УДК 004.89

К.В.Мельник, к.т.н.,
С.В.Лавренчук, к.т.н.
Луцький національний технічний університет, Луцьк

ВИЯВЛЕННЯ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТКАМИ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

Шахрайством з кредитними картками оцінюється в десятки мільярдів доларів. Наприклад, згідно звіту 2018 року Європейського центрального банку (ЄЦБ) [1], збитки від шахрайства з картками складає 1,8 мільярда євро в Єдиній європейській платіжній зоні (SEPA).

Структура шахрайства: 79% - це шахрайства за відсутності фізичної картки (CNP) (тобто платежів через Інтернет, поштою чи телефоном), 15% – транзакцій у момент здійснення - термінали продажу (POS), наприклад, особисті платежі в роздрібних магазинах або ресторанах, і 6% від транзакцій в банкоматах.

Загальний рівень шахрайства в карткових платіжках свідчить про важливість постійного моніторингу шахрайства та заходів безпеки з боку наглядачів карткових систем.

Для виявлення моделей шахрайства з кредитними картками необхідно здійснювати аналіз великих обсягів даних транзакцій. В останні роки саме алгоритми машинного навчання дозволяють шукати та виявляти шаблони у великих обсягах даних і підвищують ефективність систем виявлення шахрайства.

При застосуванні алгоритмів машинного навчання необхідно враховувати такі проблеми, як: дисбаланс класів (дані про транзакції містять набагато більше законних, ніж шахрайські транзакції); дрейф концепції: моделі транзакцій і шахрайства змінюються з часом; вимоги майже до реального часу; категоричні ознаки **(**ідентифікатор клієнта, термінал, тип картки); показники ефективності (стандартні показники для систем класифікації, такі як середня помилка неправильної класифікації або AUC ROC, не дуже підходять через проблему дисбалансу класів і складну структуру витрат на виявлення шахрайства); відсутність загальнодоступних наборів даних.

При розробці системи виявлення шахрайства т.б. бінарного класифікатора необхідно пройти два етапи: навчання системи та прогнозування мітки нових транзакцій (справжні чи шахрайські).

Як відомо, існує чотири підходи: контрольоване навчання, неконтрольоване навчання, ансамблеве навчання та глибоке навчання.

Авторами розглянуті методи: логістична регресія, дерева рішень, випадкові ліси, нейронні мережі/глибоке навчання. Розглядалися питання покращення продуктивності. Продуктивність можна розглядати, як точності виявлення шахрайства, або вимоги до обчислень (пам'ять/час виконання). Оскільки необхідно працювати з великими обсягами даних і в режимі реального часу, тому потрібно розглядати компроміси між точністю та вимогами до обчислень.

На рис.1 показані результати моделювання з параметрами за замовчуванням.

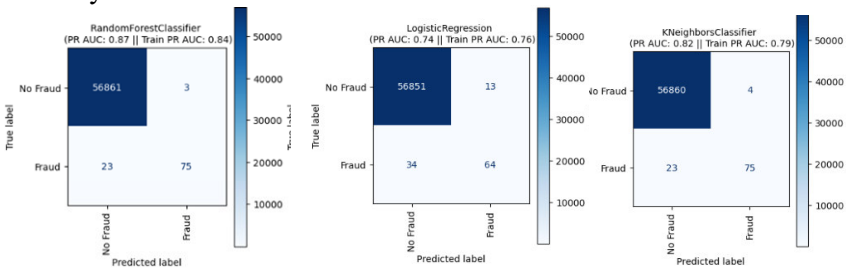

Рис.1.Методи: випадковий ліс, логістична регресія, метод найближчого сусіда.

Показані результати, що отримані за допомогою простих стратегій попередньої обробки та стандартних класифікаторів машинного навчання.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Sixth report on card fraud [Електронний ресурс] – Режим доступу. — URL: http://surl.li/gccpl (дата звернення 04.03.2023)

2. Reproducible Machine Learning for Credit Card Fraud Detection - Practical Handbook– Режим доступу. — URL: http://surl.li/gccqh (дата звернення 04.03.2023)