IST), Tehran, Iran: IEEE; 2012, p. 1088-93. <https://doi.org/10.1109/ISTEL.2012.6483148>.

18. Boullé M. Compression-Based Averaging of Selective Naive Bayes Classifiers. *Journal of Machine Learning Research* 2007;8:1659-85.
19. Correa Bahnsen A, Aouada D, Ottersten B. Example-dependent cost-sensitive decision trees. *Expert Systems with Applications* 2015;42:6609-19. <https://doi.org/10.1016/j.eswa.2015.04.042>.
20. Forough J, Momtazi S. Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing* 2021;99:106883. <https://doi.org/10.1016/j.asoc.2020.106883>.
21. Moreno MCC, Castro GLG. Unveiling Public Information in the Metaverse and AI Era: Challenges and Opportunities. *Metaverse Basic and Applied Research* 2023;2:35-35. <https://doi.org/10.56294/mr202335>.
22. Gupta B. Understanding Blockchain Technology: How It Works and What It Can Do. *Metaverse Basic and Applied Research* 2022;1:18-18. <https://doi.org/10.56294/mr202218>.
23. Jain N, Chaudhary A, Kumar A. Credit Card Fraud Detection using Machine Learning Techniques. 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India: IEEE; 2022, p. 1451-5. <https://doi.org/10.1109/SMART55829.2022.10047360>.
24. Awoyemi JO, Adetunmbi AO, Oluwadare SA. Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos: IEEE; 2017, p. 1-9. <https://doi.org/10.1109/ICCNI.2017.8123782>.
25. Abiodun OI, Jantan A, Omolara AE, Dada KV, Mohamed NA, Arshad H. State-of-the-art in artificial neural network applications: A survey. *Heliyon* 2018;4:e00938. <https://doi.org/10.1016/j.heliyon.2018.e00938>.
26. Shenvi P, Samant N, Kumar S, Kulkarni V. Credit Card Fraud Detection using Deep Learning. 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India: IEEE; 2019, p. 1-5. <https://doi.org/10.1109/I2CT45611.2019.9033906>.

FINANCIACIÓN

Los autores no recibieron financiación para el desarrollo de la presente investigación.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Roberto Carlos Dávila-Morán, Leonardo Velarde Dávila.

Curación de datos: Roberto Carlos Dávila-Morán, Rafael Alan Castillo-Sáenz.

Análisis formal: Alfonso Renato Vargas-Murillo, Leonardo Velarde Dávila.

Investigación: Camilo Fermín García-Huamantumba, Elvira García-Huamantumba.

Metodología: Carlos Enrique Guanilo Paredes, Camilo Fermín García-Huamantumba.

Redacción - borrador original: Renzo Fidel Pasquel Cajas, Elvira García-Huamantumba.

Redacción - revisión y edición: Renzo Fidel Pasquel Cajas, Carlos Enrique Guanilo Paredes.