likely to overcome these obstacles and pave the way for a smarter, more efficient chemical industry.

References:

1. Chen, L., Zhang, S., & Ji, J. (2020). A review on the application of artificial intelligence in heat exchanger design and operation. Energy Procedia, 173, 246-252.
2. Dogan, I., Guo, Y., & Cui, Z. (2019). Artificial intelligence applications in heat exchanger network synthesis and retrofit. Chemical Engineering Research and Design, 144, 96-110.
3. García, S., & Cabeza, L. F. (2021). Artificial intelligence and machine learning for the optimization of heat exchanger networks. Renewable and Sustainable Energy Reviews, 138, 110506.
4. Koupaei, J. A., & Pourfayaz, F. (2021). A comprehensive review on heat exchanger optimization using artificial intelligence. Energy Conversion and Management, 227, 113649.
5. Lee, J. C., Kim, H., & Kim, H. M. (2019). A survey of machine learning applications for the oil and gas industry. Energies, 12(13), 2577.
6. Li, Y., Gao, H., & Wang, F. (2018). A survey of deep neural network architectures and their applications. Neurocomputing, 234, 11-26.
7. Sánchez, C. A., & Martin, E. (2019). Artificial intelligence for improving energy efficiency: A review. Energy and Buildings, 202, 109374.

ОБ ОДНОМ ПОДХОДЕ ОЦЕНКИ ПЛАТЕЖНЫХ ТРАНЗАКЦИЙ НА ПРЕДМЕТ МОШЕННИЧЕСТВА

доц. Х.К. Самаров
Ташкентский университет информационных технологий
husnutdinsamarov@gmail.com

Аннотация: В данной статье предлагается алгоритм предсказания мошеннических транзакций. В алгоритме используется методы анализа, статистики, скоринга и классификации.

Ключевые слова: Мошенничество, транзакция, аккаунт, скоринг, фрод мониторинг, антифрод системы, риск, алгоритм, метод.

В настоящее время увеличивается количество финансовых транзакций, что приводит к росту финансового мошенничества и, как следствие, возникновению потерь в мировой экономике от кибератак. Выявление девиантных транзакций является актуальной темой современных исследований, поскольку для всех участников банковской системы важно минимизировать риски, которые могут возникать из-за наличия уязвимостей при совершении онлайн-операций. Рост финансовых потерь из-за увеличения финансового мошенничества актуализирует значимость применения математических методов для анализа

реальных данных. В статьи предлагается алгоритм предсказания мошеннических операций.

Методы оценки мошенничества используются для выявления и оценки транзакций с наибольшим риском — в отсутствии карты, которые нуждаются в дополнительной проверке. Они могут выявлять схемы мошеннической деятельности и отличать эти схемы от законной транзакционной деятельности.

Для каждой транзакции вычисляется числовое значение (оценка), отражающее вероятность того, что она может быть мошеннической.

В платежных системах, которые функционируют сейчас в нашей стране, чтобы провести транзакцию, достаточно иметь 16-ти значный номер карты, срок действия карты и номер телефона, к которому подключена услуга СМС-информирования. Мошенники регистрируются в платежной системе или авторизуются, если пользователь ранее пользовался этой системой, в процессе входа с нового устройства, на номер телефона отправляется СМС с кодом для подтверждения авторизации/регистрации.

Затем мошенники добавляют в аккаунт карту и производят несанкционированные транзакции [1,4].

В этом случае предотвратить хищение денежных средств поможет только система фрод-мониторинга, которая по различным параметрам как автоматизированных средств отправки транзакций плательщика (то есть, клиента банка), так и самой транзакции оценивает вероятность (или скоринг) того, что транзакция является мошеннической. Простейшим примером системы фрод-мониторинга может являться простое ограничение на сумму платежа. Если платеж больше определенной величины, то он считается подозрительным на фрод и требует дополнительной проверки (подтверждения) его легальности. Общий механизм работы антифрод-системы, который применяется в большинстве международных платежных систем сейчас, можно свести к следующему:

1. Сервер платежной организации переадресовывает сведения о транзакции в антифрод-систему и ожидает разрешения на проведение платежа.
2. Антифрод-система анализирует сведения, чтобы принять решение о легитимности этой транзакции.
3. Обрабатывается платеж, оценивается его риск, при необходимости инициируется проверка другими сервисами, например, дополнительная аутентификация клиента, после чего решение передается назад.
4. В результате финансовая транзакция оказывается подтвержденной или отклоненной.

В момент совершения финансовой транзакции сканируются браузер,IP-адрес, куки-файлы на предмет подозрительной активности, а также собирается несколько показателей (у каждой антифрод-системы они различные) – начиная от IP-адреса компьютера, версии браузера и заканчивая статистикой платежей и др. Осуществляется проверка на использование виртуальной машины или VPN, анализируется поведение клиента, проверяется информация о платежной системе, используется собственная база мошеннических действий и др.

Во втором шаге общего антифрод-механизма, в котором антифродсистема анализирует транзакцию и выносит решение подтвердить, провести дополнительную проверку или отклонить транзакцию, вышеперечисленные признаки рассматриваются последовательно Фильтрация транзакции по признакам мошенничества последовательно имеет несколько недостатков, главным из них является частое ложное срабатывание и отклонение легитимных транзакций с подозрением на мошенничество [4].

В алгоритме, предлагается присвоение баллов каждому из параметров несанкционированности транзакции — мошенничества. Список этих параметров будет динамическим, то есть администраторы платежной системы могут вводить новые параметры и присваивать им баллы, которые будут добавлены в суммарный балл транзакции при выполнении/невыполнении определенных условий. Каждая транзакция будет иметь суммарный балл (transaction fraud score - TFS), который будет высчитан, смотря на все показатели параметров совершаемой транзакции. Чем выше суммарный балл, тем опаснее считается транзакция. Здесь под опасностью понимается вероятность мошенничеств в данной финансовой операции.

Также, администраторы будут задавать пороговые значения для каждого уровня опасности транзакции (transaction fraud level - TFL), примерный перечень уровней приводится в таблице. Этот перечень тоже будет динамическим, при необходимости можно будет вводить новый уровень опасности с соответствующим пороговым значением.

По каждому признаку будет высчитываться балл — минимальному значению признака будет присваиваться минимальный балл, максимальному значению признака будет присваиваться максимальный балл, в других случаях попаданию в диапазон признака, заданным модераторами системы, балл будет вычисляться методом пропорции. Балл по каждому признаку будет добавляться в итоговый балл.

Transaction fraud pre-score (TFPS) — предварительный балл транзакции, вычисляется в этапе создания транзакции по признакам подмеченными модераторами как pre-score. Это позволяет обеспечивать быстродействие алгоритма на фоне всего цикла транзакции и сокращает время задержки во время подтверждения, которое тратится на расчет суммарного балла.

После расчета суммарного балла транзакции переходит на следующий этап — этап применения решения. Решение применяется на основе уровня опасности транзакции, который был выбран, после расчета и превышения пороговых значений каждого из уровней. Возможные исходы уровней могут быть следующие действия: проведение транзакции, дополнительная проверка с использованием дополнительного подтверждения — 3D-Secure, подтверждение через высланный одноразовый код с помощью SMS/Push уведомления и пр., проведение транзакции с занесением его в список подозрительных, который будет рассмотрен администраторами платежной системы, или же полный отказ в проведении вплоть до блокировки аккаунта/карты пользователя [2,3]. Выполнение алгоритма также можно свести в задачу классификации с применением методов машинного обучения.

Предложенный алгоритм выявления несанкционированных транзакций, который дает балловую оценку каждой проводимой транзакции и определяет уровень опасности по заданным признакам модераторами платежной системы, а также перечни признаков несанкционированных транзакций для расчета суммарного балла транзакций (TFS) и уровней опасности (TFL), который получается по итогу расчета суммарного балла;
Практически все ограничения или лимиты фрод-мониторинговых решений строятся на простых правилах:

- ограничение количества покупок по одной банковской карте или одним пользователем за определенный период времени
- ограничение на максимальную сумму разовой покупки по одной карте или одним пользователем в определенный период времени
- ограничение на количество банковских карт, используемых одним пользователем в определенный период времени
- ограничение на количество пользователей, использующих одну карту
- учёт истории покупок по банковским картам и пользователями (так называемые «черные» или «белые» списки)

Обязательным требованием к реализации таких правил является распознавание пользователя по различным параметрам и алгоритмам. Соответственно, преимущество антифрод сервиса определяется его способностью быстро и с максимальной степенью вероятности распознать мошенника. Ещё одним плюсом фрод-мониторинга является способность оценивать поведение покупателя в процессе проведения платежа. Насколько правдивую информацию указывает о себе человек и насколько совокупность параметров пользователя соответствует стандартным шаблонам поведения добропорядочных покупателей — это дополнительные факторы, которые фрод-мониторинговые сервисы стараются учесть при оценке вероятности мошенничества.

Список литературы:

1. Малолетко, Н. Е. Новые подходы к обеспечению безопасности электронных платежей / Н. Е. Малолетко, Т. И. Воробьева // Актуальные проблемы и перспективы развития экономики: российский и зарубежный опыт. – 2019. – № 5(24). – С. 28-31.
2. Мамин, В. А. Исследование безопасности электронных платежных систем // ИТ Арктика. – 2017. – № 3. – С. 63-76.
3. Растяпин Ю. В., Трофимов Е. А. К вопросу противодействия мошенничеству в сфере дистанционного платежа в условиях цифровизации общественных отношений // Криминологический журнал. – 2021. – №3. – С. 129–132. https://doi.org/10.24412/2687-0185-2021-3-129-132.
4. Шейнов, А. И. Современные способы выявления мошеннических транзакций в сети интернет / А. И. Шейнов, О. Н. Пастухова // Вестник Тульского филиала Фин. университета. – 2019. – № 1-2. – С. 311-313.