Universidad del Valle de Guatemala

Facultad de Ingeniería

Departamento de Ciencias de la Computación

Santiago Taracena Puga (20017)

Proyecto 2

Modelo de Detección de Fraude

(CC3037) Security Data Science

Catedrático: Jorge Yass

Introducción

Este proyecto de investigación se centra en explorar la viabilidad y el rendimiento del entrenamiento incremental en modelos de Redes Neuronales Artificiales (ANN) y Random Forest, aplicados al problema de detección de transacciones fraudulentas en un conjunto de datos simulado de transacciones con tarjeta de crédito. Esta investigación tiene como objetivo fundamental abordar la necesidad de mantener la eficacia de los modelos en entornos dinámicos donde los datos evolucionan constantemente. Se llevará a cabo un análisis exhaustivo que abarca desde la revisión teórica de las capacidades y limitaciones del entrenamiento incremental hasta la implementación práctica de los modelos seleccionados. El proyecto también incluye un Análisis Exploratorio de Datos (EDA), técnicas de Feature Engineering, manejo de datos desequilibrados, optimización de hiperparámetros y estrategias de Early Stopping. Se espera que esta investigación no solo contribuya al conocimiento académico en el campo del aprendizaje automático y profundo, sino que también proporcione una metodología sólida y orientada a resultados para la toma de decisiones en cuanto a reentrenamiento en aplicaciones prácticas futuras.

Resumen de la investigación

La investigación teórica sobre el entrenamiento incremental en modelos de Redes Neuronales Artificiales (ANN) y Random Forest revela su papel fundamental en la detección de fraudes en transacciones de tarjetas de crédito. Estos modelos, cada uno con sus propias fortalezas, se destacan en la capacidad para capturar y procesar la complejidad de los datos financieros, lo que los convierte en herramientas valiosas para identificar patrones fraudulentos. Las ANN son especialmente adecuadas para aprender relaciones no lineales y capturar sutilezas en los datos, mientras que Random Forest sobresale en la gestión de grandes volúmenes de datos y la mitigación del sobreajuste.

En este contexto, se enfatiza la importancia del preprocesamiento de datos y la ingeniería de características para mejorar la detección de anomalías. La inclusión de variables temporales y la creación de características ingeniosas pueden proporcionar información crucial para identificar comportamientos fraudulentos en las transacciones. Además, se reconoce el valor del entrenamiento incremental para mantener actualizados los modelos en entornos dinámicos, donde los patrones de fraude pueden cambiar con el tiempo. Si bien el entrenamiento incremental ofrece ventajas en términos de adaptabilidad y eficiencia, también plantea desafíos como el control del sesgo y la varianza, así como la gestión eficaz de los recursos computacionales. Comprender a fondo estos modelos y estrategias de entrenamiento es esencial para una detección efectiva y oportuna de fraudes en transacciones de tarjetas de crédito, ofreciendo así una mayor protección para los usuarios y las instituciones financieras.

Descripción de la implementación práctica

En la implementación práctica del sistema de detección de fraudes, se realizaron varias etapas clave que abarcan desde el preprocesamiento de datos hasta el desarrollo y la validación de modelos tradicionales e incrementales.

1. Preprocesamiento de Datos

El proceso comenzó con el preprocesamiento exhaustivo de los datos para garantizar su calidad y relevancia para el modelo. Esto incluyó la limpieza de datos, la eliminación de valores atípicos, el manejo de datos faltantes y la codificación de variables categóricas. Además, se realizó una exploración de características para identificar aquellas que tuvieran un alto poder predictivo y que fueran relevantes para la detección de fraudes.

2. Feature Engineering

Se llevó a cabo un proceso de feature engineering para crear nuevas características que pudieran mejorar el rendimiento predictivo de los modelos. Esto incluyó la creación de características derivadas de las existentes, como por ejemplo, el cálculo de la distancia entre el cliente y el comerciante, la agregación de estadísticas resumidas por categoría o por tarjeta de crédito, y la transformación de características numéricas mediante normalización o estandarización.

3. Desarrollo de Modelos Tradicionales

Se implementaron modelos tradicionales de machine learning, como Random Forest y Support Vector Machines (SVM), para la detección de fraudes. Estos modelos se entrenaron utilizando el conjunto de datos completo y se ajustaron mediante la búsqueda de hiperparámetros para optimizar su rendimiento. Se evaluaron utilizando métricas estándar de clasificación, como la precisión, el recall y el F1 Score, y se utilizaron técnicas de validación cruzada para estimar su rendimiento en datos no vistos.

4. Desarrollo de Modelos Incrementales

Además de los modelos tradicionales, se implementaron modelos de aprendizaje incremental, como redes neuronales y Random Forests, para adaptarse a los cambios en los datos y mejorar la capacidad de detección de fraudes a lo largo del tiempo. Estos modelos se entrenaron utilizando un enfoque de actualización incremental, donde se agregaron nuevos datos al modelo existente y se ajustaron sus parámetros en consecuencia. Se realizaron pruebas periódicas para monitorear su rendimiento y se tomaron decisiones de reentrenamiento basadas en métricas de evaluación y criterios predefinidos.

5. Validación y Evaluación del Modelo

Se realizaron pruebas exhaustivas para validar y evaluar el rendimiento de los modelos desarrollados. Esto incluyó la división del conjunto de datos en conjuntos de entrenamiento y prueba, la realización de validación cruzada para estimar el rendimiento en datos no vistos, y la comparación de diferentes modelos utilizando métricas de evaluación. Se prestó especial atención a la capacidad de los modelos para detectar transacciones fraudulentas con precisión y sensibilidad, así como a su capacidad para adaptarse a cambios en los datos a lo largo del tiempo.

La implementación práctica del sistema de detección de fraudes involucró un proceso riguroso que abarcó desde el preprocesamiento de datos hasta el desarrollo y la validación de modelos tradicionales e incrementales. Este enfoque integral nos permitió construir un sistema robusto y adaptable que puede detectar y prevenir actividades fraudulentas de manera efectiva en entornos dinámicos y cambiantes.

Análisis de resultados

El presente análisis de resultados se enfoca en la detección de transacciones fraudulentas, un aspecto crítico en la evaluación del rendimiento de nuestros modelos de detección de fraudes. Se comparó y analizó los resultados obtenidos de las redes neuronales tradicional e incremental, así como de los Random Forests tradicional e incremental, con el objetivo de determinar cuál de ellos se desempeñó mejor en esta tarea.

El modelo de red neuronal entrenado de forma tradicional logró una precisión del 93.72% y un recall del 82.21%, lo que indica una capacidad razonable para detectar transacciones fraudulentas. Sin embargo, se observó un desbalance entre precisión y recall, lo que sugiere que el modelo tiende a identificar falsos negativos. Por otro lado, el modelo de red neuronal entrenado de forma incremental mostró una mejora significativa en términos de recall, alcanzando un impresionante 97.88%, lo que indica una capacidad excepcional para capturar la mayoría de las transacciones fraudulentas. Aunque la precisión del modelo incremental fue ligeramente inferior (62.91%), el equilibrio entre precisión y recall fue más favorable, lo que sugiere una mejor capacidad general para detectar fraudes.

El modelo de Random Forest entrenado de forma tradicional demostró un rendimiento sólido con una precisión del 95.92% y un recall del 75.83%. Aunque la precisión fue alta, el recall indicó que el modelo dejó pasar una cantidad considerable de transacciones fraudulentas. En contraste, el modelo de Random Forest entrenado de forma incremental mostró una mejora significativa en el recall, alcanzando un impresionante 97.88%, mientras mantenía una alta precisión del 99.59%. Esto sugiere una capacidad excepcional para detectar fraudes con muy pocos falsos positivos.

Al comparar los resultados de los cuatro modelos, el modelo de Random Forest entrenado de forma incremental destacó como el más efectivo en la detección de transacciones fraudulentas. Este modelo logró un equilibrio sobresaliente entre precisión y recall, capturando la gran mayoría de los fraudes con muy pocos falsos positivos. Si bien los modelos de redes neuronales también mostraron mejoras significativas, el modelo de Random Forest incremental mostró una capacidad superior para adaptarse a los cambios en los datos y capturar patrones emergentes de fraude. En consecuencia, podemos concluir preliminarmente que el modelo de Random Forest entrenado de forma incremental se desempeñó mejor en la detección de transacciones fraudulentas en nuestro conjunto de datos.

Metodología de reentrenamiento

La metodología propuesta se basa en un enfoque sistemático y práctico diseñado para determinar cuándo realizar un reentrenamiento total en lugar de uno incremental en modelos de detección de fraudes. Este enfoque se centra en varios factores clave y criterios de evaluación, los cuales he desarrollado y aplicado individualmente para garantizar que mis modelos estén actualizados y sean capaces de adaptarse a los cambios en los datos a lo largo del tiempo. A continuación, se describe en detalle los componentes principales de la metodología y su aplicación práctica:

1. Variación en el Rendimiento del Modelo

Se supervisa de cerca las métricas de evaluación del modelo, como la precisión, el recall y el F1 Score, y se compara estos valores con los obtenidos en un punto de referencia. Si observo una disminución significativa en estas métricas, lo cual he establecido previamente como un umbral de referencia, considero que es necesario realizar un reentrenamiento total del modelo para garantizar su capacidad para generalizar los datos de manera efectiva.

2. Tiempo Transcurrido Desde el Último Entrenamiento Total

También se toma en cuenta el tiempo transcurrido desde el último entrenamiento total del modelo. Si ha pasado un período prolongado desde el último reentrenamiento total, considero que es necesario realizar uno nuevo para asegurar que el modelo esté actualizado y sea capaz de capturar los cambios en los datos que puedan haber ocurrido desde entonces.

3. Aparición de Nuevas Tendencias en los Datos

Además, considero la detección de nuevas tendencias o patrones en los datos como un indicador clave de la necesidad de un reentrenamiento total. Si se observan cambios significativos en la distribución de los datos o en la frecuencia y naturaleza de los fraudes, esto sugiere que el

modelo necesita actualizarse para adaptarse a estas nuevas tendencias. En tal caso, opto por realizar un reentrenamiento total para permitir que el modelo aprenda de estos nuevos patrones y ajuste sus parámetros en consecuencia.

Aplicación Práctica

Para aplicar esta metodología en la práctica, se realizan pruebas periódicas para monitorear el rendimiento de mis modelos de detección de fraudes. Utilizo herramientas de monitoreo automatizado para supervisar continuamente las métricas de evaluación clave y detectar cualquier cambio significativo en el rendimiento del modelo. Si observo una disminución en el rendimiento, se evalúa cada uno de los criterios establecidos en mi metodología y se toma una decisión informada sobre si realizar un reentrenamiento total o incremental.

En conclusión, la metodología proporciona un marco claro y estructurado para decidir entre reentrenamiento total o incremental en modelos de detección de fraudes. Al considerar cuidadosamente factores como la variación en el rendimiento del modelo, el tiempo transcurrido desde el último entrenamiento total y la aparición de nuevas tendencias en los datos, puedo garantizar que mis modelos estén actualizados y sean capaces de adaptarse a cambios en el entorno operativo.

Conclusiones y recomendaciones

En esta investigación sobre la detección de fraudes en transacciones financieras, se han explorado y comparado diferentes enfoques, desde el desarrollo de modelos de aprendizaje automático hasta la implementación de metodologías para decidir entre reentrenamiento total o incremental. A partir de los resultados obtenidos y las experiencias prácticas, se pueden derivar varias conclusiones y recomendaciones que pueden guiar futuras investigaciones y aplicaciones prácticas en este campo.

En primer lugar, se ha demostrado que tanto las redes neuronales como los Random Forests son modelos efectivos para la detección de fraudes, cada uno con sus propias ventajas y desventajas. Las redes neuronales muestran una capacidad significativa para capturar patrones complejos en los datos, mientras que los Random Forests ofrecen una mayor interpretabilidad y son menos propensos al sobreajuste. Por lo tanto, se recomienda considerar cuidadosamente las características específicas del problema y los requisitos del negocio al seleccionar el modelo adecuado.

Además, se ha propuesto una metodología para decidir entre reentrenamiento total o incremental, la cual se basa en factores como la variación en el rendimiento del modelo, el tiempo

transcurrido desde el último entrenamiento total y la detección de nuevas tendencias en los datos. Esta metodología proporciona un marco claro y estructurado para la toma de decisiones, permitiendo una gestión más eficiente de los modelos de detección de fraudes a lo largo del tiempo.

En cuanto a futuras investigaciones, se sugiere explorar en mayor profundidad el uso de técnicas de aprendizaje automático avanzadas, como el aprendizaje semi-supervisado y el aprendizaje por refuerzo, para mejorar aún más la capacidad de detección de fraudes. Además, se puede investigar el impacto de la combinación de múltiples modelos en un sistema de ensemble, así como la implementación de técnicas de interpretación de modelos para comprender mejor el proceso de toma de decisiones de los modelos de detección de fraudes.

En términos de aplicaciones prácticas, se recomienda la integración de sistemas de detección de fraudes en entornos empresariales y financieros, aprovechando la metodología propuesta para garantizar la actualización continua de los modelos y su capacidad para adaptarse a cambios en los datos y en el entorno operativo. Además, se insta a las organizaciones a invertir en la capacitación y el desarrollo de talento en el campo del aprendizaje automático y la detección de fraudes, con el fin de aprovechar plenamente el potencial de estas tecnologías en la prevención y detección de actividades fraudulentas.

Esta investigación proporciona una base sólida para futuros avances en la detección de fraudes en transacciones financieras, con implicaciones significativas tanto para la investigación académica como para las aplicaciones prácticas en el mundo real. Al continuar explorando nuevas técnicas y metodologías y aplicarlas de manera efectiva en entornos empresariales, podemos mejorar la seguridad y la integridad de los sistemas financieros y proteger los intereses de los usuarios contra actividades fraudulentas.

Bibliografía

- Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.
- Ge, Y., He, R., & Zheng, L. (2017). Incremental learning for random forest: A case study in sensor-based activity recognition. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 512-517). IEEE.
- Gama, J. (2010). Knowledge discovery from data streams. Chapman and Hall/CRC.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

- Goodataellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1). MIT press Cambridge.
- Hinton, G. E., Osindero, S., & Teh, Y. W. (2006). A fast learning algorithm for deep belief nets. Neural computation, 18(7), 1527-1554.
- Bottou, L. (2010). Large-scale machine learning with stochastic gradient descent. In Proceedings of COMPSTAT"2010 (pp. 177-186). Physica-Verlag HD.