DETECCIÓN DE SUCESOS RAROS CON MACHINE LEARNING

AUTOR
Ander Carreño López

DIRECTOR
Alfonso Mateos Caballero

Escuela Técnica Superior de Ingenieros Informáticos
Universidad Politécnica de Madrid

13/07/2017

Ander Carreño López: *Detección de Sucesos Raros con Machine Learning*, 13/07/2017.

Tesis Fin de Máster presentada dentro del Máster Universitario en Inteligencia Artificialen la Escuela Técnica Superior de Ingenieros Informáticos (UPM).

A mi familia y amigos.

RESUMEN

En los últimos años el análisis de fraude ha sido tema de interés entre los investigadores así como entre las administraciones públicas y empresas. El fraude fiscal, en concreto, la evasión del Impuesto sobre el Valor Añadido (IVA), hace que la Agencia Estatal de Administración Tributaria (AEAT) pierda millones de euros anualmente. Es por ello que el Departamento de Informática Tributaria (DIT) trabaja utilizando algoritmos sobre grafos así como técnicas de aprendizaje automático para intentar descubrir a aquellas personas, empresas o grupos que realizan actividades ilegales con el fin de defraudar. Afortunadamente, la relación entre la cantidad de entidades que defraudan y las que no, es muy baja. Por ello, en esta Tesis Fin de Máster se avanza un paso más en esta búsqueda introduciendo técnicas de detección de sucesos raros y *one-class classification* sobre las declaraciones de la renta reales recogidas cada año por la AEAT.

ABSTRACT

In the last years, the analysis of fraud has been a subject of interest among researchers, as well as between public administrations and business. The fiscal fraud, specifically the evasion of TAX-es, makes the Spanish Tribute Administration Agency (AEAT) loses millions of euros annually. For this reason, the Tribute Computer Science Department works over Machine Learning algorithms and Graph Theory in order to discover people, companies or groups whose carry out illegal activities with the purpose of defraud. Fortunately, the relationship between the amount of defrauding entities is much lower than those whose are still legal. For that reason, in this thesis I step forward using novel techniques such as anomaly detection, one-class classification and balance of clases using the TAX declarations supplied by the AEAT.

AGRADECIMIENTOS

En primer lugar agradecer al doctor Alfonso Mateos por su excelente colaboración y dedicación. Así mismo, el apoyo recibido por la Agencia Tributaria, en concreto la proporcionada por Ignacio González y Eloy Vicente ha sido de gran ayuda.

También me gustaría agradecer encarecidamente el apoyo de Nerea Martín durante los buenos y malos momentos de este proyecto.

Agradecer a mi hermano Asier por las recomendaciones y por el apoyo durante todo el trabajo. Así mismo, agradecer a mi padre Javier, a mi tío Fernando y mis abuelas Mª Luisa y Dolores por la ilusión y emoción que me han transmitido.

Por último agradecer a la Escuela Técnica Superior de Ingenieros Informáticospor la posibilidad de realizar este proyecto, a la Agencia Tributaria, al Departamento de Informática Tributaria y a la Organización Nacional de Investigación contra el Fraude.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Parte I

Capítulos

1 INTRODUCCIÓN

En este capítulo se introduce la tesis fin de máster realizada por Ander Carreño López titulada *"Detección de Sucesos Raros con Machine Learning"*.

1.1 PROBLEMA ABORDADO

El objetivo principal del proyecto es encontrar tramas que defrauden al fisco, concretamente, aquellas que defraudan al declarar el Impuesto sobre el Valor Añadido (IVA). En concreto, se centra en detectar a aquellas entidades denominadas *truchas*.

Afortunadamente, los casos en los que una entidad es fraudulenta son muy inferiores a los casos que cumplen con la actividad legal. Por ello, se habla de sucesos raros (*rare events*).

Cabe destacar que este proyecto se basa en dos módulos principales, en una primera fase, el programa detectará mediante técnicas de minería de datos y aprendizaje automático la empresa potencialmente fraudulenta. A continuación, mediante teoría de grafos, se descubrirá la trama completa. Es importante decir que en este documento únicamente se tratará la primera fase.

El proyecto se lleva a cabo utilizando el lenguaje de programación *Python* y la librería esencial *scikit-learn*. Para ello, se tienen los datos proporcionados por la Agencia Estatal de Administración Tributaria (AEAT).

1.2 MOTIVACIÓN

El aprendizaje automático es uno de los campos de la Inteligencia Artificial con mayor actividad científica en los últimos años. Es por ello que la utilización de este tipo de técnicas sobre casos reales, como es el fraude

fiscal, hace que este sea un proyecto muy ambicioso y con grandes expectativas.

El fraude hace que de media, las entidades pierdan un 5 % de beneficio anualmente (Baesens, Veronique Van Vlasselaer y Verbeke, 2015). Es por ello que hacer hincapié en la detección es una tarea muy importante al igual que compleja.

Cabe destacar que gracias a los datos proporcionados por la AEAT, este proyecto se realiza sobre situaciones reales, partiendo de declaraciones fiscales entre los años 2010 y 2015.

1.3 PROPÓSITO

El propósito de este proyecto consiste en utilizar técnicas noveles en el estado del arte para detectar el fraude fiscal. Además, cabe desatacar que estas técnicas no han sido aplicadas sobre este campo en la AEAT por lo que supone una aportación novedosa. Para ello, se parte de técnicas de aprendizaje supervisado, no-supervisado y semi-supervisado para establecer un punto de partida. A continuación, se hace uso de técnicas relacionadas con el campo de detección de anomalías, *one-class classification* o *novelty detection*.

Los algoritmos utilizados como punto de partida son los siguientes: *K-Nearest Neighbours* (Silverman y Jones, 1951), *Decision Tree* (Salzberg, 1994), *Random Forest* (Breiman, 2001), *Support Vector Machine* (Vladimir Vapnik, 2013; V. N. Vapnik y Vlamimir Vapnik, 1998; Vladimir Vapnik, 1998), *Naïve Bayes* (Minsky, 1961), *Logistic Regression* (Freedman, 2009).

Para este proyecto además se incluye el paquete externo *Scikit-learn* (Pedregosa et al., 2011) que implementa lo necesario para el aprendizaje de los clasificadores nombrados anteriormente.

Para ilustrar su correcto funcionamiento, se han tenido en cuenta medidas propias del aprendizaje automático, como son *accuracy*, *False Possitive Rate (FPR)*, *True Possitive Rate (TPR)*, *F-Measure*, *Precision* y el área bajo la curva ROC; además de la matriz de confusión.

1.4 RAZONES DE LA ELECCIÓN DEL TFM

La elección de este proyecto ha sido motivada por una serie de razones que se describen a continuación.

- Estrecha relación con los proyectos personales. Dado que me gustaría continuar mi formación académica en el ámbito de la inteligencia artificial, creo que es conveniente introducirme en esta materia. Además, en vistas de que me gustaría empezar el doctorado el año que viene sobre las técnicas de detección de anomalías, este proyecto me parece una magnífica oportunidad.

- Las herramientas y los lenguajes utilizados para el desarrollo de este proyecto son libres y multiplataforma. Una de las premisas más importantes a la hora de desarrollar algo es que sea lo más accesible posible para cualquier tipo de usuario. Por eso, utilizar herramientas que posibiliten esta capacidad ha sido decisivo.

- Trabajar en un proyecto real. Crear programa que sea útil y que se utilice el trabajo realizado en el ámbito académico es una de las causas principales por las que se ha realizado este trabajo. Unir el ámbito académico con el empresarial es algo que se ha valorado positivamente.

- La afinidad con los directores de proyecto ha sido clave para elegir esta tesis fin de máster.

1.5 ESTRUCTURA DEL DOCUMENTO

Este documento está formado por 5 capítulos. El primero de ellos ofrece una introducción sobre el problema a tratar, junto con los objetivos del proyecto. Además, se explica la motivación, el propósito y las razones de la elección de esta tesis. En el Capítulo 2 se dan extensas explicaciones sobre el fraude. Asimismo, se muestran los avances realizados en el estado del arte así como una comparativa de resultados. Por último, el capítulo incluye una descripción detallada sobre el fraude *carrousel*; fraude que es

investigado en este documento. A continuación, en el Capítulo 3, se expone la explicación detallada de cada uno de los paradigmas de aprendizaje automático que tienen relación con el proyecto tratando de dejar claro el enfoque de las técnicas utilizadas. Después, en el Capítulo 4 se describen los algoritmos que se han utilizado en esta tesis de manera formal. Posteriormente en el Capítulo 5 se exponen los resultados obtenidos por los algoritmos y una discusión e interpretación sobre los mismos. Para concluir, en el Capítulo 6 se exponen tanto las conclusiones como el trabajo futuro junto a una reflexión personal.

2 EL FRAUDE

En este capítulo se explican las principales características del fraude, además, se hace especial hincapié en el fraude en el Impuesto sobre el Valor Añadido (IVA).

2.1 EL FRAUDE Y SUS TIPOS

Una de las premisas fundamentales para combatir el fraude es conocer y definir bien el objetivo. Para esto, la Real Academia de la Lengua Española (RAE) define el fraude como:

> Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

No obstante, esta definición no alberga todas las acepciones que comúnmente se conocen como acto fraudulento. Por ello, el *Oxford Dictionary* define el fraude con la siguiente expresión:

> *Wrongful or criminal deception intended to result in financial or personal gain.*

En esta ocasión, la definición incluye el término financiero el cual se acerca al tópico de este proyecto. Sin embargo, una de las mejores definiciones la propuso (Véronique Van Vlasselaer et al., 2015) y es la que se muestra a continuación:

> *Fraud is an uncommon, well-considered, imperceptibly concealed, time-evolving and often carefully organized crime which appears in many types and forms.*

Esta definición resalta seis características que son necesarias para crear un sistema de reconocimiento del fraude. La primera de las características a resaltar es que el fraude es **poco común** o raro, por esto, en este proyecto se utilizan técnicas de aprendizaje automático en búsqueda de sucesos raros. Esta característica está muy relacionada con que el fraude está **imperceptiblemente oculto**. Esto se debe a que es una gran minoría. Además, otra característica como que está **bien considerada** y planeada hace que la tarea se vuelva más difícil. Por otro lado, las personas que realizan el acto de defraudar, es decir, los defraudadores, acostumbran a refinar sus métodos de forma que sigan sin ser detectados a medida que las técnicas de detección avanzan, es por ello que estas **evolucionan con el tiempo**. Otra de las características es que el fraude está **cuidadosamente organizado**, significando que los defraudadores a menudo no defraudan de manera solitaria, es decir, suelen ser un conjunto de individuos los que realizan el fraude y no solo una persona. Por último, la última idea que describe Van Vlasselaer es que el fraude puede darse en **diferentes tipos y formas**. Por ello, en las Tablas 1 y 2 se muestran los diferentes tipos de fraudes que existen según (Baesens, Veronique Van Vlasselaer y Verbeke, 2015). Además, en la Figura 1 se puede ver el resumen de áreas sobre las que afecta el fraude.

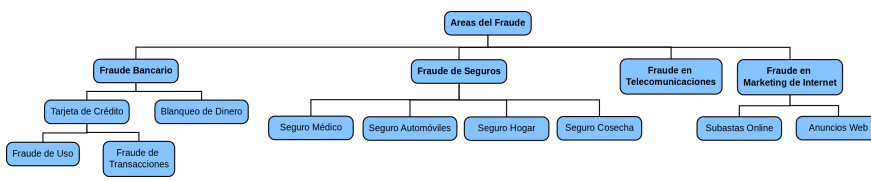

Figura 1: Esquema de las áreas en las que actúa el fraude.

Tabla 1: Tipos de fraude.

Fraude de tarjetas de crédito	En este tipo de fraude existe un uso no autorizado de un tercero sobre la tarjeta de crédito personal de otro individuo. Los subtipos de este fraude son: la falsificación de tarjetas, el uso de tarjetas de crédito perdidas o robadas o el uso de tarjetas obtenidas ilegalmente a través del correo.
Defraudar al seguro	Este tipo de fraude hace referencia a la actividad fraudulenta por parte tanto del comprador como del vendedor de un seguro. Por parte del vendedor, estos fraudes se deben a la venta de pólizas a entidades ficticias, no aplicar las ventajas establecidas al cliente o la disolución o revocación de pólizas para poder obtener las comisiones de nuevo. El tipo de fraude referente al comprador incluye la petición de un valor mucho mayor al valor de los bienes que cubre el seguro, falsificación de historiales médicos, fingir el secuestro o el asesinato, o fingir un daño como puede ser del coche o la vivienda.
Corrupción	La corrupción es el uso indebido de poderes confiados, bien sea en casos de herencia, educación, matrimonio, elecciones, u otros, para beneficio privado o personal.
Falsificación	Este fraude se define como el intento de incorporar una falsificación como un producto genuino. La falsificación comúnmente se refiere a objetos de alto valor, tarjetas de crédito, tarjetas de identidad o al dinero físico etc.
Fraude en la garantía de un producto	La garantía de un producto es una protección que el vendedor o el creador dan sobre el funcionamiento y la condición del item que están vendiendo. Esta protección hace alusión al posible cambio, devolución o reparación del mismo, principalmente cuando el objeto no se encuentra en las condiciones esperadas. Cuando se hace de forma intencionada algún daño al producto para exigir esta garantía al vendedor o a la marca, se considera fraude.

Tabla 2: Tipos de fraude (continuación).

Fraude sanitario	Este fraude hace alusión a la salud. El individuo finge tener un malestar o un problema de salud para exigir al seguro un beneficio. Estos beneficios pueden ser: la obtención de pastillas o recetas para después venderlas en el mercado negro, beneficiar a un tercero que debiera practicar al paciente un tratamiento por el malestar que sufre, entre otros.
Fraude en las telecomunicaciones	Este tipo se basa en utilizar servicios de telecomunicaciones para actividades fraudulentas. Un tipo de fraude llamativo es el de duplicar el número de telefono de una víctima para hacer uso del mismo, suplantando este número.
Lavado de dinero	Este puede que sea uno de los más conocidos. Es el proceso de introducir los beneficios obtenidos por actividades ilegales y hacer que parezcan legales. Esto hace que los criminales puedan transformar sus ganancias en fondos legítimos. Es un problema mundial que se estima que supera los 300 mil millones de dólares en todo el mundo.
Fraude del click	Es el acto que ocurre cuando el beneficiaro por cada click en un anuncio hace click repetidas veces para auto-incrementar sus ganancias. Esta actividad puede hacerla el mismo beneficiario del anuncio, o un tercero, así como máquinas preparadas para esta actividad que lo hacen repetidas veces.
Robo de identidad	Es el crimen de obtener la información personal o financiera de otra persona con el fin de suplantar el nombre o la identidad de la misma con el propósito de hacer transacciones o compras, entre otros. En esta categoría también se contemplan los robos de bases de datos con información personal de los usuarios, por ejemplo, de una página web.
Evasión de impuestos	La evasión de impuestos es una actividad ilegal que supone no pagar los impuestos que se deben. En el ámbito empresarial, la evasión fiscal ocurre tanto con impuestos sobre compras y ventas como en el pago de los salarios de los empleados, así como los impuestos regulados por el estado, comunidad autónoma y provincia.
Plagio	El plagio está definido como el robo o paso de ideas o palabras como si fueran de uno mismo, sin hacer referencia al autor de las mismas.

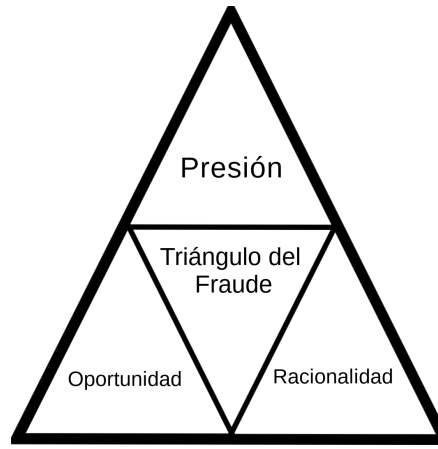

Figura 2: Triángulo del fraude. Factores por los que se da el fraude.

En el fondo, las actividades fraudulentas tienen intención de beneficiar al que las realiza. Las causas o el móvil que hace que una persona llegue a realizar estas actividades se puede ver en la Figura 2. Como se puede observar, este tipo de actividades se apoya en 3 características fundamentales.

- **Presión.** El individuo dispuesto a hacer fraude lo realiza normalmente porque se siente presionado bien sea por causas sociales, financieras o de cualquier naturaleza.
- **Oportunidad.** En ocasiones no es posible defraudar si no se tiene la oportunidad. Por esto, tener acceso a recursos y servicios que posibiliten este tipo de actos es fundamental.
- **Racionalidad.** Es una situación en la cual los autores de este tipo de actividades piensan que hacen lo correcto. Es decir, los defraudadores creen que está bien el acto delictivo que están haciendo y que aprovecharse de, por ejemplo, vacíos legales con el fin de obtener beneficio es lo correcto.

Para poder ver el alcance de este problema, (Abdallah, Maarof y Zainal, 2016) expone la cantidad de dinero que se ha perdido con actividades

fraudulentas. El estudio que se muestra en la Tabla 3 fue redactado por *Internet Crime Complaint Centre* (IC3). Esta organización es la encargada de investigar y detectar el crimen que se realiza a través de Internet.

Tabla 3: Estudio de pérdidas a causa del fraude por IC3.

Año	Quejas recibidas	Pérdidas en Dolares
2011	314,246	485253871 Millones
2012	289874	581441110 Millones
2013	262813	781841611 Millones
2014	269422	800492073 Millones

2.2 MEDIDAS CONTRA EL FRAUDE

Dado que es importante hacer frente al avance de este tipo de actividades, han existido diferentes técnicas para afrontar el problema. Por ello, en esta sección se exponen las diferentes aproximaciones del estado del arte.

En cuanto a qué se puede hacer en esta situación, hay varias posibilidades. Una de ellas es la prevención contra el fraude, la cual intenta que no lleguen a ocurrir estos sucesos. Sin embargo, existe otra vertiente que se caracteriza por detectar los casos de fraude una vez ocurridos conocida como detección del fraude.

Como se puede ver en la Tabla 4 se han realizado estudios desde el año 2002 y todavía hoy sigue siendo un tema de gran interés en la comunidad científica. Además, las técnicas, a medida que avanza el tiempo, tienden a pertenecer más a la inteligencia artificial, como son las redes de neuronas, el aprendizaje automático o la minería de datos. No obstante, también cabe destacar que los métodos estadísticos siguen presentes en esta tarea y que por tanto, este problema atrae a investigadores de diferentes ramas del conocimiento, como pueden ser economistas, científicos de datos o matemáticos entre otros.

Tabla 4: Resumen de técnicas y aproximaciones de lucha contra el fraude en el estado del arte.

Referencia	Técnica	Área del Fraude
(Bolton y Hand, 2002; Kou et al., 2004; Phua et al., 2010; Allan y Zhan, 2010; Pejic-Bach, 2010)	Sistemas inteligentes: redes neuronales, inteligencia difusa, algoritmos genéticos, programación genética, estrategias evolutivas y optimización por enjambres de partículas.	Telecomunicaciones, seguros, revisión de cuentas, atención médica, transacciones de tarjetas de crédito, comercio online, apuestas y verificación de identidad.
(Behdad et al., 2012)	Técnicas inspiradas en la naturaleza.	Email, spam, phising e intrusión en redes.
(Li et al., 2008; Travailé, 2011; Q. Liu y Vasarhelyi, 2013)	Ténicas de minería de datos sobre series espaciales o temporales.	Seguros médicos.
(Rebahi et al., 2011)	Ténicas basadas en reglas y técnicas de aprendizaje supervisado y no supervisado.	Llamadas sobre IP (VoIP).
(S. Wang, 2010; Richhariya y P. K. Singh, 2012; Ngai et al., 2011; Lookman y Balasubramanian, 2013)	Minería de datos y estadística.	Detección del fraude financiero, seguro de hogar, seguros de motor y seguros médicos.
(Delamaire, Abdou y Pointon, 2009; Chaudhary, J. Yadav y Mallick, 2012; Zareapoor, Seeja y Alam, 2012; A. Singh, Narayan et al., 2012; Tripathi y Pavaskar, 2012; Sethi y Gera, 2014)	Tipos de fraude, aproximaciones de ténicas de fraude, técnicas de detección del fraude y sus tipos; y retos o dificultades.	Fraude de tarjetas de crédito, fraude en las telecomunicaciones, fraude en el seguro médico, fraude en el seguro de automóvil y fraude en apuestas por internet.

Si se observa de forma específica las técnicas que se utilizan sobre los tipos de fraude diferentes, se puede ver que no todas las técnicas comentadas anteriormente son aplicadas a todos los tipos de fraude, esto se debe en mayor medida a las características o las causas por las que se da este suceso. Por ejemplo, en los correos electrónicos, se utilizan técnicas inspiradas en la naturaleza mientras que el problema de los seguros de salud ha sido abordado con técnicas que tienen en cuenta el factor tiempo.

De forma gráfica, en la Figura 3 se pueden ver los avances en el ámbito de la investigación contra el fraude por los distintos investigadores.

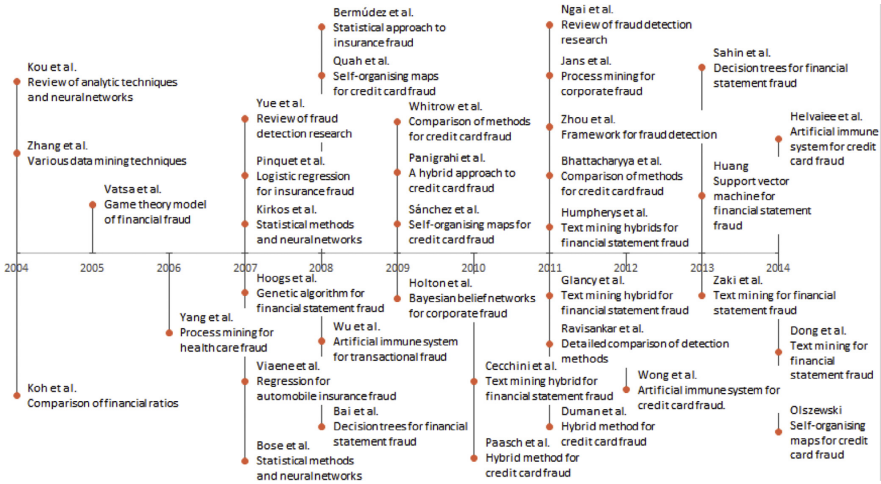

Figura 3: Evolución temporal de la investigación contra el fraude.

Dado que en este proyecto se tienen en cuenta las técnicas de aprendizaje automático, se hace especial hincapié en este tipo de aproximaciones del estado del arte. Por ello, en (Abdallah, Maarof y Zainal, 2016), se exponen las ventajas del uso de este tipo de técnicas. En primer lugar, los patrones del fraude son extraídos de forma automática. Además, se puede especificar un umbral para detectar los sucesos fraudulentos, de manera que es posible investigar casos más o menos sospechosos. Por último, es posible detectar nuevos tipos de fraude.

En cuanto a las técnicas de minería de datos, se pueden obtener seis categorías, siendo: clasificación, *clustering*, regresión, detección de datos atípicos, visualización y predicción.

2.2.1 Detección del fraude basado en anomalías

Esta técnica es utilizada bajo el marco de detección del fraude. El método se basa en obtener patrones de comportamiento para cada individuo. Si alguno de estos comportamientos se desvía de un comportamiento normal, es revisado (Jyothsna, V. R. Prasad y K. M. Prasad, 2011). Una de las grandes ventajas que tiene esta técnica de detección es que se pueden de-

tectar nuevos tipos de fraude que no se han dado con anterioridad. Este tipo de detección, se puede subcategorizar en los siguientes tipos:

- **Detección de anomalías supervisadas.** Bajo este entorno, las instancias están etiquetadas. No obstante, es difícil obtener este tipo de conjuntos de datos. Además, otra dificultad es que en muchas ocasiones, la clasificación binaria (anómalo o no) resulta difícil porque no es posible categorizar de forma tan exacta los individuos.

- **Detección de anomalías no supervisadas.** Este caso es el contrario al descrito anteriormente; las instancias no están clasificadas. Este entorno aunque parezca complicado es el más usual en la realidad ya que describe una situación en la que se supone que existen actividades fraudulentas pero que no se sabe quien las puede estar realizando ni quien no las realiza. Por ello, estas técnicas tratan de agrupar las instancias en diferentes grupos para poder representar comportamientos similares.

- **Detección de anomalías semi-supervisadas.** En este campo, se intenta solucionar el problema expuesto anteriormente. Dado que las instancias en ocasiones no pueden pertenecer de forma exacta a una u otra clase, en este entorno mediante técnicas probabilísticas o haciendo uso de clasificadores específicos, se solventa este problema (Zhu, Y. Wang y Wu, 2011; Akhilomen, 2013).

2.2.2 Retos y problemas de la detección del fraude

La detección de el fraude es una tarea muy complicada dado que se apoya en un dominio muy complejo. Se pueden encontrar sistemas que apenas fallan en la detección de este tipo de comportamiento, que tienen una muy baja tasa de *accuracy* o que ofrecen una gran tasa de falsos positivos. Esto se debe a que el fraude es un fenómeno que esta en constante evolución y por ello, es mutable. En consecuencia, el sistema inteligente de detección del fraude tiene que hacer frente al concepto de mutabilidad del tipo de técnicas que se usan para actividades fraudulentas, este fonómeno también es conocido como asimetría de los datos; el desbalanceo que existe en la mayoría de problemas fraudulentos, la gran cantidad de datos que

existen en estos entornos y la necesidad de crear un sistema de detección en tiempo real.

Para afrontar todos estas dificultades los investigadores han utilizado diferentes soluciones que se exponen a continuación:

- **Asimetría de los datos.** El principal problema que existe es que en el momento de la predicción, puede que la etiqueta no pertenezca a ninguna etiqueta del conjunto de datos de entrenamiento porque el escenario ha mutado. Para solventar este problema, se han utilizado algoritmos que tienen en cuenta este tipo de mutabilidad. De esta forma, se utilizan algoritmos de aprendizaje incremental (Bolton y Hand, 2002).

- **Desbalanceo de los datos.** Este problema subyace de la premisa de *es más común estar bajo la legalidad que hacer actividades fraudulentas.* Por ello, dados a observar un experimento, es más común que la mayoría de los sucesos pertenezcan al marco legal que al fraudulento; lo que incurre en una gran cantidad de datos de clase legal y muy pocos de clase fraudulenta. Para esto, se utilizan algoritmos que modelan el comportamiento como son el *isolation forest* (F. T. Liu, Ting y Zhou, 2008), o comúnmente, se han utilizado algoritmos que sean sensibles al coste intentando eliminar el *overfitting* propio de los datos. Otro punto de vista para lidiar con este conflicto es tratar de eliminar este desbalanceo. Para ello, se utilizan técnicas de remuestreo como pueden ser el *oversampling* o el *undersampling*, siendo la creación de forma sintética instancias de la clase minoritaria o la eliminación o desestimación de las instancias de la clase mayoritária hasta conseguir el ratio deseado, respectivamente.

- **Gran cantidad de datos**. La gran cantidad de datos puede hacer que nuestro sistema no pueda procesar los mismos. Por ello, existen técnicas de reducción tanto de variables como de instancias que pueden ayudar al procesamiento.

- **Detección en tiempo real.** Para que esto sea posible, el tiempo de respuesta del sistema inteligente debe ser muy alta en la parte de predicción, por ello, ciertos algoritmos quedan fuera para este tipo de tareas.

2.2.3 Resultados de técnicas específicas contra el fraude en casos reales

Una vez que se tiene claro cuales han sido los avances en este ámbito, los principales retos y problemas con los que es necesario lidiar y las diferentes técnicas para solventarlos, es importante ver la aplicación de casos concretos y algoritmos específicos. Por ello, en esta sección se exponen los resultados más significativos del estado del arte (West y Bhattacharya, 2016).

Como se puede observar en la Figura 4, se ven los resultados de distintos algoritmos sobre el fraude de tarjetas de crédito y el fraude financiero. Cabe destacar que esta es una figura resumen y que los estudios originales se pueden consultar en las Tablas 29 y 30 situada en el Apéndice A.

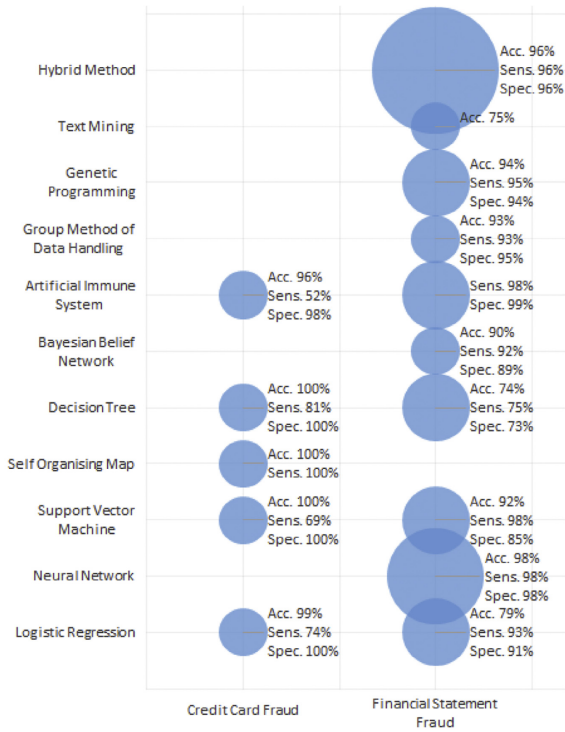

Figura 4: Resultados de diferentes técnicas en estudios del estado del arte.

Un dato destacable es que los algoritmos de aprendizaje supervisado, tales como los árboles de decisión, las redes Bayesianas o las máquinas de vector soporte, consiguen muy buenos resultados. Además, las redes neuronales destacan por ser la que mejores figuras de mérito consigue, no obstante, dado que el razonamiento de clasificación de una red neuronal es difícil de obtener, en muchos ámbitos no es posible incorporar este tipo de modelos. Por último, destacar que cuando se mezclan todo tipo de técnicas, obteniendo métodos híbridos, se consiguen resultados realmente buenos. Esto quiere decir que en la lucha contra el fraude no solo es necesario utilizar unos algoritmos de clasificación sino que el conocimiento del dominio es muy importante. Por ello, técnicas basadas en grafos como en (Fernandez, 2017; Olszewski, 2014) son de especial interés.