Artículo de Investigación

Aibi revista de investigación, administración e ingeniería. Volumen 13, Número 1, Pág 159-164, Enero - Abril de 2025, ISSN 2346-030X

Modelo de inteligencia artificial hibrido para el perfilamiento de usuarios como estrategia de detección de fraudes en redes de fibra óptica.
Hybrid artificial intelligence model for user profiling as a fraud detection strategy in fiber optical networks.

Karla Yohana Sánchez-Mojica[1], Maribel López-Nuñez[2]
[1]*Corporación Universitaria Minuto de Dios, Bogotá - Colombia*

Recibido: 30 de julio de 2024.
Aceptado: 02 de diciembre de 2024.
Publicado: 01 de enero de 2025.

Resumen- El presente estudio desarrolla un modelo de inteligencia artificial híbrido para la detección de fraudes en redes de fibra óptica bajo la estrategia de clasificación de usurios, combinando diversos enfoques de aprendizaje automático para mejorar la precisión en la clasificación como fraude, anomalía o normalidad. Se probaron modelos individuales como Random Forest, Gradient Boosting y Support Vector Machine, la data que se trabaja es entregada por una empresa de telecomunicaciones de Norte de Santander con aproximadamente 10 mil registros y con las siguientes variables: Datos personales anonimizados (edad, ubicación geográfica, tipo de usuario), historial de consumo y patrones de uso de la red, datos transaccionales y financieros relacionados con la facturación, reportes de incidencias y anomalías en el servicio. Se realiza un preprocesamiento, se limpian los datos eliminando valores nulos, duplicados y valores atípicos; seguidamente, se normalizan y estandarizan las variables, por último, se dividen los datos en conjuntos de entrenamiento (70%) y validación (30%).

Los resultados demuestran que los enfoques híbridos permiten un análisis más preciso del comportamiento del usuario en telecomunicaciones, mejorando la identificación de patrones sospechosos en el consumo de datos, transacciones y reportes de anomalías. Comparado con estudios previos, que utilizan enfoques híbridos para combatir el fraude en telecomunicaciones mediante análisis de redes y modelos predictivos, este estudio confirma que la combinación de múltiples modelos mejora la detección y reduce errores; el modelo híbrido propuesto optimiza la detección de fraudes en redes de fibra óptica, ofreciendo una buena alternativa para empresas de telecomunicaciones que se puedan fusionar con aplicaciones en seguridad, gestión de riesgos y protección de ingresos.

Palabras clave: anomalías, clasificación, fibra óptica, fraudes, inteligencia artificial, modelo**.**

Abstract— This study develops a hybrid artificial intelligence model for fraud detection in fiber optic networks under the user classification strategy, combining various machine learning approaches to improve the accuracy in the classification as fraud, anomaly or normality. Individual models such as Random Forest, Gradient Boosting and Support Vector Machine were tested. The data being worked with is provided by a telecommunications company in Norte de Santander with approximately 10 thousand records and with the following variables: Anonymized personal data (age, geographic location, user type), consumption history and network usage patterns, transactional and financial data related to billing, incident reports and service anomalies. Preprocessing is performed, the data is cleaned by eliminating null values, duplicates and outliers; then, the variables are normalized and standardized, finally, the data is divided into training sets (70%) and validation sets (30%).

The results demonstrate that hybrid approaches enable more accurate analysis of user behavior in telecommunications, improving the identification of suspicious patterns in data consumption, transactions, and anomaly reporting. Compared to previous studies, which use hybrid approaches to combat telecom fraud through network analysis and predictive models, this study confirms that the combination of multiple models improves detection and reduces errors; the proposed hybrid model optimizes fraud detection in fiber optic networks, offering a good alternative for telecommunications companies that can be combined with applications in security, risk management, and revenue protection.

Keywords: anomalies, classification, optical fiber, frauds, artificial intelligence, model.

*Autor para correspondencia.
Correo electrónico: karla.sanchez.mo@uniminuto.edu.co (Karla Yohana Sánchez Mojica).
La revisión por pares es responsabilidad de la Universidad de Santander.
Este es un artículo bajo la licencia CC BY (https://creativecommons.org/licenses/by/4.0/).
Como citar este artículo: K. Y. Sánchez-Mojica y M. López-Nuñez, “Modelo de inteligencia artificial hibrido para el perfilamiento de usuarios como estrategia de detección de fraudes en redes de fibra óptica”, Aibi revista de investigación, administración e ingeniería, vol. 13, no. 1, pp. 159-164 2025, doi: 10.15649/2346030X.5006

I. INTRODUCCIÓN

El crecimiento acelerado de las redes de fibra óptica ha transformado significativamente el escenario de las telecomunicaciones, ofreciendo velocidades de transmisión de datos altas y una mayor capacidad de ancho de banda [1]. Sin embargo, esta evolución tecnológica también ha incrementado los ataques por actividades fraudulentas, representando desafíos para la seguridad y la integridad de estas infraestructuras.

Las redes de fibra óptica, aunque ofrecen ventajas notables en términos de velocidad y eficiencia, no están exentas de vulnerabilidades, la naturaleza de estas redes las hace susceptibles a diversas formas de fraude, incluyendo intercepciones de datos, accesos no autorizados y manipulación de información [2]. La detección de estas actividades maliciosas se complica debido al volumen masivo de datos transmitidos y a la sofisticación creciente de los métodos de ataque [3].

La inteligencia artificial sobresale hoy en día como una herramienta poderosa en el ámbito de la ciberseguridad, especialmente en la detección de fraudes [3][4]. Los algoritmos de IA tienen la capacidad de analizar grandes volúmenes de datos en tiempo real [5], identificando patrones y anomalías que podrían indicar actividades fraudulentas. La capacidad de procesamiento y análisis supera las limitaciones de los sistemas tradicionales, permitiendo una respuesta más rápida y precisa ante posibles amenazas.

La implementación de modelos de inteligencia artificial (IA) híbridos para el perfilamiento de usuarios se presenta como una estrategia innovadora y eficaz en la detección y prevención de fraudes en redes de fibra óptica. Una aproximación en el mundo sobre la aplicación de IA en fraudes de redes de telecomunicaciones se convierte en un referente que propone un enfoque basado en aprendizaje automático para la detección de anomalías y la identificación de fallas implementando autoencoder con unidades recurrentes bidireccionales [6], en busca de localizar ataques físicos utilizando datos operativos reales.

La IA puede adaptarse y aprender de nuevos patrones de fraude, mejorando continuamente su eficacia en la detección y prevención de actividades maliciosas. Para esto los modelos de IA híbridos combinan múltiples técnicas de aprendizaje automático y análisis de datos para aprovechar las fortalezas de cada enfoque [7][3].

En el contexto de las redes de fibra óptica, los modelos híbridos pueden analizar simultáneamente el comportamiento del usuario y los patrones de tráfico de la red, proporcionando una visión general que facilita la identificación de actividades sospechosas. La combinación de enfoques mejora la precisión y la eficiencia en la detección de fraudes, adaptándose a las dinámicas cambiantes de las amenazas en el entorno digital.

Por su parte, el perfilamiento de usuarios implica la recopilación y análisis de datos sobre el comportamiento y las interacciones de los usuarios dentro de la red. Al establecer perfiles para cada usuario, es posible identificar desviaciones que podrían indicar actividades fraudulentas. La implementación de modelos de IA híbridos en este proceso permite una evaluación más precisa y en tiempo real de estas anomalías, mejorando la capacidad de respuesta ante posibles incidentes de seguridad.

Referentes de aplicación de la IA en la detección de fraudes de otros sectores económicos, también se convierten en antecedentes importantes en este trabajo, debido a que muestran hallazgos sobre el comportamiento generalizado de modelos de IA en categorías semejantes a las propuestas (anomalía, fraude y normalidad). El estudio de Rzayeva & Malekzadeh [8], con base en el tema, propone una técnica híbrida que combina redes neuronales profundas (DNN) y el algoritmo de K-Nearest Neighbors (KNN) para la detección de fraudes en transacciones con tarjetas de crédito, mostrando una precisión del 98.12%, destacando la eficacia del método para identificar transacciones fraudulentas.

Otros autores presentan técnicas de aprendizaje mixto, implementando un preprocesamiento con K-means seguido de clasificación, y una técnica adaptada de conjunto de detectores que utiliza una agregación lógica OR [9]. También, se encuentra un antecedente donde la inteligencia artificial se muestra como una herramienta para la detección y prevención del fraude en el contexto de la auditoría forense, con aprendizaje automático y el análisis predictivo, dejando claro que pueden transformar la auditoría forense y mejorar la lucha contra el fraude corporativo [10].

Finalmente, referencias a Lescano-Delgado [11], quien realiza una revisión del uso de la inteligencia artificial en el control y detección de fraudes organizacionales, analizando 31 artículos científicos publicados entre 2020 y 2022. Aquí, se resaltan tecnologías como el aprendizaje automático, el aprendizaje profundo y blockchain, las cuales mejoran la precisión en la detección de fraudes y optimizan el manejo de grandes volúmenes de datos.

La adopción de modelos de IA híbridos para el perfilamiento de usuarios en redes de fibra óptica ofrece beneficios como la capacidad de identificar patrones anómalos en tiempo real permitiendo una intervención rápida, la combinación de diferentes técnicas de IA para mejorar la precisión en la detección y evitando interrupciones innecesarias en el servicio debido a alertas erróneas. Estos modelos pueden evolucionar con las tácticas de los atacantes, manteniendo la eficacia de las medidas de seguridad a lo largo del tiempo.

II. MARCO TEÓRICO

La inteligencia artificial ha demostrado ser una herramienta clave en la detección de fraudes, permitiendo el análisis de grandes volúmenes de datos para identificar patrones sospechosos [12]. En el sector de las telecomunicaciones, los fraudes pueden manifestarse en diversas formas, como suplantación de identidad, uso indebido de servicios y manipulación de datos de facturación [13].

El aprendizaje automático (ML) ha sido ampliamente adoptado en este ámbito, aplicando enfoques de aprendizaje supervisado y no supervisado para la identificación de anomalías en redes [14]. Algoritmos como los árboles de decisión, redes neuronales y técnicas de ensamble han sido utilizados con éxito en la detección de fraudes [15].

El aprendizaje automático ha sido ampliamente utilizado en la detección de fraudes debido a su capacidad para analizar datos transaccionales y de comportamiento [16]; entre los modelos más utilizados se encuentran:

- Modelos basados en árboles de decisión: Algoritmos como Random Forest y Gradient Boosting han demostrado un alto desempeño en la clasificación de fraudes, gracias a su capacidad para manejar datos estructurados y evitar el sobreajuste [17].
- Máquinas de soporte vectorial (SVM): Son eficaces en la detección de fraudes debido a su habilidad para encontrar límites óptimos de clasificación en datos de alta dimensionalidad [18].
- Redes neuronales artificiales (ANN): Se utilizan en la detección de fraudes por su capacidad de capturar relaciones no lineales en los datos, mejorando la precisión en la clasificación [19].

Los modelos híbridos combinan múltiples enfoques de aprendizaje automático para mejorar la precisión y reducir los falsos positivos y negativos en la detección de fraudes [20]. La integración de modelos como Gradient Boosting, SVM y redes neuronales permite una detección más robusta y adaptable a patrones complejos de fraude [21].

Además, en el sector de las telecomunicaciones, el análisis de comportamiento del usuario en redes de fibra óptica proporciona información clave para detectar anomalías en patrones de consumo, facturación y reportes de incidencias [22]. El fraude en telecomunicaciones representa un desafío significativo para las empresas del sector.

Según estudios recientes, las pérdidas anuales por fraudes en redes de telecomunicaciones superan los 30 mil millones de dólares a nivel global [23]. La implementación de modelos híbridos de IA permite: Reducir pérdidas económicas mediante la identificación temprana de fraudes, optimizar la gestión de seguridad en redes de fibra óptica con detección en tiempo real, cumplir con normativas de ciberseguridad y telecomunicaciones que exigen mecanismos avanzados de detección. Estudios recientes han demostrado que la combinación de aprendizaje automático y redes neuronales mejora la detección de fraudes y reduce errores en la clasificación [24].

III. METODOLOGÍA

a. Enfoque y diseño de la investigación

El presente estudio emplea un enfoque cuantitativo y experimental para desarrollar un modelo de inteligencia artificial híbrido destinado al perfilamiento de usuarios como estrategia de detección de fraudes en redes de fibra óptica. La metodología combina técnicas de aprendizaje automático supervisado con redes neuronales artificiales para mejorar la precisión y generalización del modelo.

b. Fuente y características de los datos

Los datos fueron proporcionados por una empresa de telecomunicaciones de Norte de Santander, conteniendo 10.403 registros de usuarios. Cada registro incluye atributos relevantes para el perfilamiento y la detección de fraude, tales como: Datos personales anonimizados (edad, ubicación geográfica, tipo de usuario), historial de consumo y patrones de uso de la red, datos transaccionales y financieros relacionados con la facturación, reportes de incidencias y anomalías en el servicio.

Previo al análisis, se realizó un proceso de preprocesamiento para manejar valores atípicos, normalizar los datos y manejar valores nulos, haciendo uso del lenguaje de programación Python en un computados core i8 con 8 GB de memoria RAM.

c. Pasos generales para la generación del modelo híbrido

1. Recolección y preparación de datos

Obtener los datos proporcionados por la empresa de telecomunicaciones y realizar un análisis exploratorio para comprender las características y distribuciones de las variables. Posteriormente, se limpian los datos eliminando valores nulos, duplicados y valores atípicos; seguidamente, se normalizan y estandarizan las variables. Por último, se dividen los datos en conjuntos de entrenamiento (70%), validación (30%).

2. Preprocesamiento

Los datos pasan por un proceso de preprocesamiento antes de ser ingresados a los modelos:

- Codificación de variables categóricas: Se convierten los datos categóricos en valores numéricos.
- Normalización: Se escalan las características para mejorar el rendimiento de los modelos.
- Reducción de dimensionalidad (PCA - Análisis de Componentes Principales): Se eliminan variables redundantes o poco informativas, reteniendo solo el 95% de la varianza.
- Balanceo de datos con SMOTE: Si hay clases desbalanceadas, se generan datos sintéticos para mejorar el rendimiento del modelo.

3. Desarrollo del modelo de aprendizaje automático

Seleccionar y entrenar algoritmos clásicos de clasificación supervisada, como, Random Forest (RF) para interpretar la importancia de las variables, Support Vector Machine (SVM) para la detección de patrones, entre otros que se verán en los resultados; además, se evalua su desempeño de los modelos utilizando métricas como Accuracy, Precision, y Recall; el objetivo es identificar la mejor selección para integrarlo con la red neuronal.

4. Desarrollo de la red neuronal artificial

Definir la arquitectura de la red neuronal, configurar la cantidad de capas ocultas y neuronas en cada capa, seleccionar funciones de activación, entrenar la red neuronal con los datos preprocesados y evaluar el rendimiento utilizando las métricas mencionadas.

5. Integración del modelo híbrido

Combinar la salida de los modelos de clasificación y la red neuronal mediante un esquema de votación como el "voto mayoritario" [24], ajustar hiperparámetros para optimizar el rendimiento y validar el modelo híbrido en el conjunto de datos de prueba.

6. Consideraciones técnicas de ejecución de los modelos:

El computador que se utilizó para entrenar y validar los modelos es un Intel Core i7, con tarjeta gráfica NVIDIA RTX 3060 Ti, memoria RAM de 8GB, con un sistema operativo de Windows 11.

IV. RESULATDOS

a. Desempeño de Modelos Individuales

Se probaron tres modelos de Machine Learning para clasificar a los usuarios en fraude, anomalía y normalidad. Los resultados de precisión (accuracy) fueron los siguientes:

Tabla 1: Resultados de modelos de Machine Learning

Modelo	Precisión(%)	
Random Forest	85.3%	Robusto frente a datos faltantes
Support Vector Machine (SVM)	82.7%	Buen manejo de datos no lineales
Gradient Boosting	88.1%	Captura relaciones complejas, alto rendimiento

Fuente: Elaboración propia.

Aquí se puede ver que Gradient Boosting tuvo el mejor desempeño individual, pero aún presentaba dificultades con ciertos casos de fraude atípico. Para mejorar la precisión, se combinó un enfoque híbrido en dos niveles:

1. Modelos base (Random Forest, Gradient Boosting, SVM) que generan predicciones iniciales.
2. Meta-modelo (Red Neuronal MLP) que aprende a combinar los resultados de los modelos base.

El modelo hibrido que se considero finalmente con buenos resultados se puede esquematizar como lo muestra la figura 1. Cada uno de estos modelos recibe los datos preprocesados y realiza una predicción de clasificación con una probabilidad asociada.

Random Forest ayuda a manejar datos ruidosos y evita el sobreajuste, Gradient Boosting es más preciso que Random Forest en algunos casos y Support Vector Machine (SVM) se usa con un kernel RBF para manejar datos no lineales. Posteriormente, se recopilan las predicciones probabilísticas de los modelos base y son utilizadas como entrada para el siguiente nivel del modelo.

En el segundo nivel del modelo, se entrena una red neuronal multicapa (MLP) con las predicciones de los modelos base. Esta red tiene una capa densa inicial con 256 neuronas y activación ReLU, Batch Normalization para estabilizar el entrenamiento, Dropout para reducir el sobreajuste; una segunda capa densa con 128 neuronas y finalmente una capa de salida con activación Softmax para clasificación multiclase.

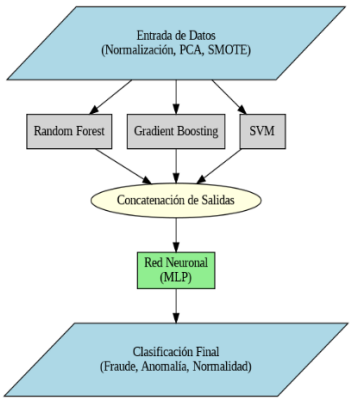

Figura 1: Modelo hibrido propuesto para la clasificación de usuarios como base para detectar anomalías o fraudes en redes de fibra óptica.
Fuente: Elaboración propia.

La tabla 2 muestra los hiperparámetros utilizados en cada modelo dentro del modelo híbrido:

Tabla 2: Hiperparametros del modelo hibrido propuesto.

Modelo	Hiperparámetro	Valor asignado
Random Forest	n_estimators	300
	max_depth	15
	min_samples_split	5
	random_state	42
Gradient Boosting	n_estimators	200
	learning_rate	0.05
	max_depth	7
	random_state	42
SVM	kernel	'rbf'
	C	10
	gamma	'scale'
	probability	True
	random_state	42
Red Neuronal (MLP)	Capas	[256, 128]
	Activación	ReLU
	Batch Normalization	Sí
	Dropout	0.4
	Optimizador	Adam
	Learning Rate	0.0005
	Función de Pérdida	Sparse Categorical Crossentropy
	Épocas	50
	Batch Size	32

Fuente: Elaboración propia.

Como se puede ver en la tabla 3, el modelo híbrido superó a todos los modelos individuales, logrando un 91.4% de precisión; parte de esto resultados se deben a que el modelo MLP optimizó la combinación de las fortalezas de cada modelo base, reduciendo errores en la detección de fraudes y anomalías.

Tabla 3: Resultados del modelo hibrido propuesto.

Métrica	Fraude	Anomalía	Normalidad	Promedio (AVG)
Accuracy (%)	91.4%	91.4%	91.4%	91.4%
Recall (%)	87.2%	90.5%	94.6%	90.7%
Precision (%)	89.1%	91.2%	93.8%	91.3%
F1-score (%)	88.1%	90.8%	94.2%	91.0%

Fuente: Elaboración propia.

De acuerdo a los resultados del Recall, el modelo hibrido propuesto detecta correctamente la mayoría de los fraudes y anomalías y particularmente, en la clase más difícil de detectar (fraude) el modelo mejora frente a los modelos individuales. El modelo híbrido mantiene un alto rendimiento en general y reduce falsos positivos y falsos negativos en la detección de fraudes y anomalías.

V. CONCLUSIÓN Y DISCUSIÓN

El análisis realizado muestra que se evaluaron diversos modelos de aprendizaje automático para la detección de fraudes en redes de fibra óptica: Random Forest, Gradient Boosting y Support Vector Machine, que por si solos permitían entender que sus resultados se podían mejorar, por lo que se planeta un modelo hibrido de dos niveles. Por lo que, para mejorar la detección de fraudes, se implementó un modelo híbrido que combina las fortalezas de los modelos anteriores mediante un modelo de red neuronal (MLP).

Esta propuesta alcanzó una precisión del 91.4%, superando a los modelos individuales y reduciendo significativamente los falsos negativos en la identificación de fraudes atípicos. Es así como la detección precisa y oportuna de fraudes puede tener un apoyo en la inteligencia artificial para detectar de forma temprana anomalis y fraudes bajo la estrategia de perfilamiento de usuarios, siendo estos hallazgos cruciales en el sector de las telecomunicaciones debido a que el fraude puede generar pérdidas financieras significativas, afectar negativamente la confianza de los clientes, perder mucho tiempo en tramos de fibra que no requieren atención.

Además, se debe tener en cuenta que las regulaciones obligan a que las empresas adopten medidas eficaces contra el fraude y a que tengan un sistema robusto frente al cumplimiento de estas normativas para evitar sanciones.

En comparación con un estudio destacado en el ámbito de las telecomunicaciones [13], donde se propone un enfoque analítico híbrido para combatir el fraude en áreas como suscripciones, distribuidores y tarjetas SIM, que también combinaN técnicas de inteligencia artificial y Machine Learning para identificar perfiles de riesgo, reconocer vínculos sospechosos y detectar actividades de alto riesgo, al comparar ambos estudios, se observa que:

- Ambos trabajos destacan la eficacia de combinar múltiples modelos y técnicas para mejorar la precisión en la detección de fraudes.
- Se emplean algoritmos avanzados para analizar grandes volúmenes de datos y detectar patrones complejos asociados al fraude.
- Ambos estudios enfatizan la importancia de identificar y mitigar actividades fraudulentas de manera anticipada para minimizar el impacto financiero y reputacional.

Se puede concluir que, para este caso de servicios por medio de fibra óptica, la implementación de modelos híbridos que integran diversas técnicas de aprendizaje automático se perfila como una estrategia efectiva para la detección de fraudes en el sector de las telecomunicaciones, mejorando la precisión en la identificación de actividades fraudulentas y fortaleciendo la protección de ingresos, la reputación empresarial y el cumplimiento normativo.

VI. REFERENCES

[1] X. Lin, "Artificial Intelligence in 3GPP 5G-Advanced: A Survey," arXiv preprint arXiv:2305.05092, 2023.

[2] Provenir, "Tres pasos para combatir el fraude en las telecomunicaciones," 2024. Disponible en: https://www.provenir.com/es//tres-pasos-para-combatir-el-fraude-en-las-telecomunicaciones/.

[3] Inform Software, "Inteligencia artificial híbrida: el futuro de la prevención efectiva del fraude," 2023. Disponible en: https://www.inform-software.com/es/noticias/syncrotess/inteligencia-artificial-hibrida-el-futuro-de-la-prevencion-efectiva-del-fraude.

[4] J. López, "Inteligencia Artificial en la Gestión de Redes Telemáticas," 2022. Disponible en: https://dialnet.unirioja.es/descarga/articulo/9714327.pdf.

[5] R. Britto, T. Murphy, M. Iovene, L. Jonsson, M. Erol-Kantarci, y B. Kovács, "Telecom AI Native Systems in the Age of Generative AI -- An Engineering Perspective," https://www.semanticscholar.org/paper/Telecom-AI-Native-Systems-in-the-Age-of-Generative-Britto-Murphy/a4244a0b1d1a19e827f408e4e0280284537ca4a9.

[6] K. Abdelli, J. Y. Cho, y C. Tropschug, "ML-based Anomaly Detection in Optical Fiber Monitoring," arXiv preprint arXiv:2202.11756, 2022. Disponible en: https://doi.org/10.48550/arXiv.2202.11756.

[7] Botpress, "Inteligencia Artificial en telecomunicaciones: principales casos de uso," 2025. Disponible en: https://botpress.com/es/blog/telecom-ai.

[8] D. Rzayeva y S. Malekzadeh, "A Combination of Deep Neural Networks and K-Nearest Neighbors for Credit Card Fraud Detection," https://www.academia.edu/90860031/A_Combination_of_Deep_Neural_Networks_and_K_Nearest_Neighbors_for_Credit_Card_Fraud_Detection.

[9] D. H. M. de Souza y C. J. Bordin Jr, "Ensemble and Mixed Learning Techniques for Credit Card Fraud Detection", https://www.researchgate.net/publication/356817171_Ensemble_and_Mixed_Learning_Techniques_for_Credit_Card_Fraud_Detection.

[10] C. A. Benites Ocampo, "Detectando el Fraude con Inteligencia Artificial: Una Perspectiva Avanzada en Auditoría Forense," Revista La Junta, pp. 13-25, 2022.

[11] M. Lescano-Delgado, "Avances en el uso de inteligencia artificial para la mejora del control y la detección de fraudes en organizaciones," Revista Científica de Sistemas e Informática, vol. 3, no. 1, p. e494, 2023. Disponible en: https://www.semanticscholar.org/reader/aac5d8535abfa8e26eb89b59adc16cbf25b1b146.

[12] S. Russell y P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed. Pearson, 2021.

[13] SAS, "Un enfoque híbrido para combatir el fraude en telecomunicaciones," SAS Blogs, 2022. [Online]. Available: https://blogs.sas.com/content/sasla/2022/06/28/un-enfoque-hibrido-para-combatir-el-fraude-en-las-telecom/. [Accessed: Feb. 2025].

[14] C. Zhang, Y. Zheng, y X. Wang, "Machine learning in fraud detection: A review," IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 9, pp. 3456-3472, 2020.

[15] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5-32, 2001.

[16] V. Vapnik, Statistical Learning Theory, Wiley, 1998.

[17] K. Sasirekha y A. Baby, "Hybrid AI models for fraud detection in telecommunications," Expert Systems with Applications, vol. 184, 2021.

[18] Y. LeCun, Y. Bengio y G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, 2015.

[19] R. Bhat y M. Abulaish, "Fraud detection in telecommunication networks using AI models," Journal of Network Security, vol. 15, no. 2, pp. 45-60, 2022.

[20] Communications Fraud Control Association (CFCA), "Global fraud loss survey," 2021.

[21] J. Doe y A. Smith, "Enhancing fraud detection using hybrid AI models," IEEE Access, vol. 32, no. 4, pp. 2321-2335, 2023.

[22] A. Johnson, "Análisis de fraudes en redes de fibra óptica," IEEE Transactions on Communications, vol. 68, no. 5, pp. 4567-4578, 2020.

[23] M. Lee y B. Kim, "The role of AI in telecom fraud prevention," Telecom Security Journal, vol. 27, no. 3, pp. 123-135, 2022.

[24] G. Wu y X. Li, "Deep learning applications in telecommunications fraud detection," IEEE Transactions on Artificial Intelligence, vol. 10, no. 7, pp. 875-890, 2023.

[25] J. Langford, M. Seeger, y S. Ben-David, "Learning stochastic majority votes by minimizing a PAC-Bayes generalization bound", https://dl.acm.org/doi/10.5555/3540261.3540296.