Universidad de Costa Rica

Escuela de Matemática

Bitácora 2

Por:

Juan Carlos Aguilar Alfaro, A90081

Manfred D. Porras Rojas, B86119

Holmar Rivera, B86564

Dominick Rodríguez Trejos, B76600

Mayo 2024

Índice

1. Objetivos

1.1. General

- Entender como funcionan los métodos o algoritmos de detección y prevención de fraude para poder aplicarlos y evaluar su eficacia

1.2. Específicos

- Describir los conceptos esenciales para entender la problemática de fraude crediticio.
- Investigar los diversos métodos de detección y prevención de fraude crediticio, específicamente aquellos que puedan ser implementados por medio de Python.
- Determinar las ventajas y limitaciones de los diversos métodos de detección y prevención de fraude y evaluar su eficacia.

2. Marco Teórico

2.1. Fraude crediticio

Para empezar, es fundamental tener una idea clara de nuestro objeto de estudio, así que a continuación se explorarán los conceptos relacionados a la problemática de fraude crediticio, junto con las definiciones necesarias para comprender, estudiar y, eventualmente, detectar y prevenir.

Podemos definir fraude crediticio como lo hace Afriyie et al (2023) [1] en términos bastante sencillos como el uso de la tarjeta de crédito de un tercero sin su permiso previo, ya sea por hurto del plástico o por otros medios. Esta definición sirve como un punto de partida, el concepto en sí es simple y fácil de entender, pero puedo complicarse bastante en cuanto a la manera en la que se clasifican los delitos de este tipo y en como los criminales aprovechan las herramientas que tienen a disposición para cometer el delito.

A la definición anterior es sensato añadir un tipo diferente de fraude crediticio, el cuál no involucra el robo directo de la tarjeta de crédito de otro individuo, Baesens et all (2015) [2] brinda la definición de fraude en solicitudes, application fraud en ingles, él cuál consiste en el robo o manufacturación de credenciales e información personal para la solicitud de tarjetas de crédito, las cuales son usadas lo más rápido posible para evitar detección, en casos esta práctica tiene efectos sobre el crédito de los individuos cuyos datos han robado.

Con una definición más concreta de fraude crediticio podemos indagar un poco más en como se desarrolla esta problemática en la actualidad, ahora más que nunca el acceso a la información sensible de nuestras cuentas de crédito es sumamente importante, en un mundo de transacciones digitales y en linea, resguardar y mantener la información de nuestras cuentas crediticias en secreto es fundamental en la batalla contra el fraude, ya que con acceso a esta información es muy sencillo para los estafadores realizar transacciones sin consentimiento previo.

Es integral reconocer que, en los recientes años, la problemática de fraude se ha intensificado bastante debido a los avances y promoción de transacciones digitales, e-commerce y simplemente en la manera en que accedemos a nuestros ingresos, todos se ha vuelto digital, esto, en combinación con las malas practicas de las personas en términos de seguridad, ha resultado en un aumento considerable en casos de fraude, bien lo exponen Pencarelli (2019) [3] en su publicación, observando el efecto de estos cambios sobre la industria del turismo, una que es bastante importante en Costa Rica.

En la batalla contra el fraude, es importante aclarar exactamente a que nos referimos cuando hablamos de detección y prevención, Baesens [2] propone las siguientes definiciones:

- **Detección de fraude:** se refiere a la habilidad de reconocer fraude, ya sea crediticio o de otro tipo.
- **Prevención de fraude:** se refiere a las medidas o acciones que se pueden tomar con el objetivo de eliminar o reducir la posibilidad de ser víctima de fraude.

Es importante notar la diferencia entre los conceptos, aunque ambos tienen el mismo objetivo de combatir el fraude, la prevención se desarrolla previa al fraude mientras que la detección se hace cuando ya se ha cometido el delito, pero ambas son fundamentales en la mitigación de esta problemática.

Continuando con el tema de detección y prevención, Baesens [2] hace una exploración del perfil del estafador y concluye que, en la mayoría de los casos, el estafador toma las medidas necesarias para esconder su verdadera identidad, es cuidadoso, organizado y posee la habilidad de pasar desapercibido, además de tener la habilidad de adaptarse a la situación que se le presente, lo cuál dificulta mucho la detección de sus actividades delictivas. Sin duda, la capacidad de adaptación del estafador es uno de los principales desafíos al momento de plantear un método de detección y prevención.

Considerando lo anterior, se puede decir que es importante tomar en cuenta todos los métodos y herramientas disponibles para contrarrestar el fraude crediticio, lo cual ha motivado, desde el inicio, a realizar una exploración de diversos métodos de detección y prevención de fraude, para determinar las ventajas y limitaciones de cada uno, y así aprovechar todos los recursos disponibles para la lucha contra el fraude.

Para finalizar con esta sección, y continuar con una exploración de los diversos métodos y algoritmos investigados, se debe recalcar el impacto que ha tenido esta problemática en nuestra sociedad; como ejemplo tome lo sucedido entre los años 2021 y 2022 [5] época en la cuál los casos de fraude acumularon números preocupantes alcanzando su máximo durante el mes de marzo del 2022, donde el Organismo de investigación Judicial (OIJ) recibió un total de 722 denuncias por fraude, nótese que las 4886 denuncias de fraude reportadas en la publicación de Semanario Universidad provienen solamente de San José, lo cuál es alarmante.

Considerando todo lo anterior expuesto, y la dirección que nuestra sociedad esta tomando hacia un mundo de transacciones digitales y de métodos de pago digitales, nuestro estudio es fundamental para el desarrollo correcto de nuestro futuro financiero, por lo que se continua con la tarea de explorar los diversos métodos y recursos disponibles para solucionar esta problematica.

2.2. Machine Learning

El aprendizaje automático es una subcategoría de la inteligencia artificial (IA). Su objetivo principal radica en comprender cómo se estructuran los datos y asociarlos a modelos que puedan ser comprendidos y utilizados por humanos. Aunque la inteligencia artificial y el aprendizaje automático suelen ser mencionados juntos, son conceptos distintos. La IA es un concepto más amplio que abarca máquinas de toma de decisiones, aprendizaje de nuevas habilidades y resolución de problemas, mientras que el aprendizaje automático es un conjunto dentro de la IA que capacita a los sistemas inteligentes para aprender de forma autónoma a partir de datos. [4]

Existen diferentes formas en las que una máquina aprende. En algunos casos, los modelos son entrenados con cierta idea en mente, mientras que en otros casos, aprenden por sí mismos. Existen tres tipos principales de aprendizaje automático: Aprendizaje Supervisado, Aprendizaje No Supervisado y Aprendizaje por Reforzamiento [4]. En el presente trabajo nos enfocaremos en el aprendizaje supervisado ya que es el que nos compete.

2.2.1. Aprendizaje supervisado

El aprendizaje supervisado es una técnica diseñada para aprender a partir de ejemplos proporcionados. En este enfoque, el proceso de aprendizaje se asemeja a tener un maestro supervisando el proceso de enseñanza. [4] En el aprendizaje supervisado, los datos se componen de dos partes principales: una variable de entrada y una variable de salida. Cuando decimos que un conjunto de datos está etiquetado, significa que cada instancia de datos de entrada tiene una correspondiente salida conocida o esperada[4]. Por ejemplo, si estamos entrenando un algoritmo para reconocer imágenes de gatos y perros, cada imagen en nuestro conjunto de datos estará asociada con una etiqueta que indica si la imagen representa a un gato o un perro. Estas etiquetas son esenciales porque proporcionan al algoritmo ejemplos claros de lo que se espera que aprenda a reconocer durante el proceso de entrenamiento.

Regresiones: Se utilizan cuando existe una relación entre una (o varias) variable de entrada y una variable de salida. Se emplean cuando el valor de la variable de salida es continuo o real, como en el caso de predecir el precio de una casa, pronosticar el clima, predecir el precio de las acciones, entre otros [4]. El objetivo principal en la regresión es predecir un valor lo más cercano posible al valor real de salida, y luego evaluar la precisión del modelo calculando el valor del error. Cuanto menor sea el error, mayor será la precisión del modelo de regresión.

Clasificación: Es un proceso en el que se agrupan las salidas en diferentes clases basadas en una o más variables de entrada. Se utiliza cuando el valor de la variable de salida es discreto o categórico, es decir, cuando se puede dividir en categorías claras [4]. Por ejemplo, en la clasificación binaria, cómo determinar si un correo electrónico es "spam.º "no spam", o en la clasificación multiclase, como reconocimiento de caracteres escritos a mano donde las clases pueden ir del 0 al 9.

2.2.2. Aprendizaje no supervisado

No se ocupan de datos etiquetados, lo que significa que existen datos de entrada pero no una variable de salida correspondiente. Esto es lo opuesto al aprendizaje automático supervisado. En el aprendizaje no supervisado, los usuarios no necesitan enseñar o supervisar el modelo. No hay una salida correcta ni un supervisor para enseñar.
El algoritmo mismo aprende de los datos de entrada y descubre los patrones e información de los datos para aprender y agrupar los datos según similitudes. En resumen, el aprendizaje no supervisado se centra en la exploración y descubrimiento de la estructura y relaciones dentro de los datos sin la guía de salidas etiquetadas o supervisores [4].
Los problemas donde se utiliza aprendizaje no supervisado se pueden resumir en dos: clustering y asociación.

2.2.3. Aprendizaje de reforzamiento

El último tipo de aprendizaje automático. Se trata de un aprendizaje basado en retroalimentación. En el aprendizaje por refuerzo, la máquina aprende automáticamente utilizando retroalimentación sin datos etiquetados. Aquí, el modelo aprende por sí mismo a partir de su experiencia [4].
En el aprendizaje por refuerzo, la maquina utiliza el proceso de ensayo y error. Si se realiza un paso exitoso, recibe una recompensa; de lo contrario, por cada error, recibe una penalización. Su objetivo es maximizar la recompensa total[4].

Referencias

[1] Afriyie J., Tawiah K., Pels W., Addai-Hene S., Dwamena H., Odame E., Ayeh S. y Eshun J. *Decision Analytics Journal*, vol 6, *A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions*, Elsevier, 2023.

[2] Baesens B., Van Vlasselaer V. y Verbeke W. *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*, Wiley, 2015.

[3] Pencarelli T. *The digital revolution in the travel and tourism industry*, Springer Nature, 2019

[4] Hiran, K. K., Jain, R. K., Lakhwani, K., and Doshi, R. *Machine Learning: Master Supervised and Unsupervised Learning Algorithms with Real Examples*, 1st ed., BPB Publications, 2021.

[5] Zeledon N., *OIJ recibio 4886 denuncias de fraude a cuentas de bancos entre 2021 y 2022*, Semanario Universidad, 2022