УДК 004.738.5

ПОРІВНЯННЯ ТРАДИЦІЙНОЇ МОДЕЛІ ВИЯВЛЕННЯ ШАХРАЙСТВА, З МАШИННИМ НАВЧАННЯМ

Міночкін Д. А., Кошмак А.І.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dmytro.minochkin@gmail.com , koshmak02@gmail.com

COMPARISON OF TRADITIONAL FRAUD DETECTION MODEL WITH MACHINE LEARNING

The article analyzes machine learning, its methods, advantages and disadvantages, combating fraud.

Шахрайство в мережі є серйозною проблемою, від якої страждають люди. Воно передбачає несанкціоноване використання, втручання або маніпуляції з мобільним телефоном або особистими даними, з метою незаконного отримання грошей. Шахраї можуть використовувати різні вразливі місця та лазівки в інфраструктурі мобільних мереж, пристроях і послугах для здійснення своїх зловмисних дій. Машинне навчання стає все більш популярним у боротьбі з цим. За допомогою цієї технології можна виявляти шахраїв та уникати фінансових втрат [1].

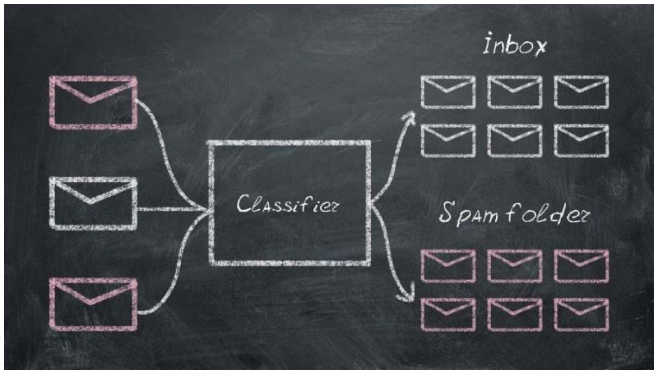
Історія розвитку машинного навчання виявлення шахрайства почалася в 1990-х роках, коли комп'ютерна технологія стала досить розвиненою, щоб обробляти велику кількість даних та виконувати складні завдання. Початково машинне навчання застосовувалось для виявлення шахрайства в фінансових транзакціях, але згодом воно стало застосовуватись в багатьох інших сферах, таких як медицина, транспорт, торгівля та інші.

У 2000-х роках машинне навчання почало розвиватись з використанням глибокого навчання, що дало можливість створювати більш точні та надійні моделі виявлення шахрайства. Глибоке навчання дозволяє навчити комп'ютер розпізнавати складні залежності між різними ознаками транзакцій та виявляти навіть найскладніші форми шахрайства.

Сьогодні машинне навчання стало необхідністю для багатьох організацій, які працюють з великою кількістю даних та проводять транзакції в Інтернеті. Воно дозволяє автоматизувати процес виявлення шахрайства та зменшити кількість помилок, що можуть бути зроблені людським фактором. Крім того, здатне швидко виявляти нові форми шахрайства, які можуть виникнути в майбутньому, що дозволяє забезпечити більш ефективне захист від шахрайства [2].

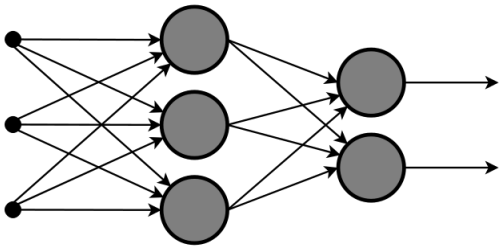
Машинне навчання є кращим для визначення шахрайства в порівнянні з іншими методами. Ось основні методи машинного навчання для виявлення шахрайства:

Класифікація: цей метод полягає в тому, щоб навчити комп'ютер розпізнавати шаблони шахрайства на основі історичних даних та використовувати їх для виявлення нових випадків. Цей метод зазвичай використовується для виявлення фішингових атак, коли шахраї відправляють листи, щоб перехопити особисту інформацію.



Кластеризація: цей метод полягає в тому, щоб навчити комп'ютер групувати схожі транзакції за специфічними ознаками, такими як місцезнаходження або час. Якщо певний клас транзакцій виявляється як шахрайство, то можна більш ефективно виявляти подібні шаблони шахрайства у майбутньому.

Нейронні мережі: цей метод полягає в тому, щоб навчити комп'ютер розпізнавати складні зв'язки між різними ознаками транзакції. Це дає можливість виявляти більш складні форми шахрайства, такі як використання штучного інтелекту.



Методи класифікації, кластеризації та нейронних мереж дозволяють автоматизувати процес виявлення шахрайства та зменшити кількість помилок, які можуть виникнути в результаті ручного аналізу. Проте, успішне використання машинного навчання в сфері виявлення шахрайства потребує якісних даних, а також постійного оновлення навчальних моделей для забезпечення ефективного виявлення найновіших форм шахрайства.

Машинне навчання має кілька переваг в порівнянні з традиційними методами. Ось деякі з них:

Відсутність людського фактору: Комп'ютерні алгоритми, навчені на підставі історичних даних, можуть бути більш точними та ефективними виявляти шахрайство, оскільки не піддаються людському впливу.

Швидкість та ефективність: Машинне навчання може обробляти великі обсяги даних в значно менші терміни, порівняно з людськими аналітиками. Це дозволяє виявляти шахрайство швидше та з меншою кількістю помилок.

Автоматизація: Машинне навчання може бути повністю автоматизованою системою, що дозволяє виявляти шахрайство в режимі реального часу. Це дозволяє реагувати на шахрайство швидко та ефективно, тим самим запобігаючи великій кількості втрат.

Спроможність адаптуватися: Машинне навчання може адаптуватися до нових форм шахрайства, що постійно з'являються. Це дозволяє підтримувати високий рівень ефективності при виявленні шахрайства, незалежно від того, наскільки складним воно може бути. [3]

Традиційна модель виявлення шахрайства, яка базується на статичній системі, на основі правил, має свої переваги та недоліки. Основна перевага полягає у тому, що правила відображають досвід та знання експертів, тому вони можуть бути досить ефективними виявляти підозрілу активність в мережі. Однак, ці системи мають кілька значних недоліків.

По-перше, статична система на основі правил сильно залежить від людської праці. Навіть якщо правила розробляють найкращі експерти, це все одно обмежує можливості системи, оскільки вона не може адаптуватися до нових видів шахрайства та інших змін у мережі. По-друге, створення та вдосконалення правил потребує часу та зусиль. Нові види шахрайства постійно з'являються, тому статична система на основі правил не завжди може бути вчасно оновлена, щоб виявляти нові загрози. По-третє, статична система може бути досить складною та містити велику кількість правил, що може ускладнювати її підтримку та розуміння сторонніми користувачами.

В цілому, традиційна модель може бути корисною, але її обмеженості та недоліки можуть бути проблемою для ефективного виявлення шахрайства в сучасних цифрових середовищах.

Виявлення шахрайства за допомогою машинного навчання може вирішити всі ці проблеми. Навіть перевершити традиційні системи виявлення шахрайства за швидкістю, якістю та економічною ефективністю.

Література

1. C. M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.
2. Hiyam, A. E. Tawashi, Detecting Fraud in Cellular Telephone Networks Jawwal Case Study. MBA thesis Islamic University, Faculty of Commerce, Department of Business Administration, Gaza. 2010.
3. Bolton, R. J. and Hand, D. J., Statistical Fraud Detection, A review, Institute of Mathematical Statistics, 2002. 17(3).