Framework SDF Machine Learning en transacciones financieras y detección temprana de fraudes

Fabian Frola[1], Carlos Iván Chesñevar[2], Carlos Alvez[1], Graciela Etchart[1], Ernesto Miranda[1],Silvia Ruiz[1], Juan José Aguirre[1], Juan Carlos Teze[1,2]

[1] Facultad de Ciencias de la Administración - Universidad Nacional de Entre Ríos

Av. Tavella 1424 (E3202KAC), Concordia, Entre Ríos, Argentina.

[2] Instituto de Ciencias e Ingeniería de la Computación (ICIC CONICET UNS)

Universidad Nacional del Sur, San Andrés 800, 8000 Bahía Blanca, Argentina.

fabianenlared@gmail.com, cic@cs.uns.edu.ar, {caralv,getchart, emiranda, sruiz, juaagu}@fcad.uner.edu.ar, jcarlt02@gmail.com

Resumen

En la actualidad, con el crecimiento exponencial de transacciones financieras de tarjetas de crédito y débito, la disminución de barreras de acceso, la globalización y la inclusión financiera se ha incrementado en mayor medida el fraude y la inteligencia creativa para la mutación del comportamiento fraudulento. Es de vital importancia la detección temprana de fraude aplicando distintas estrategias basadas en inteligencia artificial que puedan mitigar, disminuir, y prevenir este flagelo. El objetivo de este trabajo es estudiar, analizar los fundamentos, técnicas, estrategias y herramientas de machine learning que nos permitan dar el paso necesario para abordar el tema de autorizaciones financieras y detección de fraude, cuyo abordaje se hace inalcanzable con estrategias determinísticas o algoritmia tradicional. A partir del estudio mencionando se construirá un *framework* consolidado aplicable en cada etapa del proceso, desde la adquisición de datos, tanto en línea como históricos, el pre-procesamiento, la clasificación y los aportes al modelo predictivo para la detección de fraude.

Palabras clave: machine learning, inteligencia artificial, detección de fraude financiero.

Contexto

Esta línea de trabajo está siendo desarrollada en conjunto por la Facultad de Ciencias de la Administración de la Universidad Nacional de Entre Ríos y el Instituto de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur (ICIC CONICET UNS); los resultados vinculados al mismo se enmarcan en una tesis de la Maestría en Sistemas de Información (en desarrollo), dictada en la FCAD-UNER, y en el trabajo interdisciplinar con el grupo de investigación relacionado al proyecto PID 07/G044 (donde el foco radica en la identificación de personas a partir de

rasgos biométricos), dando continuidad a la aplicabilidad de modelos predictivos en nuevos contextos.

Introducción

En nuestra experiencia en el mundo financiero nos hemos encontrado con un crecimiento exponencial de transacciones, así como de los fraudes asociados a ellas, lo que incrementa la complejidad a la hora de detectarlos tempranamente como sería deseable. Por otro lado, se aprecia que la banca y todo el conjunto de entidades financieras que forman parte de este escenario se ha regido tradicionalmente por modelos algorítmicos tradicionales (determinísticos). Esta situación, si bien parece deseable, es en realidad el principal obstáculo tanto a la hora de autorizar una transacción de crédito/débito, así como la capacidad para detectar un eventual fraude, donde suele haber información incompleta y potencialmente inconsistente, lo que obliga a la construcción de modelos utilizando técnicas de inteligencia artificial a través de Machine Learning.

La toma de decisiones utilizando reglas de negocio pautadas de antemano (que muchas veces carecen de justificaciones racionales) representa un factor negativo tanto en la satisfacción del cliente así como la capacidad de aprendizaje del propio modelo de lo que está ocurriendo en la realidad, limitando las adecuaciones necesarias para acompañar la globalización y la diversificación de la economía, factores con un alto impacto a nivel bancario.

La economía digital se ha consolidado con un crecimiento exponencial en los últimos años, sumado a la expansión de los modelos de pagos electrónicos, transacciones, tarjetas de crédito y débito, e-commerce. El fraude ha acompañado este crecimiento exponencial, generando costos de varios miles de millones de dólares anuales, tanto en pérdidas de los individuos como para las organizaciones. Si bien desde el punto de vista del fraude financiero su aparición suele ser menor al 1/100 de las transacciones (y muchas veces el costo en sí de una acción fraudulenta no justifica el costo para detectarla oportunamente), el costo intrínseco del fraude no se puede valorar solo desde una óptica monetaria, sino que también intervienen otras variables como ser la fidelización de clientes y la erosión de la confianza (asociada a la permanencia o pérdida de clientes). El diseño de algoritmos de detección de fraudes es particularmente desafiante en el ámbito financiero de transacciones con tarjetas de crédito y débito, debido a la distribución no estacionaria de los datos, la clasificación altamente desequilibrada y disponibilidad de pocas transacciones etiquetadas por los investigadores de fraude.

El fraude en el sector financiero afecta la economía de individuos, organizaciones y naciones. Se estima que más de una de cada tres organizaciones han sufrido cualquier tipo de fraude en los últimos dos años. Pero es aún más sorprendente que alrededor del 10% de los delitos financieros se detectan esencialmente por casualidad [1]. En el ámbito financiero, históricamente muy conservador, muy pocos se arriesgan a adoptar criterios poco determinísticos a la hora de decidir si autorizar o negar una transacción financiera; lo mismo ocurre en la detección asociada a un fraude, que generalmente pasa a ser de índole forense, *a posteriori* de la ocurrencia del mismo y sin un registro sistemático (lo que permitiría realizar trabajo de inteligencia sobre quienes cometen el fraude). Más allá de esto, es común que una vez detectado el modus operandi por el sistema bancario generalmente el criminal tiende a cambiar la forma de realizarlo. El desequilibrio relativo del fraude en un conjunto de datos puede comenzar en con la proporción de un defraudador cada 1000 clientes normales, por lo que se trasforma en un problema cuya detección es extremadamente compleja. Si

tomamos los algoritmos de clasificación de minería de datos para tratar de clasificarlos y lograr un modelo predictivo aplicable a futuras ocurrencias se ha llegado a verificar tasas de acierto de hasta 99% [4], pero esto no es suficiente dado que la identificación de falsos positivos deriva a menudo en mayores problemas (como ser la pérdida de un cliente asiduo).

En este trabajo confluyen varias líneas de investigación, entre las que se destacan la aplicación de minería de datos [5] [6] y las técnicas de clasificación [1] [8] [9] [10] y predicción (con las particularidades que presenta un domino de aplicación en el cual aparece una clase ampliamente predominante -clientes normales- y en contraposición muy pocos eventos a clasificar en forma negativa (esto es, los fraudes) [2].

También debemos reconocer que cualquier sistema predictivo de fraude deberá tener un conjunto de datos de entrenamiento apropiado para generar el modelo, y esto representa una de las grandes barreras a la investigación dado que generalmente los datos a utilizar son privativos a algunas pocas organizaciones que tienen acceso (estando protegidos por leyes que amparan la privacidad de los mismos). Sin perjuicio de esto último resulta relevante abordar el desempeño integral de un clasificador "minoritario" (como se sugiere en [3]) que permita consolidar a los modelos predictivos como la alternativa para detección de fraude o previsión de situaciones que conllevan acciones fraudulentas.

Cabe destacar que la amplia adopción del estándar ISO-8583 [7] en el sistema financiero uniformiza la adquisición de datos de transacciones que permitan la captura de información relevante (necesaria como datos de entrada para la generación de modelos predictivos basados en el aprendizaje automatizado).

Líneas de Investigación y Desarrollo

Una de las principales líneas de investigación de este trabajo es la aplicación de machine learning en la detección temprana de fraude de transacciones financieras con tarjetas de crédito / débito, realizando una revisión actualizada de las investigaciones en el estado del arte. Se busca así avanzar hacia la construcción de un *framework* SDF (Sistema Detección de Fraude).

Uno de los principales objetivos de SDF será el reconocimiento de transacciones fraudulentas con elevados niveles de certeza, en un contexto especialmente complejo por el gran desbalanceamiento de las clases (contrastando la clase minoritaria de fraudes frente al universo mayoritario de transacciones financieras genuinas).

Cabe señalar que cada individuo tiene características diferentes de comportamiento en un contexto de no estacionalidad de los datos. Por ende no resulta sencillo realizar procesos de detección de fraude en este ámbito: hay una alta sensibilidad a los impactos negativos que ocasionen los falsos positivos (que erosionan la confianza entre el cliente y la institución financiera), lo que hace que muchas veces es deseable para las mismas padecer los costos directos del fraude y no afectar al cliente. Al mismo tiempo, también es apreciable que la masificación de la inclusión financiera, así como los impactos de la globalización que han profundizado las consecuencias de la inadecuada gestión del fraude.

Resultados y Objetivos

El objetivo es identificar las mejoras aplicables a la clasificación de datos en la clase minoritaria, en entornos de transacciones financieras, para la minimización de falsos positivos. Con este fin se está desarrollando una arquitectura (Fig. 1) con capacidades predictivas de

situaciones de fraude, seleccionando técnicas de machine learning aplicables a las autorizaciones financieras y detección de fraudes en la generación de modelos predictivos, combinando el enfoque supervisado y no supervisado.

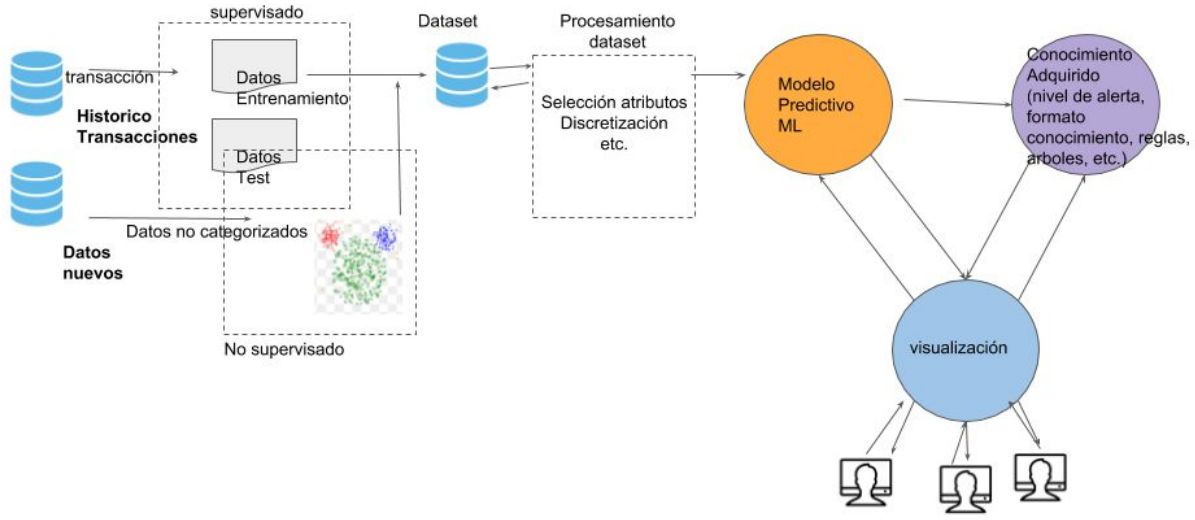

Fig. 1: Arquitectura *framework* Propuesta

Formación de Recursos Humanos

La presente línea de investigación se lleva adelante por un equipo de integrantes de la FCAD/UNER y el ICIC CONICET UNS (Bahía Blanca, Argentina). Se desprende que esta sinergia favorece la formación de recursos humanos en el ámbito de la inteligencia artificial. La línea de investigación involucra varios docentes investigadores y cinco tesistas de maestría. En este contexto se está realizando una tesis de Maestría (orientada a la caracterización de la arquitectura SDF), brindándose también un aporte significativo en otras líneas de trabajo del grupo de investigación..

Referencias

[1] Stefan Axelsson Edgar Alonso Lopez-Rojas. A review of computer simulation for fraud detection research in nancial datasets. IEEE, 2017

[2] Fabrizio Carcillo, Yann-Ael Le Borgne, Olivier Caelen, y Gianluca Bontempi. Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization. I. J. Data Science and Analytics, 5(4):285-300, 2018. doi:10.1007/s41060-018-0116-z. URL https://doi.org/10.1007/s41060-018-0116-z.

[3] Michele Carminati, Alessandro Baggio, Federico Maggi, Umberto Spagnolini, y Stefano Zanero. Fraudbuster: Temporal analysis and detection of advanced financial frauds. En Cristiano Giuffrida, Sébastien Bardin, y Gregory Blanc, eds., Detection of Intrusions and Malware, and Vulnerability Assessment, págs. 211-233. Springer International Publishing, Cham, 2018. ISBN 978-3-319-93411-2.

[4] Andrea Dal Pozzolo. Adaptive Machine Learning for Credit Card Fraud Detection. Tesis Doctoral, Machine Learning Group, Computer Science Department. Universite Libre de Bruxelles, 2015.

[5]Alex Guimaraes Cardoso de Sá, Adriano C. M. Pereira, y Gisele L. Pappa. A customized classification algorithm for credit card fraud detection. Eng. Appl. of AI, 72:21-29, 2018. doi:10.1016/j.engappai.2018.03.011. URL https://doi.org/10.1016/j.engappai.2018.03.011.

[6] Wei Dong, Shaoyi Liao, y Zhongju Zhang. Leveraging financial social media data for corporate fraud detection. Journal of Management Information Systems, 35(2):461-487, 2018. doi:10.1080/07421222.2018.1451954. URL https://doi.org/10.1080/07421222.2018.1451954.

[7] ISO8583-1 Financial transaction card originated messages -- Interchange message specification. Part 1: Messages, data elements and code value. ISO, 2003. URL https://www.iso.org/obp/ui/#iso:std:iso:8583:-1:ed-1:v1:en

[8] Dongxu Huang, Dejun Mu, Libin Yang, y Xiaoyan Cai. Codetect: Financial fraud detection with anomaly feature detection. IEEE Access, 6:19161-19174, 2018. doi:10.1109/ACCESS.2018.2816564. URL https://doi.org/10.1109/ACCESS.2018.2816564.

[9] Rafiq Ahmed Mohammed, Kok Wai Wong, Mohd Fairuz Shiratuddin, y Xuequn Wang. Scalable machine learning techniques for highly imbalanced credit card fraud detection: A comparative study. En PRICAI 2018: Trends in Artificial Intelligence - 15th Pacific Rim International Conference on Artificial Intelligence, Nanjing, China, August 28-31, 2018, Proceedings, Part II, págs. 237-246. 2018. doi:10.1007/978-3-319-97310-4n 27. URL https://doi.org/10.1007/978-3-319-97310-4_27.

[10] Kuldeep Randhawa, Chu Kiong Loo, Manjeevan Seera, Chee Peng Lim, y Asoke K. Nandi. Credit card fraud detection using adaboost and majority voting. IEEE Access, 6:14277-14284, 2018. doi:10.1109/ACCESS.2018.2806420. URL https://doi.org/10.1109/ACCESS.2018.2806420.