Análisis del uso de técnicas supervisadas de aprendizaje automático y profundo en la detección de fraude financiero

Analysis of the use of the supervised machine and deep learning techniques in the detection of financial fraud

Katherin Lizeth Rodriguez-Tovar[1], Fernando Gutiérrez-Portela[2], Ludivia Hernández-Aros[3]

Rodriguez-Tovar, K.L; Gutiérrez-Portela, F; Hernández-Aros, L. Análisis del uso de técnicas supervisadas de aprendizaje automático y profundo en la detección de fraude financiero. *Tecnología en Marcha*. Vol. 36, número especial. Octubre, 2023. V Congreso Internacional en Inteligencia Ambiental, Ingeniería de Software, Salud Electrónica y Móvil. Pág. 50-56.

https://doi.org/10.18845/tm.v36i8.6927

1 Universidad Cooperativa de Colombia, Colombia.
Correo electrónico: katherinl.rodriguez@campusucc.edu.co
https://orcid.org/0000-0002-9576-7778
2 Universidad Cooperativa de Colombia, Colombia.
Correo electrónico: fernando.Gutierrez@campusucc.edu.co
https://orcid.org/0000-0003-3722-3809
3 Universidad Cooperativa de Colombia, Colombia.
Correo electrónico: ludivia.Hernandez@campusucc.edu.co
https://orcid.org/0000-0002-1571-3439

Palabras clave

Fraude financiero; Inteligencia Artificial (IA); factores incidentes; exactitud; detección.

Resumen

En el mundo moderno se hace necesario el uso de técnicas, metodologías y acciones en busca de la integración de los diversos avances, herramientas y elementos vigentes para el trabajo conjunto en la solución a las problemáticas que afectan las finanzas de las organizaciones, puesto que ellas hacen que exista una dinámica empresarial, creando valor económico. Teniendo en cuenta lo anterior, en este estudio se analiza la prevención de fraudes empresariales, mediante el uso de técnicas de aprendizaje automático y profundo para generar prevención, tratamiento y resolución a los fraudes llevados a cabo en sistemas del orden financiero. A nivel metodológico, se obtuvo información en bases de datos a nivel documental, con fuentes fidedignas y estudios de caso, donde se prueba la efectividad en el uso de las técnicas anteriormente nombradas en la detección temprana del fraude empresarial.

Los resultados obtenidos en los documentos consultados expresan que los algoritmos que presentan mayor efectividad en la prevención de estos fraudes son árbol de decisión, C5.0-SVM, Naïve Bayes y Random Forest, con porcentajes de: 92%, 83.15%, 80,4% y 76, 7% respectivamente. Frente al aprendizaje profundo, la literatura mostró que al hacer uso de unidades lógicas aritméticas neuronales y realizando la correcta clasificación de las neuronas iNALU y ReLU el porcentaje de efectividad incrementa en gran proporción.

En la parte final de este documento se presentan y consolidan resultados y conclusiones, todo en el marco de la temática abordada, además la información recopilada en este documento está debidamente respaldada por los derechos de autor a quien corresponde.

Keywords

Financial fraud; Artificial Intelligence (AI); incident factors; accuracy; detection.

Abstract

In the modern world, it is necessary to use techniques, methodologies, and actions in search of the integration of the various advances, tools, and current elements for joint work in solving the problems that affect the finances of organizations, since they make a business dynamic exist, creating economic value. Taking into account the above, this study analyzes the prevention of business fraud, through the use of automatic and deep learning techniques to generate prevention, treatment, and resolution of fraud carried out in financial systems. At the methodological level, information was obtained in databases at the documentary level, with reliable sources and case studies where the effectiveness of the use of the aforementioned techniques in the early detection of business fraud is tested.

The results obtained in the documents consulted express that the algorithms that are most effective in preventing these frauds are decision tree, C5.0-SVM, Naïve Bayes, and Random Forest, with percentages of 92%, and 83.15%, 80, 4%, and 76.7% respectively. In contrast to deep learning, the literature showed that by making use of neural arithmetic logic units and performing the correct classification of the iNALU and ReLU neurons, the percentage of effectiveness increases greatly.

In the final part of this document, results and conclusions are presented and consolidated, all within the framework of the topic addressed, in addition, the information compiled in this document is duly supported by the copyright to whom it corresponds.

Introducción

Según Castellau [1] un fraude financiero “Se define como una acción que una persona o grupo de personas realizan para dañar la economía de otra persona, empresa o entidad bancaria, a cambio de su propio beneficio, por supuesto”, teniendo en cuenta lo anterior, se hace necesario el minimizar riesgos financieros en las organizaciones con herramientas que usen la Inteligencia Artificial (IA). Al hablar de fraudes se aborda el tema de los altos porcentajes de casos donde personas generan daños financieros a una organización y los altos índices de perdida que esto desencadena cada año para dichas empresas que han sido objeto de estas actividades ilícitas que referimos.

Dependiendo del tamaño y su escala de daño, las consecuencias del fraude pueden ser severas y afectar no solo a la empresa internamente, sino también a sus clientes y al entorno social en el que opera la compañía [2]. En este sentido, el uso de técnicas de aprendizaje automático supervisadas y técnicas de aprendizaje profundo, para la detección de los fraudes financieros, han evidenciado, según la literatura consultada, resultados con altos índices de efectividad en la contribución a las organizaciones en el proceso de contrarrestar los daños causados por personas fraudulentas y al mismo tiempo, proteger los activos de las empresas.

Las técnicas de aprendizaje automático supervisadas son aquellas que hacen uso de datos categorizados y estructurados para la clasificación y predicción de posibles anomalías en un sistema, lo anterior, permite la toma de decisiones y la planificación de estrategias para la protección de los bienes de una organización [3] dentro de los modelos más utilizados encontramos, las máquinas de soporte vectorial, árbol de decisión, regresión logística, vecinos cercanos, redes neuronales recurrentes (RNN) y redes neuronales convolucionales (CNN).

Para el aprendizaje profundo, diversas fuentes tecnológicas coinciden en que [4] es una red neuronal con varias capas, las cuales simulan el comportamiento del cerebro humano, además de la ayuda en la automatización de procesos y realización de tareas analíticas. Es capaz de procesar datos no estructurados y mecanizar la extracción de funciones. Son usados en diversos servicios de nuestra vida cotidiana, algunos de ellos como: el reconocimiento de voz, imágenes, documentos o audio, servicios de atención al cliente y el cuidado de la salud; con base en ello pueden prevenirse diversas situaciones donde pudieran llegarse a presentar fraudes.

Frente a este escenario, la investigación analiza el uso de técnicas supervisadas de aprendizaje automático y profundo para la detección de los fraudes empresariales en las organizaciones, abordando los estudios documentales que giran entono a la temática y contrastando los resultados obtenidos para una debida prevención, control y tratamiento de los fraudes financieros.

Este documento inicia con el abordaje de la problemática de las organizaciones frente a los fraudes financieros, luego se explican los antecedentes frente a las técnicas de aprendizaje profundo y automático, y a nivel metodológico se exponen las fases del estudio, para finalmente presentar los resultados y conclusiones.

Planteamiento del problema

Las compañías se ven diariamente afectadas por personas inescrupulosas que tratan de realizar fraude por diversos medios produciendo un detrimento en las finanzas de una organización con la finalidad del beneficio personal y para ello, tienen en cuenta las variables del fraude como la capacidad, la innovación, la oportunidad, la presión, racionalización y la motivación.

En igual sentido, firmas de auditoría como KPMG [5], manifiestan el aumento significativo de los fraudes empresariales en el mundo, dentro de la encuesta anual de fraude titulada “Una triple amenaza en las Américas: Perspectivas de Fraude de KPMG 2022”; señalan que, un 83% de los encuestados han sufrido un ciberataque en los últimos doce meses y el 71% han experimentado algún fraude en sus organizaciones. Además, se respalda que el mayor porcentaje de pérdidas financieras han sido a causa de un fraude llevado a cabo desde un ente externo. Por otra parte, los porcentajes y tipos de amenaza han llegado al 59% en casos de phishing, 43% en estafas y 26% en malwares; también se señala que más del 70% no pagarían un rescate en caso de un ataque.

Por otra parte, la pandemia también generó grandes repercusiones en la eficiencia de los protocolos de seguridad y medidas de prevención de fraude en sus empresas y la mitigación de riesgo en la normativa interna y externa en temas de ciberseguridad. De alguna manera se puede asegurar que los porcentajes de ocurrencia de estos sucesos solamente tienden a incrementar y a causa de la falta o inexistencia de sistemas de prevención, control y tratamiento, los índices de pérdidas son funestos para el correcto funcionamiento de las organizaciones.

Estas cifras muestran la importancia del uso de sistemas inteligentes para la detección y prevención de fraudes con el uso del aprendizaje automático y profundo en la mitigación, tratamiento y control de los fraudes que a diario se presentan en las organizaciones. Con base en esto, este estudio aborda los resultados de algunas investigaciones frente al tema.

Referente teórico

Como la IA ha ayudado a las organizaciones en sus procesos gracias a su interrelación directa con la innovación, lo anterior es en razón a la programación de las máquinas para ser capaces de solucionar problemas y tomar decisiones de manera prácticamente autónoma. La IA ha contribuido en el diseño de mejores estrategias, destacar en la competencia, incrementar el porcentaje de conocimiento en el público, a impactar, entre muchas otras. Lo anterior es respaldado con estadísticas donde se evidencia: aumento en la productividad, mejora en la calidad de vida de los trabajadores de la organización, mejora en la capacitación del personal y la simplificación en procesos de control, calidad y gestión.

Soportado en lo anterior, este documento analiza cuatro estudios que usan modelos de aprendizaje profundo y automático, con sus métricas de evaluación de rendimiento frente a conjuntos de datos de fraudes empresariales, así:

Los autores en un estudio [6] seleccionaron dos modelos de aprendizaje automático con mayor índice de rendimiento de acuerdo con cinco indicadores de evaluación que incluyeron la precisión, recuperación, especificidad, AUC y el costo de clasificación errónea. Se recopilaron un total de veintinueve características sobre 2318 empresas de CSMAR, los autores realizaron un preprocesamiento mediante procesos discretización de la data y la estandarización del puntaje Z, se obtuvieron 18557 datos; debido a los datos desequilibrados, se utilizaron tres métodos: muestreo insuficiente, el muestreo excesivo y el SMOTETomek. Se tomó la decisión de realizar la división de los datos en dos partes, 80% para entrenamiento y 20% para prueba. Como resultado obtuvieron un modelo integrado, basado en Naïve Bayes y KNN con una relación de ponderación de 2 a 1, con el método Over Sampling para tratar datos desequilibrados. Este modelo puede ayudar en la detección de fraudes financieros a un menor costo.

En otro estudio [7] realizaron un método basado en aprendizaje profundo para la detección de fraude financiero apoyado en la técnica Long Short-Term Memory (LSTM); usaron un conjunto de datos reales de fraudes y los resultados los compararon con un modelo de aprendizaje

profundo existente denominado modelo de codificador automático y algunas otras técnicas de aprendizaje automático. Los resultados experimentales ilustraron un desempeño perfecto de LSTM donde logró un 99,95 % de precisión en menos de un minuto.

Según los autores [8] el modelo propuesto aplicó cuatro algoritmos utilizados en el aprendizaje automático: Naïve Bayes, Random Forest, Logistic Regression y SVM en un conjunto de datos muy grande para predecir el fraude el cual contenía aproximadamente 31 características. Las transacciones declaradas fraudulentas fueron del 0,172%, es decir, 492 instancias en todo el conjunto de datos. El modelo se entrenó con el 70 % del conjunto de datos total y el testeo con el 30% restante de los datos. El modelo con mayor efectividad Naïve Bayes con 80,4%, la precisión de otros algoritmos como Random Forest es del 76,7 %, para SVM es del 63,4 % y para la regresión logística es del 65,9.

En otro estudio [9] los autores, implementaron una arquitectura de red neuronal que incorpora Unidades Lógicas Aritméticas Neurales Mejoradas recientemente propuestas. Se construyó un conjunto de datos sintéticos de referencia, el cual refleja el problema de capturar automáticamente tales relaciones matemáticas dentro de los datos; evaluaron dos conjuntos de datos de fraude financiero del mundo real y dos sintéticos para diferentes parámetros de red. El conjunto de datos con 590.540 transacciones, de las cuales 20.663 están etiquetadas como fraude (3,5 %) y 569877 como benignas (96,5 %). Los resultados muestran que el modelo propuesto es capaz de mejorar el rendimiento de las redes neuronales.

Metodologia

El estudio documental, exploratorio y analítico de esta investigación se basa principalmente en los documentos que reposan en las bases de datos Science Direct, Scopus, Taylor and Francis, IEEE, entre otras, para dar mayor soporte científico a la información que se expone. Para ello, se realiza a nivel documental la revisión de literatura científica y notas académicas de tipo investigativo, en el que se referirán a diversos autores que analizan el tema de investigación abordado. La sesión exploratoria, define una serie de hallazgos que permiten entender el fenómeno planteado, además de la correspondiente evaluación y recopilación de información dispersa alojada en fuentes oficiales y por ende confiables. Por último, se aborda el aspecto analítico que mide los datos e información recopilada y genera resultados en el documento.

El estudio tiene en cuenta las siguientes fases: Primera Fase. Se establece la ecuación de búsqueda, permite el ajuste de información, características y términos útiles de los referentes bibliográficos y brinda la agilización del proceso de búsqueda. Segunda Fase. Se realiza exploración bibliográfica en diversas fuentes y autores. Tercera Fase. Se procede a construir formato para consolidación, comparación y análisis de autores, base de datos, sistema de gestión, algoritmos usados, resultados, conclusiones y referencias. Cuarta Fase. Con base en los resultados obtenidos en cada estudio, se procede a organizarlos en orden de porcentajes de efectividad en cada uno de los parámetros necesarios y con ello, realizar el análisis comparativo correspondiente. Quinta Fase. Se elabora el documento en donde consoliden los resultados y se presenta a la comunidad científica.

Propuesta modelo de implementación

El modelo de implementación contiene los diversos aportes y avances que se han generado en la literatura científica frente la minimización del fraude financiero con el uso de la Inteligencia artificial que tenga en cuenta las técnicas supervisadas y sus métricas de evaluación de rendimiento con mejores resultados en comparación con otros autores que han realizado experimentos con conjuntos de datos académicamente reconocidos y generados de contextos reales y propios.

Los estudios anteriores permiten ver las limitaciones y alcances obtenidos en cada una de estas investigaciones, lo cual contribuye se logren mejores resultados en el proceso de análisis, predicción, implementación y pruebas de campo. Para dar solución al problema de detección de fraude financieros mediante el uso del aprendizaje automático, se aplican una seria de etapas como son: la compresión del problema, el análisis de los datos, el preprocesamiento, la selección y extracción de características, la división del modelo entre data para enteramiento, validación y testeó , la evaluación del modelo y por último el análisis de los resultados.

El modelo considera la aplicación de técnicas de preprocesamiento de datos y el uso de modelos supervisados con sus métricas de evaluación que permitan la interpretación y se generen las conclusiones de detección que cumpla con los requerimientos necesarios para entrar en estudio, perfilamiento, corrección y posterior ejecución en diversos entornos; los cuales permitan el entrenamiento funcional del modelo desarrollado.

Conclusiones

Los estudios han demostrado que el tema de fraude financiero trae consigo una complejidad que las empresas deben analizar, controlar y prevenir y es allí, donde el aprendizaje automático como herramienta de detección y prevención aporta de manera significativa a minimizar riesgos con la finalidad de la no masterización del fraude.

Las investigaciones muestran métricas de rendimiento que en algunos casos contribuyen de manera temprana en la detección de un fraude financiero; sin embargo, se observa que los sistemas de detección con aprendizaje automático generan un porcentaje considerable de falsas alarmas lo cual hace que dichos sistemas deban ser mejorados en función del logro de resultados favorables en beneficio de las finanzas de las organizaciones.

Para futuras investigaciones, se hace necesario incursionar en el uso de nuevos modelos no supervisados y profundos en la detección de anomalías por fraude en los sistemas financieros que son parte vital para el sostenimiento de una organización.

Reconocimiento

Este trabajo fue apoyado por la Universidad Cooperativa de Colombia, Sede Ibagué-Espinal, Tolima, Colombia, en el marco del proyecto No. INV 3247.

Referencias

[1] R. Castellnou, «Captio,» 11 Noviembre 2021. [En línea]. Available: https://www.captio.net/blog/tipos-fraudes-financieros-comunes.

[2] Solé, Mireia, «Captio,» 12 Mayo 2021. [En línea]. Available: https://www.captio.net/blog/casos-fraudes-empresas-importantes.

[3] IBM, «IBM COMPANY,» [En línea]. Available: https://www.ibm.com/cloud/learn/machine-learning.

[4] IBM Institute Studio, «Deep Learning,» 2022.

[5] KPMG, «Aumento Fraude financiero en el mundo - 2022,» 2022.

[6] Minghuan Shou, Xueqi Bao & Jie Yu, «An optimal weighted machine learning model for detecting financial fraud,» 2021.

[7] Yara Alghofaili, Albatul Albattah & Murad A. Rassam, «A Financial Fraud Detection Model Based on LSTM Deep Learning Technique,» 2020.

[8] Amit Gupta, M. C. Lohani & Mahesh Manchanda, «Financial fraud detection using naive bayes algorithm in highly imbalance data set,» 2021.

[9] Schlör, D., Ring, M., Krause, A., Hotho, A., «Detección de fraude financiero con unidades de lógica aritmética neuronal mejoradas,» 2021.

Análisis del uso de técnicas supervisadas de aprendizaje automático y profundo en la detección de Fraude financiero

Katherin Lizeth Rodriguez Tovar, Fernando Gutiérrez Portela, Ludivia Hernández Aros

CONTEXTO:

OBJETIVOS

- Desarrollar las fases del proceso de Aprendizaje Automático para la obtención de los resultados de las métricas de rendimiento.
- Desarrollar las fases del proceso de Aprendizaje Automático para la obtención de los resultados de las métricas de rendimiento.
- Desplegar el sistema de detección de fraude empresarial en un entorno simulado o laboratorio empresarial.

PROBLEMA.

Diariamente las compañías se ven afectadas por personas inescrupulosas que tratan de realizar fraude por diversos medios produciendo un detrimento en las finanzas de la organización con la finalidad del beneficio personal y para ello, tienen en cuenta las variables del fraude como la capacidad, la innovación, la oportunidad, la presión, racionalización y la motivación. Estudios respaldan un alto incremento en la puesta en marcha de fraudes empresariales en el mundo; ello es atribuido a la falta o inexistencia de sistemas de prevención, control y tratamiento. Por lo anterior se hace necesario el uso de sistemas inteligentes para la detección y prevención haciendo uso del aprendizaje automático y profundo en la mitigación, tratamiento y control de los fraudes que a diario se presentan.

PRINCIPAL INNOVACION INPLEMENTADA:

Desarrollo e implementación de un Sistema de detección de fraude financiero haciendo uso de técnicas de aprendizaje automatico y profundo.

PRINCIPALES METODOS

Para dar inicio a nuestra propuesta innovadora se llevo a cabo cinco fases enfocadas a la búsqueda y consolidación de la información necesaria respecto a la temática abordada. Estas fases fueron: construcción de la ecuación de búsqueda., exploración bibliográfica, análisis y comparación de información, clasificación de estudios basado en resultados obtenidos y valores de métricas y de rendimiento y finalmente la construcción de nuestro documento de consolidación; en el se encuentra la información pertinente para iniciar el proceso de diseño de nuestros algoritmos de detección.

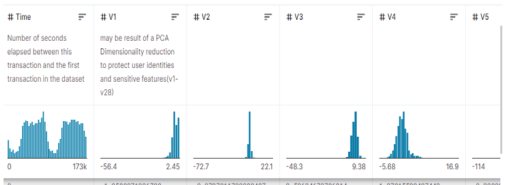
Posterior a ello se inicio la programación de nuestro algoritmos de inteligencia artificial realizando pruebas con la data existente; esta fue construida con el apoyo de una organización privada que brindo los espacios pertinentes para la implementación de ataques controlados a la data que ellos almacenaron de un periodo de tiempo especifico, es de vital importancia señalar que fue una base alterna a la de ellos y se consolido como propia.

Nuestro proyecto esta en la fase de estudio, implementación y prueba de los diversos parámetros que se le fueron administrados para la detección de posibles fraudes o detección de actividades anómalas o fraudulentas.

Información de Contacto

katherinl.rodriguez@campusucc.edu.co

fernando.Gutierrez@campusucc.edu.co



# Time	# V1	# V2	# V3	# V4	# V5
Number of seconds elapsed between this transaction and the first transaction in the dataset	may be result of a PCA Dimensionality reduction to protect user identities and sensitive features(v1-v28)				
0	-1.3598071336738	-0.072781173398497	2.536346737969 14	1.37815522427443	-0.3383
0	1.19185711131486	0.26615071205963	0.16648011335321	0.448154078468911	0.06001
1	-1.35835406159823	-1.34016307473609	1.77320934263119	0.379779593034328	-0.5031
1	-0.966271711572087	-0.185226008082898	1.79299333957872	-0.863291275036453	-0.0103
2	-1.15823309349523	0.877736754848451	1.548717846511	0.403833933955121	-0.4071
2	-0.425965884412454	0.960523044882985	1.14119934232219	-0.168252079760302	0.42098
4	1.229657634567 93	0.141003507049326	0.045370773589944 9	1.20261273673594	0.19188
7	-0.644269442348146	1.41796354547385	1.07430803763556	-0.492199018495015	0.94893
7	-0.894286008220202	0.286157196276544	-0.113192212729871	-0.271526130088604	2.66959

PASOS FUTUROS:

Apoyado en los resultados que obtengamos en la fase en donde nos encontramos consolidaremos variaciones y correcciones a los modelos o algoritmos entrenados, haciendo cambios en los parámetros suministrados.

Además esperamos poder integrar otros algoritmos de inteligencia artificial para consolidaran un sistema mas fuerte de detección de este tipo de fraude.

RESULTADOS:

Consideramos que obtendremos un avance exponencial de resultados positivos en el área de detección de anomalías o puesta en marcha de fraudes en las datas de las diversas organizaciones.

Hasta el momento nos encontramos realizando las pruebas necesarias que fundamenten y apoyen la mejora en estos sistemas.

Hemos evidenciado altos índices de rendimiento en el uso de ciertos algoritmos ya usados en anteriores estudios y basado en las recomendaciones o incidencias de error de estos buscamos no recaer en ello y direccionar nuestro estudio en el camino correcto.

RECURSOS Y REFERENCIAS:

Bases bibliográficas como Scopus, Taylor & Francis, IEEE,Science Direct.

Creado por: Dr. Cassandre Alvarado, University of Texas at Austin
Dr. Julie Schell, University of Texas at Austin