ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.897

Effectiveness of Machine Learning in Fraud Detection. A Systematic Review

Diego Alonso Fernández-Alburuqueque[1]; Jose David Guerrero-Manayay[2]; Nestor Abel Sánchez-Goycochea[3]
[1,2,3]Universidad Tecnológica del Perú, Perú, *U21228858@utp.edu.pe, U21225344@utp.edu.pe, nsanchezg@utp.edu.pe*

Abstract*– Fraudulent transactions represent a significant global issue due to their economic and social impact. This research aims to identify the most effective machine learning models for detecting fraudulent transactions. A systematic literature review was conducted as the primary methodology, structured around three specific questions derived from the main research question: Which machine learning models are the most effective for detecting fraudulent transactions? A total of 78 articles were analyzed, extracted from the Scopus and Web of Science databases up to September 2024. Of these, 39 met the inclusion criteria established under the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol. The results highlight that machine learning and deep learning models, such as Random Forest, Extreme Gradient Boosting, Long Short-Term Memory, Artificial Neural Networks, and some hybrid ML-DL models, are the most effective for detecting fraudulent transactions. It is concluded that these techniques provide robust and reliable solutions to prevent losses caused by fraud, contributing to the development of advanced strategies in organizations and financial sectors.

***Keywords*-- fraud detection, crime, machine learning, deep learning, learning systems.**

Efectividad del Aprendizaje Automático en la Detección del Fraude. Una Revisión Sistemática

Diego Alonso Fernández-Alburuqueque[1]; Jose David Guerrero-Manayay[2]; Nestor Abel Sánchez-Goycochea[3]
[1,2,3]Universidad Tecnológica del Perú, Perú, *U21228858@utp.edu.pe, U21225344@utp.edu.pe, nsanchezg@utp.edu.pe*

Resumen*– Las transacciones fraudulentas representan un problema significativo a nivel mundial debido a su impacto económico y social. Esta investigación tiene como objetivo identificar los modelos de machine learning más efectivos para detectar transacciones fraudulentas. Como metodología principal, se realizó una revisión sistemática de la literatura, estructurada a partir de tres preguntas específicas derivadas de la pregunta principal: ¿Cuáles son los modelos de machine learning más efectivos para detectar transacciones fraudulentas? Se analizaron 78 artículos extraídos de las bases de datos Scopus y Web of Science hasta septiembre de 2024, de los cuales 39 cumplieron con los criterios de inclusión establecidos según el protocolo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Los resultados destacan que los modelos de machine learning y deep learning, como Random Forest, Extreme Gradient Boosting, Long Short-Term Memory, Artificial Neural Network y algunos modelos híbridos de ML y DL, son los más efectivos para la detección de transacciones fraudulentas.Se concluye que estas técnicas proporcionan soluciones robustas y confiables para prevenir las pérdidas ocasionadas por el fraude, contribuyendo al desarrollo de estrategias avanzadas en organizaciones y sectores financieros.

Palabras clave*-- detección del fraude, delincuencia, aprendizaje automático, aprendizaje profundo, sistemas de aprendizaje.

I. Introducción

En la actualidad, el fraude en transacciones financieras representa una creciente preocupación social y económica para las personas, empresas e instituciones financieras. La digitalización y el aumento de las transacciones electrónicas, impulsados por el comercio en línea y las nuevas tecnologías de pago, han transformado la forma en que las personas interactúan con los servicios financieros [1]. De este modo, las habilidades técnicas y el avance de la tecnología están más disponibles para los delincuentes, por lo que sus tácticas para cometer delitos se vuelven más difíciles de combatir [2]. Esto ha traído consigo un aumento en la cantidad de intentos de fraude, afectando no solo a la economía global, sino también la seguridad y confianza de los usuarios [3]. Pues cada año se pierden miles de millones debido a actividades fraudulentas, lo que pone de relieve la necesidad de mecanismos de detección más sólidos [4]. Ante esta situación se han impulsado numerosas investigaciones sobre cómo detectar y prevenir actividades fraudulentas. Un enfoque prometedor en este campo es el uso de métodos avanzados de detección de fraude, destacando las técnicas de machine learning (ML) y deep learning (DL). Modelos de ML como Decision Tree (DT) han demostrado en diferentes estudios tener éxito ya que suelen ser muy efectivas en tareas como la clasificación de patrones en tiempo y monto, pero aún no se han explorado lo suficiente [5]. Por otro lado, el uso de técnicas de DL ha mostrado resultados prometedores en la detección de fraude, ya que algunos modelos de este enfoque pueden identificar transacciones sospechosas incluso con un conjunto limitado de datos etiquetados. Modelos de DL como Long Short-Term Memory (LSTM) han sido implementados con éxito debido a su capacidad para identificar patrones temporales y secuenciales en los datos financieros [6],[7]. Sin embargo, a pesar del rápido avance en el uso de estas tecnologías para analizar patrones complejos y detectar anomalías en tiempo real, lo cual resulta fundamental en la lucha contra el fraude financiero, aún existen dudas sobre su efectividad en comparación con los métodos tradicionales [8]. Por lo tanto, la justificación de este estudio se fundamenta en la necesidad de evaluar cómo las técnicas de ML pueden contribuir a detectar transacciones fraudulentas y convertirse en la última línea de defensa ante este problema [9]. Los resultados de esta investigación ayudarán a determinar el modelo de ML más efectivo para detectar transacciones fraudulentas y proporcionarán una base sólida para futuras investigaciones, que permita mejorar los métodos utilizados y promover un entorno financiero más seguro y confiable para la sociedad [10], [11], [12].

II. Metodología

El presente estudio se llevó a cabo mediante una revisión sistemática de literatura, enfocada en evaluar la efectividad en la detección de transacciones fraudulentas mediante modelos de ML. A partir de esta variable de estudio, se planteó la siguiente pregunta principal: ¿Qué modelo de machine learning es el más efectivo para detectar transacciones fraudulentas? Para responderla, se desglosó en tres preguntas específicas que permitieron analizar la variable de estudio, el método de solución y el resultado del modelo de solución en el problema. Estas preguntas se muestran en la Tabla I.

TABLA I
PREGUNTAS Y KEYWORDS

Pregunta principal: ¿Qué modelos de machine learning son los más efectivo para detectar transacciones fraudulentas?		
Especificación	**Pregunta**	**Keywords**
1. Variable de estudio ¿Cómo se mide?	¿Cuáles son los criterios para determinar si una transacción es fraudulenta?	Fraud detection y trasaction.

2. El método de solución. Características.	¿Qué modelos de machine learning existen para la detección de transacciones fraudulentas?	Machine learning y deep learning.
3. El resultado del modelo de solución en el problema.	¿Qué nivel de efectividad tiene los modelos de machine learning en detección de transacciones fraudulentas?	Effectiveness, effective y efficiency.

Este estudio se fundamenta en una investigación bibliográfica realizada utilizando las bases de datos SCOPUS y Web of Science, para la búsqueda de fuentes de información se consideraron palabras clave correspondientes a las preguntas específicas anteriormente mencionadas en la Tabla I, mediante esto se obtuvo la siguiente cadena de búsqueda en SCOPUS:

(TITLE-ABS-KEY ("fraud detection" AND "transaction") AND TITLE-ABS-KEY ("machine learning" OR "deep learning") AND TITLE-ABS-KEY ("effectiveness" OR "effective" OR "efficiency"))

En la primera parte de la cadena se utilizó el operador de búsqueda "AND" con el fin de conectar los keywords "fraud detection" y "transaction", así se obtuvieron resultados más específicos que abordaban el tema de transacciones fraudulentas. En la segunda parte de la cadena se utilizó el operador de búsqueda "OR" para que las fuentes de información consideren los keyword "machine learning" o "deep learning", lo que amplió la cantidad de resultados obtenidos, especificando que los estudios consideren modelos o técnicas, tanto de ML como DL. Finalmente, en la tercera parte de la cadena también se utilizó el operador de búsqueda "OR" para considerar los keywords "effectiveness", "effective" o "efficiency" en los resultados de búsqueda, lo que amplió la cantidad de resultados obtenidos, además de especificar que estos incluyan información sobre la efectividad de los modelos. Esta misma cadena de búsqueda también se empleó en la base de datos Web of Science. Para limitar el número de resultados obtenidos con esta cadena de búsqueda, se optó por establecer filtros que permitieron orientar la investigación hacia el cumplimiento del objetivo. Al aplicar los filtros detallados en la Tabla II, se obtuvo la siguiente cadena de búsqueda, la cual se empleó en las bases de datos previamente mencionadas:

(TITLE-ABS-KEY ("fraud detection" AND "transaction") AND TITLE-ABS-KEY ("machine learning" OR "deep learning") AND TITLE-ABS-KEY ("effectiveness" OR "effective" OR "efficiency")) AND PUBYEAR > 2021 AND PUBYEAR < 2025 AND (LIMIT-TO (OA,"all")) AND (LIMIT-TO (SUBJAREA,"COMP")) AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (LANGUAGE,"English"))

TABLA II
FILTROS PARA LA CADENA DE BUSQUEDA

FILTRO	DESCRIPCIÓN
F1: PUBYEAR > 2021 AND PUBYEAR < 2025	Se estableció filtrar los años de publicación de las investigaciones entre 2022 y 2024, para acortar la cantidad de resultados y asegurar que la información a analizar sea la más reciente.
F2: LIMIT-TO (OA,"all")	Se estableció que todas las investigaciones a analizar sean de libre acceso, para garantizar la disponibilidad de estas.
F3: LIMIT-TO (SUBJAREA,"COMP")	El área temática establecida fue ciencias de la computación, debido a que engloba estudios relacionados la variable de estudio.
F4: LIMIT-TO (DOCTYPE,"ar")	El tipo de documento establecido fue artículo, para asegurar que las fuentes muestren datos, alineados al objetivo de esta investigación.
F5: LIMIT-TO (LANGUAGE,"English")	El idioma establecido fue inglés, dado que es el idioma predominante en estas publicaciones.

Tras identificar 56 artículos en SCOPUS y 22 en Web of Science, sumando un total de 78 documentos hasta el 24/09/2024 a las 16:34 horas, se decidió realizar una revisión sistemática conforme a las directrices de la declaración PRISMA. Esta declaración facilita la obtención de resultados de publicaciones científicas que están alineadas con los objetivos de la investigación. El protocolo PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) se fundamenta en un proceso de etapas de filtrado [12]. La Fig. 1 muestra que, tras obtener 78 artículos, se inició la primera etapa, la cual consistió en eliminar los resultados obtenidos que estén duplicados, es decir, que se encuentren alojados en ambas bases de datos consultadas. En esta etapa se excluyeron un total de 39 artículos, para ello, la información se organizó en dos hojas usando la herramienta Excel: una para los artículos de SCOPUS, que incluía campos como título, autores, DOI y resúmenes; y otra para los artículos de Web of Science. Posteriormente, se generó una tercera hoja denominada "Scopus y WOS sin duplicados", en la cual se compararon los títulos de los artículos para excluir los duplicados. En la segunda etapa, se descartaron 14 artículos cuyos resúmenes no correspondían al tema de interés o no proporcionaban información relevante. En la tercera etapa, se excluyeron 4 artículos más porque no se podía acceder a sus PDF completos por ser de pago. Finalmente, tras una revisión detallada del contenido completo de los documentos, se eliminó 1 artículo que no estaba relacionado con la detección de transacciones fraudulentas, quedando 39 artículos para la revisión sistemática. La Tabla III muestra los criterios para incluir y excluir fuentes de información que se establecieron según el objetivo de la investigación.

TABLA III
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

CRITERIOS DE INCLUSIÓN	CRITERIOS DE EXCLUSIÓN
CI1: Fuentes de información relacionadas con la problemática de transacciones fraudulentas.	CE1: Fuentes de información que no estén relacionadas a la problemática de transacciones fraudulentas.

CI2: Fuentes de información que emplean métricas para evaluar los modelos de machine learning que estén estudiando.	CE2: Fuentes de información que no empleen métricas para evaluar los modelos de machine learning.
CI3: Fuentes de información que estén en formato PDF y sean de acceso libre.	CE3: Fuentes de información que no estén disponibles en acceso abierto.

Como se puede visualizar en la Fig. 1 Este enfoque, basado en la declaración PRISMA, sigue una guía especializada para la elaboración de revisiones sistemáticas, asegurando que los informes sean transparentes, completos y precisos. Así, el uso de PRISMA garantiza la exhaustividad y transparencia en la selección de estudios y cumple con los estándares actuales para presentar informes en revisiones sistemáticas, beneficiando a la comunidad científica en general.

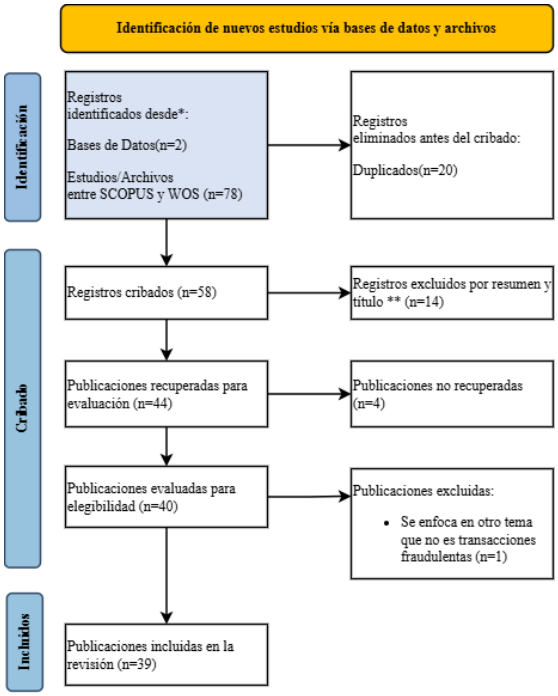

Fig.1: PRISMA

Se desarrollo una hoja de cálculo en la cual se estructuró el análisis de los artículos, esta hoja se evidencia en el siguiente enlace: https://doi.org/10.5281/zenodo.14363908

III. Resultados y Discusiones

Esta investigación presenta una recopilación de los artículos examinados, estos han sido categorizados por la fecha de publicación y lugar de origen. Al analizar la Fig. 2, se observa una evolución significativa en la producción científica durante el período comprendido entre 2022 y 2024. En particular, el año 2023 destaca con un incremento de 10 publicaciones en comparación con el año anterior. Este crecimiento se mantiene en 2024, alcanzando un total de 17 publicaciones hasta Setiembre, se estima un incremento hasta el cierre de la indización del mismo año. Estos datos reflejan un renovado interés en el tema de estudio, acompañado de una contribución continua y en ascenso durante el período analizado. Aunque no es posible predecir con certeza, es probable que esta tendencia de crecimiento en la producción científica persista en los próximos años. Este análisis ofrece una visión detallada y actualizada de la evolución temporal de la investigación científica, subrayando su relevancia y desarrollo en el campo temático examinado.

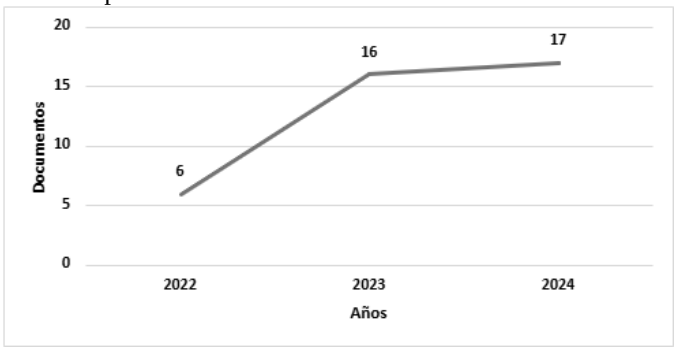

Fig. 2: Artículos organizados por año de publicación.

La distribución geográfica de los artículos estudiados, presentada en la Tabla IV, evidencia una diversidad significativa en la contribución científica de distintos países al tema de investigación. India destaca como el país con mayor aporte en la producción científica, contribuyendo con 21% del total de estudios examinados. Esto refleja el interés y compromiso del país en la búsqueda e implementación de soluciones innovadoras en el área temática examinada. Arabia Saudita aporta el 15% de los artículos, seguida de cerca por China, con un 13%. Estos países destacan por su enfoque en el desarrollo de soluciones tecnológicas y científicas, consolidando su relevancia en el ámbito de la investigación. Finalmente, paises como Marruesco, Reino Unido, Pakistan, Australia, Bangladés, Equipto, Corea del Sur y Turquía acumulan el 51% de los estudios analizados, lo que resalta la naturaleza global y colaborativa de la investigación en este campo. Este análisis geográfico pone de manifiesto la importancia de la cooperación internacional y el compromiso de diversas naciones en el avance de las soluciones científicas y tecnológicas, destacando a India como el principal motor de esta contribución.

TABLA IV
ARTÍCULOS ORGANIZADOS POR PAÍS DE PUBLICACIÓN

PAISES	FRECUENCIA
India	21%
Arabia Saudita	15%
China	13%
Marruecos	10%
Reino Unido	10%
Pakistán	8%
Australia	5%
Bangladés	5%
Egipto	5%
Corea del Sur	5%
Turquía	3%

Nota: Elaborado a partir de los documentos analizados

A partir de la revisión de la literatura, se han identificado los keywords más utilizados en estos estudios. Los resultados que se observa en la Tabla V indican que el keyword fraud detection es el predominante entre los estudios analizados, obteniendo una frecuencia del 72%. Esto indica la importancia del uso de este keyword para facilitar el acceso a estudios relacionados con delitos económicos y financieros. Por otro lado, el keyword crime, obtuvo la mayor fuerza de enlace, obteniendo un total de 232. Este dato indica que este keyword está relacionado a otros 232 keywords, lo que permite encontrar información más extensa, ya que permite llegar a más áreas temáticas. Finalmente, el keyword machine learning, con una frecuencia de 44% y una fuerza de enlace de 117, es fundamental para encontrar información relacionada a los modelos de machine larning que se emplean en la detección de fraude, esto delimita las herramientas y enfoques tecnológicos empleados para esta tarea.

TABLA V
KEYWORDS MÁS UTILIZADOS

KEYWORD	OCURRENCIA	FUERZA DE ENLACE
fraud detection	72%	340
crime	49%	381
machine learning	44%	249
deep learning	36%	164
learning systems	31%	219
machine-learning	21%	195
fraud	18%	135
decisión tres	15%	157
learning algorithms	15%	132
support vector machines	13%	129

Nota: Elaborado a partir de los documentos analizados

La primera pregunta de esta investigación fue ¿Cuáles son los criterios para determinar si una transacción es fraudulenta? Los resultados de la Tabla VI muestran que Tiempo y Monto son los criterios más utilizados, representando el 69.23% de los artículos analizados. Estos permiten identificar anomalías en el tiempo entre cada transacción y el monto efectuado para cada una, lo que es fundamental para poder detectar transacción fraudulentes. El Monto como único criterio es utilizado en un 12.82% de los estudios analizados. No obstante, este criterio también se utilizó en conjunto con otros, lo que lo convierte en el más frecuente entre los estudios. El uso de este criterio permite detectar rápidamente comportamientos de fraude, ya que una anomalía en las transacciones suele estar directamente relacionada con la cantidad de dinero involucrada [13]. Por último, la Tabla VI también presenta otros criterios utilizados de forma individual o combinada, aunque con menor frecuencia, como Tiempo, (Tiempo, Monto y Ubicación), (Monto, Tiempo, Ubicación y Producto), y Ubicación. Esta diversidad de criterios permite comprender los diferentes aspectos que se consideran al clasificar una transacción como fraudulenta o no.

TABLA VI
CRITERIOS MÁS UTILIZADOS

CRITERIOS	PORCENTAJE	ID REFERENCIA
Tiempo y Monto	71.79%	[1] , [3] , [5], [6], [7], [8], [10], [14], [15], [16], [17], [18], [20], [21], [22], [24], [25], [26], [27], [28], [31], [33], [34], [39], [40], [41], [42], [43]
Monto	12.82%	[11], [19], [29], [30], [36]
Monto, Tiempo y Ubicacion	7.69%	[32], [37], [38]
Monto, Tiempo, Ubicacion y Producto	2.56%	[23]
Tiempo	2.56%	[13]
Ubicación	2.56%	[35]

Nota: Elaborado a partir de los documentos analizados

Asimismo, se analizaron los dataset o conjunto de datos más estudiados, los cuales involucran a los criterios mencionados. Los dataset desempeñan un papel fundamental, ya que permiten entrenar y validar la eficacia de los modelos de ML, proporcionando una base sólida para evaluar su desempeño [37]. La Fig. 3 indica que The Europe Credit Card (ECC) es el dataset más utilizado, representando el 54% de los estudios analizado. Este dataset recoge 284,807 registros de transacciones con tarjetas de crédito generados por titulares europeos durante dos días en septiembre de 2013 [16]. Su amplia preferencia se debe a que es de acceso público, lo que facilita a los investigadores trabajar con datos sin restricciones legales o económicas [28]. BANKSIM consta de 594,643 transacciones realizadas durante 180 días simulados, de la cuales 7,200 (1.2%) se consideran fraudulentas. Es especialmente valorado porque consiste en datos sintéticos generados por un simulador de transacciones bancarias [37], lo que resulta ideal en casos donde el acceso a datos reales está restringido debido a preocupaciones legales o de privacidad [25]. Por otro lado, PAYSIM se centra en la simulación de transacciones móviles. Este enfoque es útil para analizar patrones específicos de fraude en la banca móvil, un área de creciente importancia en la actualidad [26]. Por último, la categoría de “otros” refleja la diversidad de datasets utilizados en diferentes artículos. Estos incluyen datasets privados de instituciones financieras o conjuntos de datos orientados a necesidades específicas [19]. Esta variedad pone en manifiesto que, aunque ECC es el más utilizado, los investigadores seleccionan diferentes conjuntos de datos según los objetivos de sus estudios.

Por lo tanto, los criterios más relevantes para detectar transacciones fraudulentas son Tiempo y Monto, siendo el dataset ECC el más utilizado para entrenar y validar modelos de ML.

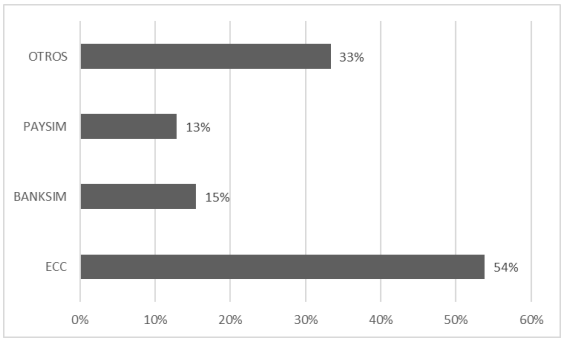

Fig. 3: Dataset más utilizados
Nota: Elaborado a partir de los documentos analizados

La segunda pregunta de esta investigación fue ¿Qué modelos de Machine Learning existen para la deteccion de transacciones fraudulentas? Los datos obtenidos muestran que previamente al entrenamiento de los modelos, los estudios emplean diversas técnicas de remuestreo o balanceo de datos, debido a que los distintos dataset presentan un aspecto en común, el desequilibrio en las clases de los datos. Este desbalance ocurre cuando las clases están representadas de manera desigual siendo las transacciones fraudulentas significativamente menos frecuentes que las transacciones legítimas [38]. Mitigar este problema permitirá generar un entorno más equilibrado ayudando a los modelos aprender patrones sin inclinarse únicamente hacia la clase mayorista [44]. La Tabla VII muestra que Synthetic Minority Oversampling Technique (SMOTE) con un 59%, es la tecnica más utilizada. SMOTE crea datos artificiales utilizando el patrón de vecinos más cercanos, seleccionando puntos de la clase minoritaria al azar e identificando sus vecinos más cercanos dentro del conjunto de datos. A partir de esto, genera datos sintéticos interpolando entre los puntos seleccionados y sus vecinos más próximos [36]. Random Under Sampling (RUS) resulta ideal cuando se busca reducir el desequilibrio de datos eliminando instancias de la clase mayoritaria para que ambas clases tengan una representación equilibrada [3]. ADASYN se posiciona como una técnica adaptativa prioriza la generación de muestras sintéticas en regiones con mayor desbalance, enfocándose en instancias minoritarias difíciles de clasificar [30]. Es ideal para mejorar la detección en escenarios complejos, reforzando la capacidad del modelo en áreas con alta proporción de la clase mayoritaria [15]. Además, la categoría OTROS refleja que los investigadores siguen explorando activamente alternativas para mejorar la calidad del entrenamiento de los modelos ML. Esto se debe a características únicas de ciertos datasets que requieren soluciones personalizadas que no se ajustan completamente a técnicas estándar como SMOTE o RUS [20]. Por último, se observa un 21% de estudios que no utilizan ninguna técnica de remuestreo. Esta decisión responde principalmente al interés por ahorrar tiempo en el preprocesamiento y mantener la integridad del conjunto de datos original, especialmente cuando los modelos están diseñados para trabajar directamente con conjuntos desequilibrados [24].

TABLA VII
TECNICAS DE REMUESTREO

TECNICAS	FRECUENCIA	ID REFERENCIA
SMOTE	59%	[6], [7], [8], [10], [11], [14], [15], [17], [20], [21], [26], [28], [30], [31], [33], [34], [35], [37], [38], [39], [41], [42], [43]
RUS	21%	[15], [16], [17], [18], [20], [21], [25], [29]
ADASYN	10%	[15], [20], [30], [32]
OTROS	33%	[1], [8], [10], [11], [15], [22], [26], [27], [30], [32], [35], [39], [41]
NO UTILIZA	21%	[3], [5], [13], [19], [23], [24], [36], [40]

Nota: Elaborado a partir de los documentos analizados

Aunque la segunda pregunta especifica se centra únicamente en modelos de ML, también se encontraron artículos que incorporaron modelos de DL. Esto se debe a que cada enfoque posee su propio conjunto de ventajas y desventajas, teniendo un buen desempeño en la detección de una clase de datos, pero tener dificultades con otras [14]. Los avances recientes en las técnicas de ML han permitido el desarrollo de modelos más sofisticados, capaces de detectar patrones intrincados y anomalías indicativas de comportamiento fraudulento [28]. Sin embargo, el DL ha ganado popularidad debido a su rendimiento superior al ML, gracias a su capacidad de aprender de manera más profunda y eficiente las relaciones internas entre las transacciones financieras [27]. Por este motivo, algunos estudios propusieron modelos híbridos que integran técnicas de ambos enfoques, o compararon distintos modelos de ML y DL, logrando así una variedad de resultados para evaluar el rendimiento de cada modelo. Finalmente, una parte más reducida de estos artículos se enfocaron en técnicas de Data Mining, lo que proporcionó una perspectiva adicional para abordar la detección de transacciones fraudulentas. Estos enfoques se analizaron acorde a los modelos específicos más frecuentes para cada uno. Los resultados presentados en la Tabla VIII muestran que dentro de los modelos ML utilizados para la detección de transacciones fraudulentas, se aprecia un destacado uso de Random Forest (RF), obteniendo un 41.03%, seguido de K-Nearest Neighbors (KNN) con un 35.90%, Support Vector Machines (SVM) con el 33.33%. y Extreme Gradient Boosting (XGB) con un 28.21%. RF sobresale como el modelo más utilizado. Este se basa en árboles de decisión que reducen el sobreajuste y mejora la precisión de las predicciones al construir múltiples árboles en diferentes muestras y características aleatorias [10]. Esto lo hace ideales para problemas de clasificación en conjuntos de datos financieros, donde los patrones de fraude a menudo no son lineales. KNN es conocido por su simplicidad y facilidad de implementación [1]. Funciona asignando una clase a una nueva instancia en función de la clase más común entre sus "k" vecinos más cercanos en el espacio de características [28]. Al aumentar la cantidad de vecinos considerados, el modelo se

vuelve más resistente al ruido y a los valores atípicos en los datos, lo que conduce a un mejor rendimiento [8]. SVM se destaca como un poderoso enfoque que tiene como objetivo encontrar el hiperplano de separación óptimo que maximice el margen entre instancias de diferentes clases, lo que permite clasificar correctamente los datos [29]. Este modelo es efectivo en la detección de fraudes por su capacidad de manejar datos complejos con alta precisión, aunque puede ser costoso computacionalmente [1]. Por último, XGB es una implementación eficiente y escalable de árboles de decisión potenciados por gradiente que construyen modelos aditivos de manera gradual [29]. Este modelo es ideal para la detección de fraudes financiero, ya que maneja eficazmente conjuntos de datos desequilibrados y tiene la ventaja de manejar valores faltantes de forma integrada [11], [45]. En el caso de los modelos de DL, los estudios destacan el uso de Long Short-Term Memory (LSTM), obteniendo un 23,08%, seguido de Artificial Neural Networks (ANN) con un 20.51%, Multi-Layer Perceptron (MLP) con un 12.82% y Convolutional Neural Network (CNN) con un 10.26%. LSTM sobresale como el modelo más estudiado. Su arquitectura, permite reconocer patrones secuenciales a largo plazo, lo que resulta invaluable para predecir etiquetas de transacciones en función de secuencias previas [42]. Le sigue el modelo de ANN, este es conocido por su alta precisión y capacidad para manejar conjuntos de datos complejos. Es capaz de reconocer patrones complejos a través de un proceso de aprendizaje que involucra tanto la propagación hacia adelante de las entradas como la propagación hacia atrás de los errores [1], [28]. MLP es una clase de redes neuronales artificiales de propagación hacia adelante, compuesta por un grupo de neuronas vinculadas entre sí mediante pesos de enlace. Esta ofrece el potencial de comprender relaciones no lineales y complejas entre varios factores en los datos de transacciones [8]. Finalmente, CNN es una red neuronal de propagación hacia adelante que se construye a partir de conexiones locales, pesos compartidos, agrupamiento y el uso de varias capas [46], [47]. Tienen la capacidad de aprender inmediatamente características de los datos sin procesar, esto permite que sea más eficiente computacionalmente y capaz de manejar conjuntos de datos de transacciones de tarjetas de crédito a gran escala [20], [39]. Finalmente, modelos clasificados en la categoría HIBRIDOS U OTROS ENFOQUES, tienen aplicaciones específicas en la detección de fraude, pero su adopción es limitada debido a que son modelos únicos, propuestos en sus respectivos estudios.

TABLA VIII
MODELOS MÁS ESTUDIADOS

TIPOS	MODELOS	FRECUENCIA	ID REFERENCIA
ML	RF	41.03%	[1], [5], [10], [14], [15], [18], [19], [25], [27], [28], [29], [32], [33], [34], [35], [36]
	KNN	35.90%	[1], [5], [8], [15], [17], [18], [21], [27], [28], [29], [32], [36], [39], [42]
	SVM	33.33%	[5], [6], [7], [8], [11], [17], [18], [25], [27], [28], [29], [34], [42]
	XGB	28.21%	[5], [7], [11], [19], [22], [24], [27], [29], [30], [34], [35]
	OTROS MODELOS DE ML	51.28%	[1], [5], [7], [8], [10], [11], [15], [18], [19], [21], [24], [27], [29], [32], [34], [35], [36], [38], [39], [41]
DL	LSTM	23.08%	[6], [14], [16], [20], [22], [27], [30], [37], [42]
	ANN	20.51%	[3], [16], [17], [22], [26], [28], [41], [42]
	MLP	12.82%	[6], [8], [17], [27], [36]
	CNN	10.26%	[14], [20], [25], [27]
	OTROS MODELOS DE DL	20.51%	[7], [10], [16], [17], [23], [41], [42], [43]
HIBRIDOS U OTROS ENFOQUES	B-LSTM-NB, Frequent Pattern Mining Model, RBM y CNN- ML	10.25%	[31], [39], [37], [36]

Nota: Elaborado a partir de los documentos analizados

Por lo tanto, RF y LSTM son los modelos más estudiados para la detección de fraude, siendo SMOTE la técnica de remuestreo más utilizada para potenciar el rendimiento de estos modelos al equilibrar los datasets.

La tercera pregunta específica para esta investigación fue: ¿Qué nivel de efectividad tienen los modelos de Machine Learning en la detección de transacciones fraudulentas? Aunque no existe una métrica ideal para evaluar la efectividad de un modelo, diversas métricas se emplean en conjunto para medir su desempeño. Los resultados de la Tabla IX, evidencian una preferencia por ciertos criterios de evaluación en los artículos analizados, empleados de forma conjunta o individual. Accuracy se posiciona como el criterio predominante, con un 79.49% de frecuencia entre los estudios analizados. Esta métrica mide la relación entre el total transacciones clasificadas correctamente respecto al total de muestras de transacciones [16], su amplio uso destaca su importancia en la evaluación global de modelos de detección de fraude. Recall mide la proporción de casos positivos correctamente identificados respecto al total de casos positivos reales [48], lo que asegura que la mayoría de las transacciones fraudulentas sean detectadas. Incrementar el Recall puede reducir el riesgo de fraude financiero causado por falsos negativos [31]. Precision se refiere a cuántas instancias de *Fraude* fueron identificadas correctamente [21]. Una alta Precision especifica que el modelo identifica correctamente los casos de fraude y minimiza los falsos positivos [49]. F1-Score representa el equilibrio optimo entre Precision y Recall. Ofrece una puntuación solitaria que incorpora la capacidad del modelo para reconocer adecuadamente las instancias positivas y negativas [33]. Es útil

cuando hay un desequilibrio entre clases, como en la detección de fraude, donde la clase *Fraude* a menudo es minoritaria [21]. AUC se refiere a la relación entre la tasa de falsos positivos y la tasa de verdaderos positivos [16]. Un valor alto de AUC indica que el modelo puede separar efectivamente las transacciones legítimas de las fraudulentas. Por último, la categoría "Otros", obtuvo un 61.54% de frecuencia, esta incluye métricas menos comunes entre los estudios.

Al analizar la relación entre estas métricas utilizando el coeficiente de correlación de Pearson, se observó una fuerte correlación positiva de 0.88 entre Precision y Recall, esto sugiere que en los artículos donde se emplea la métrica Precision, el Recall también es utilizado. Además, se obtuvo una fuerte correlación positiva de 0.65 entre Precisión y F1-Score, y una fuerte correlación positiva de 0.66 entre Recall y F1-Score, lo que indica que estas métricas son utilizadas frecuentemente para evaluar la efectividad de los modelos, además de confirma la interdependencia entre estos criterios.

TABLA IX
METRICAS PARA EVALUAR LA EFECTIVIDAD

METRICAS	FRECUENCIA	ID REFERENCIA
Accuracy	79.49%	[1], [3], [5], [7], [8], [11], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [25], [26], [28], [29], [31], [32], [33], [36], [38], [39], [40], [41], [42], [43]
Recal	74.36%	[1], [3], [5], [7], [10], [11], [14], [15], [16], [17], [18], [19], [21], [24], [26], [27], [28], [29], [31], [32], [33], [34], [36], [37], [38], [39], [41], [42], [43]
Precision	69.23%	[1], [3], [7], [10], [11], [14], [15], [16], [17], [18], [19], [21], [24], [26], [27], [28], [29], [32], [33], [34], [36], [37], [38], [39], [41], [42], [43]
F1-Score	64.10%	[1], [7], [10], [11], [14], [15], [17], [18], [19], [21], [22], [24], [27], [28], [29], [31], [32], [33], [34], [36], [37], [38], [39], [41], [43]
AUC	35.90%	[3], [6], [7], [10], [16], [19], [20], [23], [27], [29], [30], [32], [36], [39]
Otros	61.54%	[3], [5], [6], [7], [8], [10], [14], [15], [16], [17], [18], [19], [20], [22], [23], [24], [25], [26], [28], [29], [30], [32], [35], [36]

Nota: Elaborado a partir de los documentos analizados

Al ser Accuracy la metrica más utilizada para evaluar la efectividad de los modelos de ML, Dl y otros enfoques, se establecieron intervalos para clasificar solo los modelos que aplican esta métrica, según los resultados obtenidos para la misma, en sus respectivos estudios. La Tabla X muestra que los modelos de DL lograron altos niveles de efectividad en la detección de fraude, teniendo más presencia que los modelos de ML, a pesar de ser menos estudiados que estos. En el rango de 0.96 – 1.00, ANN y LSTM lideran con una presencia del 6.5% cada uno, respecto al total de articulo que emplean la métrica Accuracy. Este resultado se debe a su capacidad para capturar patrones útiles dentro del comportamiento del consumidor que ayudan a distinguir de manera efectiva las transacciones fraudulentas de las normales [42]. Aunque CNN, DNN y MLP tuvieron una menor presencia con un 3.2%, estos modelos destacaron por su capacidad para identificar patrones complejos en datos de alta dimensión, lo que resulta esencial en la detección de fraude. CNN es efectivo para procesar grandes volúmenes de datos, DNN sobresale en la captura de relaciones no lineals y MLP es ideal para generalizar a partir de datos diversos [14], [17], [8]. Con la misma presencia, el uso de Generative Adversarial Networks (GAN) en la detección de fraude representa un nuevo enfoque prometedor, por su capacidad para aprender a identificar transacciones fraudulentas con alta precisión al enseñar al discriminador a diferenciar entre datos reales y sintéticos [18]. En el análisis de los niveles de efectividad de los modelos de ML, se evidencia que XGB es el modelo más predominante en el intervalo 0.96 - 1.00, representando al 12% de los estudios. El Accuracy obtenido subraya su efectividad para identificar actividades fraudulentas, incluso en conjuntos de datos desequilibrados [11]. La adopción de este enfoque tiene un costo asociado, y puede ser difícil de implementar porque cada banco o institución financiera tiene sus propias limitaciones [19]. RF representado al 6.5% de los estudios, mostro resultado prometedores en la detección y mitigación de incidentes fraudulentos. Su efectividad se refleja en su capacidad para detectar casos de fraude correctamente y minimizar los falso positivos [33]. Los modelos Isolation Forets (IF) y LR obtuvieron una presencia del 3.2%. Por un lado, IF destaca por su capacidad para manejar grandes conjuntos de datos y detectar anomalías con una alta precisión y baja tasa de falsos positivos [38]. Mientas que LR es efectivo para clasificar las transacciones fraudulentas y no fraudulentas correctamente [21]. En la categoría OTROS ENFOQUES O HIBRIDOS, específicamente los modelos híbridos que combinan técnicas de ML y DL alcanzaron un nivel de efectividad en el intervalo de 0.96 – 1.00. Cada modelo tiene aplicaciones únicas para la detección de transacciones fraudulentas, resaltando la importancia de combinar ambos enfoques (ML y DL) para poder abordar este desafío. Sin embargo, estos modelos son únicos y propios de los autores que los proponen, por lo que su adopción generalizada aun requiere mayor validación para confirmar su efectividad en diferentes contextos.

TABLA X
MODELOS ORGANIZADOS POR ACCURACY

INTERVALOS DE ACCURACY	MODELOS ML	MODELOS DL	OTROS ENFOQUES O HIBRIDOS
[0.80 - 0.84]	No alcanzó	CNN	No alcanzó
[0.84 - 0.88]	No alcanzó	No alcanzó	No alcanzó
[0.88 - 0.92]	No alcanzó	ANN	No alcanzó
[0.92 - 0.96]	FL	SVDD, DNN y RNN	MLBM y FPMM

[0.96 - 1.00]	LR, RF, IF y XGB	CNN, LSTM, DNN, ANN, MLP y GAN	ST, CFS-LoR, RXT, FLR, Esemble (CNN-ML)
ID REFERENCIA	[5], [11], [15], [19], [21], [29], [33], [38], [43]	[3], [8], [14], [16], [17], [18], [20], [23], [25], [26], [28], [41], [42]	[1], [7], [13], [22], [31], [32], [36], [39], [40]

Nota: Elaborado a partir de los documentos analizados

Por lo tanto, Accuracy es la métrica más utiliza para evaluar la efectividad de los modelos de ML y DL en la detección de fraude. Así mismo, modelos como LSTM, ANN, XGB, RF e Híbridos, son los más efectivos para la detección de fraude, mostrando niveles de Accuracy entre 0.96 y 1.

IV. Conclusión y Discusión

Tras el análisis de los estudios se observó que los criterios más utilizados para determinar si una transacción es fraudulenta o legitima son el Tiempo y el Monto, siendo ECC el dataset más empleado, al brindar datos de transacciones reales que involucran a estos criterios, a pesar de presentar desequilibrio entre las clases de estos datos. SMOTE surge como una herramienta esencial en este aspecto, al permitir equilibrar los datos y así evitar la inclinación de los modelos hacia la clase mayoritaria. Entre los modelos existentes para la detección de fraude observó un destacado uso de RF, KNN, SVM y XGB en el enfoque de ML, mientras que entre los modelos de DL se observó un sobresaliente uso de LSTM, ANN, MLP y CNN, sin embargo, que estos sean los modelos más estudiados no quiere decir que sean los más efectivos para la detección de fraude. Así mismo, se identificó que Accuracy es la métrica más predominante en la evaluación de estos modelos, reflejando su importancia como métrica al medir el rendimiento general. La interdependencia de las métricas Precisión, Recall y F1-Score se evidenció en los coeficientes de correlación obtenidos, lo que demuestra la importancia de mantener un equilibrio entre estas para garantizar una evaluación integral de los modelos. Así mimo, modelos de ML y DL como LSTM, ANN, RF, XGB y los modelos híbridos propuestos, mostraron altos niveles de Accuracy en un rango de 0.96 y 1, evidenciando que estos son los modelos más efectivos para detectar las transacciones fraudulentas.

La detección de fraudes mediante ML y DL representa una oportunidad significativa para reducir pérdidas millonarias en el sector financiero, fortaleciendo la integridad del mercado y beneficiando a los clientes [39]. No obstante, la implementación de estas tecnologías presenta implicaciones relevantes que deben ser consideradas. Aunque los modelos de ML y DL ofrecen soluciones para gestionar grandes volúmenes de datos, su escalabilidad puede generar una mayor sobrecarga de comunicación, derivando en cuellos de botella en el rendimiento y costos operativos elevados [14]. Así mismo, el desequilibrio de clases, frecuente en los datos de transacciones, refleja los retos inherentes a la recolección de datos debido a problemas de privacidad y altos costos [17], lo que impacta en la efectividad y el costo de entrenar modelos robustos. Además, garantizar el cumplimiento de regulaciones de protección de datos y normativas añade una capa adicional de complejidad y costes [14]. Adicionalmente, la adopción de estas tecnologías implica inversiones iniciales considerables en infraestructura tecnológica, capacitación del personal y adecuación de los procesos internos, lo que representa un desafío adicional para su implementación efectiva en el entorno real.

V. Agradecimiento

Expresamos el agradecimiento al Dr. Christian Abraham Dios Castillo (c16763@utp.edu.pe), investigador de la UNIVERSIDAD TECNOLÓGICA DEL PERÚ, por su contribución en la asesoría del presente manuscrito.

Referencias

[1] A. Mniai, M. Tarik, and K. Jebari, "A Novel Framework for Credit Card Fraud Detection," IEEE Access, vol. 11, pp. 112776–112786, 2023, doi: 10.1109/ACCESS.2023.3323842.

[2] J. Nicholls, A. Kuppa, and N. A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," IEEE Access, vol. 9, pp. 163965–163986, 2021, doi: 10.1109/ACCESS.2021.3134076.

[3] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, "Multilayer perceptron artificial neural networks-based model for credit card fraud detection," Indonesian Journal of Electrical Engineering and Computer Science, vol. 26, no. 1, pp. 362–373, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp362-373.

[4] UK Finance, Annual Fraud Report 2022: The Definitive Overview of Payment Industry Fraud in 2021, London, UK: UK Finance, 2022. Available: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2022

[5] A. Shahapurkar and R. Patil, "Concept drift and machine learning model for detecting fraudulent transactions in streaming environment," International Journal of Electrical and Computer Engineering, vol. 13, no. 5, pp. 5560–5568, Oct. 2023, doi: 10.11591/ijece.v13i5.pp5560-5568.

[6] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection," IEEE Access, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[7] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," IEEE Access, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[8] I. de Zarzà, J. de Curtò, and C. T. Calafate, "Optimizing Neural Networks for Imbalanced Data," Electronics (Switzerland), vol. 12, no. 12, Jun. 2023, doi: 10.3390/electronics12122674.

[9] P. Boulieris, J. Pavlopoulos, A. Xenos, and V. Vassalos, "Fraud detection with natural language processing," Mach Learn, vol. 113, no. 8, pp. 5087–5108, Aug. 2024, doi: 10.1007/s10994-023-06354-5.

[10] Y. Ding, W. Kang, J. Feng, B. Peng, and A. Yang, "Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network," IEEE Access, vol. 11, pp. 83680–83691, 2023, doi: 10.1109/ACCESS.2023.3302339.

[11] S. M. N. Nobel et al., "Unmasking Banking Fraud: Unleashing the Power of Machine Learning and Explainable AI (XAI) on Imbalanced Data,"

Information (Switzerland), vol. 15, no. 6, Jun. 2024, doi: 10.3390/info15060298.

[12] C. Dios-Castillo, C. Chafloque-Llontop, and R. Sánchez-Rentería, "Effectiveness of Machine Learning in environmental pollution from remote sensing images. Systematic Literature Review," in Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology, Latin American and Caribbean Consortium of Engineering Institutions, 2024. doi: 10.18687/LACCEI2024.1.1.1402.

[13] D. Wiryadinata, A. Sugiharto, and Tarno, "The Use of Machine Learning to Detect Financial Transaction Fraud: Multiple Benford Law Model for Auditors," Journal of Information Systems Engineering and Business Intelligence, vol. 9, no. 2, pp. 239–252, Oct. 2023, doi: 10.20473/jisebi.9.2.239-252.

[14] T. Baabdullah, A. Alzahrani, D. B. Rawat, and C. Liu, "Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems," Future Internet, vol. 16, no. 6, Jun. 2024, doi: 10.3390/fi16060196.

[15] M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," Neural Comput Appl, vol. 36, no. 11, pp. 6231–6256, Apr. 2024, doi: 10.1007/s00521-023-09410-2.

[16] S. El Kafhali, M. Tayebi, and H. Sulimani, "An Optimized Deep Learning Approach for Detecting Fraudulent Transactions," Information (Switzerland), vol. 15, no. 4, Apr. 2024, doi: 10.3390/info15040227.

[17] N. Shome, D. D. Sarkar, R. Kashyap, and R. H. Laskar, "Detection of Credit card fraud with optimized Deep neural network in balanced data condition," Computer Science, vol. 25, no. 2, pp. 1–24, 2024, doi: 10.7494/csci.2024.25.2.5967.

[18] F. A. Almarshad, G. A. Gashgari, and A. I. A. Alzahrani, "Generative Adversarial Networks-Based Novel Approach for Fraud Detection for the European Cardholders 2013 Dataset," IEEE Access, vol. 11, pp. 107348–107368, 2023, doi: 10.1109/ACCESS.2023.3320072.

[19] S. Dalal, B. Seth, M. Radulescu, C. Secara, and C. Tolea, "Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model," Mathematics, vol. 10, no. 24, Dec. 2022, doi: 10.3390/math10244679.

[20] S. S. Sulaiman, I. Nadher, and S. M. Hameed, "Credit Card Fraud Detection Using Improved Deep Learning Models," Computers, Materials and Continua, vol. 78, no. 1, pp. 1049–1069, 2024, doi: 10.32604/cmc.2023.046051.

[21] V. Chang, B. Ali, L. Golightly, M. A. Ganatra, and M. Mohamed, "Investigating Credit Card Payment Fraud with Detection Methods Using Advanced Machine Learning," Information (Switzerland), vol. 15, no. 8, Aug. 2024, doi: 10.3390/info15080478.

[22] G. Charizanos, H. Demirhan, and D. İçen, "An online fuzzy fraud detection framework for credit card transactions," Expert Syst Appl, vol. 252, Oct. 2024, doi: 10.1016/j.eswa.2024.124127.

[23] Kanika, J. Singla, A. K. Bashir, Y. Nam, N. U. I. Hasan, and U. Tariq, "Handling class imbalance in online transaction fraud detection," Computers, Materials and Continua, vol. 70, no. 2, pp. 2861–2877, 2022, doi: 10.32604/cmc.2022.019990.

[24] D. P. Prabha and C. V. Priscilla, "Probabilistic XGBoost Threshold Classification with Autoencoder for Credit Card Fraud Detection," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, pp. 528–537, 2023, doi: 10.17762/ijritcc.v11i8s.7234.

[25] S. Xie, L. Liu, G. Sun, B. Pan, L. Lang, and P. Guo, "Enhanced E-commerce Fraud Prediction Based on a Convolutional Neural Network Model," Computers, Materials and Continua, vol. 75, no. 1, pp. 1107–1117, 2023, doi: 10.32604/cmc.2023.034917.

[26] H. Ahmad, B. Kasasbeh, B. Al-Dabaybah, and E. Rawashdeh, "EFN-SMOTE: An effective oversampling technique for credit card fraud detection by utilizing noise filtering and fuzzy c-means clustering," International Journal of Data and Network Science, vol. 7, no. 3, pp. 1025–1032, Jun. 2023, doi: 10.5267/j.ijdns.2023.6.003.

[27] S. Jiang, R. Dong, J. Wang, and M. Xia, "Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network," Systems, vol. 11, no. 6, Jun. 2023, doi: 10.3390/systems11060305.

[28] A. A. Abdirahman, A. O. Hashi, U. M. Dahir, M. A. Elmi, and O. E. R. Rodriguez, "Enhancing Security in Mobile Wallet Payments: Machine Learning-Based Fraud Detection Across Prominent Wallet Platforms," SSRG International Journal of Electronics and Communication Engineering, vol. 11, no. 3, pp. 96–105, Mar. 2024, doi: 10.14445/23488549/IJECE-V11I3P110.

[29] P. Hajek, M. Z. Abedin, and U. Sivarajah, "Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework," Information Systems Frontiers, vol. 25, no. 5, pp. 1985–2003, Oct. 2023, doi: 10.1007/s10796-022-10346-6.

[30] G. Zioviris, K. Kolomvatsos, and G. Stamoulis, "An intelligent sequential fraud detection model based on deep learning," Journal of Supercomputing, vol. 80, no. 10, pp. 14824–14847, Jul. 2024, doi: 10.1007/s11227-024-06030-y.

[31] J. Kim, H. Jung, and W. Kim, "Sequential Pattern Mining Approach for Personalized Fraudulent Transaction Detection in Online Banking," Sustainability (Switzerland), vol. 14, no. 15, Aug. 2022, doi: 10.3390/su14159791.

[32] N. Nayyer, N. Javaid, M. Akbar, A. Aldegheishem, N. Alrajeh, and M. Jamil, "A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities," IEEE Access, vol. 11, pp. 90916–90938, 2023, doi: 10.1109/ACCESS.2023.3308298.

[33] I. Jaiswal, A. Bharadwaj, K. Kumari, and N. Agarwal, "Credit Card Deception Recognition Using Random Forest Machine Learning Algorithm," EAI Endorsed Transactions on Internet of Things, vol. 10, 2024, doi: 10.4108/eetiot.5347.

[34] C. Hamza, A. Lylia, C. Nadine, and C. Nicolas, "Semi-supervised Method to Detect Fraudulent Transactions and Identify Fraud Types while Minimizing Mounting Costs." [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud

[35] D. Breskuvien and G. Dzemyda, "Categorical Feature Encoding Techniques for Improved Classifier Performance when Dealing with Imbalanced Data of Fraudulent Transactions," International Journal of Computers, Communications and Control, vol. 18, no. 3, 2023, doi: 10.15837/ijccc.2023.3.5433.

[36] S. Islam, M. M. Haque, and A. N. M. R. Karim, "A rule-based machine learning model for financial fraud detection," International Journal of Electrical and Computer Engineering, vol. 14, no. 1, pp. 759–771, Feb. 2024, doi: 10.11591/ijece.v14i1.pp759-771.

[37] A. L. Karn et al., “B-LSTM-NB based composite sequence learning model for detecting fraudulent financial activities,” Malaysian Journal of Computer Science, vol. 2022, no. Special Issue 1, pp. 30–49, 2022, doi: 10.22452/mjcs.sp2022no1.3.

[38] A. Hanae, B. Abdellah, E. Saida, and G. Youssef, “End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions.” [Online]. Available: www.ijacsa.thesai.org

[39] R. Ming, O. Abdelrahman, N. Innab, and M. H. K. Ibrahim, “Enhancing fraud detection in auto insurance and credit card transactions: a novel approach integrating CNNs and machine learning algorithms,” PeerJ Comput Sci, vol. 10, 2024, doi: 10.7717/peerj-cs.2088.

[40] N. Prabhakaran and R. Nedunchelian, “Combined Feature Set with Logistic Regression Model to Detect Credit Card Frauds in Real Time Applications,” Journal of Machine and Computing, vol. 4, no. 3, pp. 804–812, Jul. 2024, doi: 10.53759/7669/jmc202404074.

[41] O. Ndama, I. Bensassi, and E. M. En-Naimi, “Optimizing credit card fraud detection: a deep learning approach to imbalanced datasets,” International Journal of Electrical and Computer Engineering, vol. 14, no. 4, pp. 4802–4814, Aug. 2024, doi: 10.11591/ijece.v14i4.pp4802-4814.

[42] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, “Enhanced credit card fraud detection based on attention mechanism and LSTM deep model,” J Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00541-8.

[43] T. Awosika, R. M. Shukla, and B. Pranggono, “Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection,” IEEE Access, vol. 12, pp. 64551–64560, 2024, doi: 10.1109/ACCESS.2024.3394528.

[44] M. Mukherjee and M. Khushi, “Smote-enc: A novel smote-based method to generate synthetic data for nominal and continuous features,” *Applied System Innovation*, vol. 4, no. 1, 2021, doi: 10.3390/asi4010018.

[45] J. Li, W. H. Chen, Q. Xu, N. Shah, J. C. Kohler, and T. K. Mackey, “Detection of self-reported experiences with corruption on twitter using unsupervised machine learning,” *Social Sciences and Humanities Open*, vol. 2, no. 1, Jan. 2020, doi: 10.1016/j.ssaho.2020.100060.

[46] G. Habib and S. Qureshi, “Optimization and acceleration of convolutional neural networks: A survey,” Jul. 01, 2022, *King Saud bin Abdulaziz University*. doi: 10.1016/j.jksuci.2020.10.004.

[47] T. Berhane, T. Melese, A. Walelign, and A. Mohammed, “A Hybrid Convolutional Neural Network and Support Vector Machine-Based Credit Card Fraud Detection Model,” *Math Probl Eng*, vol. 2023, no. 1, Jan. 2023, doi: 10.1155/2023/8134627.

[48] M. Mandava, S. R. Vinta, H. Ghosh, and I. S. Rahat, “An All-Inclusive Machine Learning and Deep Learning Method for Forecasting Cardiovascular Disease in Bangladeshi Population,” *EAI Endorsed Trans Pervasive Health Technol*, vol. 9, May 2023, doi: 10.4108/eetpht.9.4052.

[49] H. Ghosh, M. A. Tusher, I. S. Rahat, S. Khasim, and S. N. Mohanty, “Water Quality Assessment Through Predictive Machine Learning,” in *Lecture Notes in Networks and Systems*, Springer Science and Business Media Deutschland GmbH, 2023, pp. 77–88. doi: 10.1007/978-981-99-3177-4_6.