CAN YOU DETECT FRAUD FROM CUSTOMER TRANSACTIONS?

PRESENTADO POR:

AURA LUZ MORENO DÍAZ,

CC 43758500, INGENIERÍA INDUSTRIAL

EVELYN ZHARICK SAEZ GALLEGO,

CC 1006776490, INGENIERÍA AMBIENTAL

PRESENTADO A:

RAÚL RAMOS POLLAN

UNIVERSIDAD DE ANTIOQUIA

FACULTAD DE INGENIERIA

2023

PREPROCESAMIENTO DEL DATASET

La mayor parte del tiempo fue invertido en conocer como traer los datos desde Kaggle. Se intentó inicialmente cargar los datos desde google drive pero no era funcional. Luego de leer toda la documentación disponible, pudimos crear la API KEY y traer los datos directamente desde la competencia de Kaggle.

Teníamos 5 tablas:

sample_submission

test_identity

test_transaction

train_identity

train_transaction

De estos, teniamos que elegir con cual trabajaríamos, sin embargo desde la competencia nos indicaban que ambas tablas estaban relacionadas por la clave primaria del código de la transacción, por lo que sabemos desde ya que para el desarrollo final de este trabajo debemos incluir a ambas: Identity and Transactions. ANALISIS DE LOS DATOS

TABLA IDENTITY

Las variables en esta tabla son información de identidad:

información de conexión de red (IP, ISP, Proxy, etc.) y firma digital (UA/ navegador/OS/versión, etc.) asociada con las transacciones.

Son recopilados por el sistema de protección contra fraudes de Vesta y los socios de seguridad digital.

(Los nombres de los campos están enmascarados y no se proporcionará el diccionario por pares para la protección de la privacidad y el acuerdo del contrato)

- TransactionID
- id_12 - id_38
- DeviceType
- DeviceInfo

TABLA TRANSACTIONS:

- TransactionDT: timedelta de una fecha y hora de referencia determinada (no una marca de tiempo real). timedelta de una fecha y hora de referencia dada (no una marca de tiempo real). El primer valor de TransactionDT es 86400, que corresponde a la cantidad de segundos en un día (60 * 60 * 24 = 86400), así que creo que la unidad es segundos. Usando esto, sabemos que los datos abarcan 6 meses, ya que el valor máximo es 15811131, que correspondería al día 183”
- TransactionAMT: monto del pago de la transacción en USD
- ProductCD: código de producto, el producto para cada transacción
- card1 - card6: información de la tarjeta de pago, como tipo de tarjeta, categoría de tarjeta, banco emisor, país, etc.
- dirección: dirección addr1 como región de facturación, addr2 como país de facturación
- distancia: distancias entre (no limitadas) la dirección de facturación, la dirección postal, el código postal, la dirección IP, el área telefónica, etc
- P_ y (R__) emaildomain: dominio de correo electrónico del comprador y del destinatario
- C1-C14: conteo, como cuántas direcciones se encuentran asociadas con la tarjeta de pago, etc. El significado real está enmascarado.
- D1-D15: timedelta, como días entre transacciones anteriores, etc.
- M1-M9: coincidencia, como nombres en la tarjeta y dirección, etc.
- Vxxx: características completas diseñadas por Vesta, que incluyen clasificación, conteo y otras relaciones de entidad.

Características categóricas:

ProductCD

card1 - card6

addr1, addr2

P_emaildomain

R_emaildomain

M1 - M9

La tabla más grande corresponde a la de transacciones y es la que tiene información más relevante, por ejemplo, el monto de la transacción la cual podríamos usar para saber el monto total de transacciones que son fraudulentas, cruzándola con la tabla identidad, podríamos conocer desde que navegador se realizan, o cual franquicia es la más vulnerada (Amex, Visa, Mastercard, etc) por monto o por cantidad de repeticiones.

También podríamos determinar si los fraudes se realizaron más desde celulares o desde computadores y desde qué sistema operativo se realizaron.

Cuáles son los usuarios más vulnerados según el correo electrónico que usen, por ejemplo gmail, outlook o correos con dominios privados.

PROCESAMIENTO DE DATOS

Se realiza un preprocesamiento de datos identificando las columnas de ambas tablas. Para esto, se determinan cuales son susceptibles para nuestras métricas.

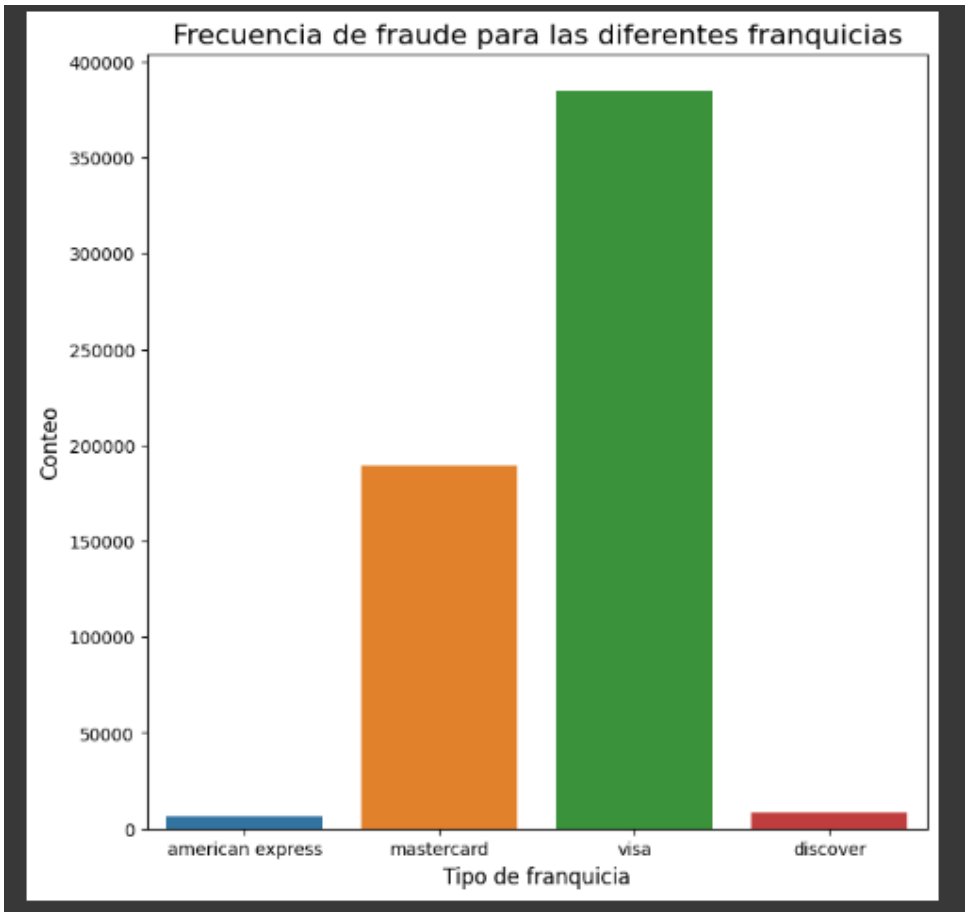
Luego se unen las dos tablas para dejar solo un Dataframe llamado df

AHORA CONCATENAMOS AMBAS TABLAS CON DATOS LIMPIOS

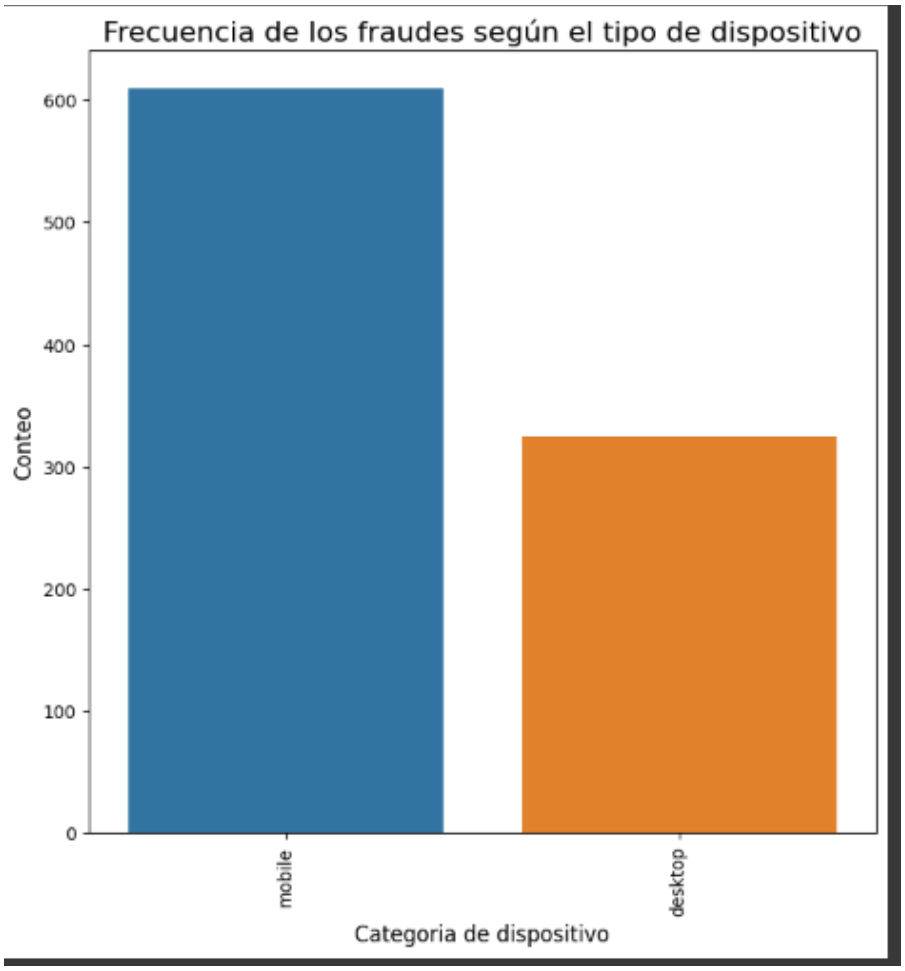
```
[30]  1 #Concatenamos los datos de dfi sin NAN con dft
      2 df = dft.merge(dfi_sinNaN,on = 'TransactionID',how = 'left')
```

ANALISIS DE LOS DATOS

Se realizan algunas aproximaciones para enteder un poco más los datos:



Por ejemplo desde que dispostivo (movil o escritorio) se realizan más fraudes:



METRICAS DE EVALUACIÒN

Como métricas de estudio para la entrega final usaremos accuracy para medir la exactitud del modelo (% de casos en que el modelo ha acertado) y f1_score para combinar la precisión y la exhaustividad en un solo valor se calcula la medida armónica.

Tendremos en cuenta la variable isFraud para saber si una transacción esta marcada como fraudulenta o no, bajo que franquicia y se evaluarán otras condiciones.

DIFICULTADES

Hemos encontrado que por ser un dataframe de datos bancarios, se vuelve información MUY sensible, haciendo que Vesta no comparta muchos de los datos que ellos usan para detectar fraude, limitando el dataset a solo algunos datos que permitan sacar conclusiones.

BIBLIOGRAFIA


UNIVERSIDAD
DE ANTIOQUIA
1803