**CREDIT CARD FRAUD DETECTION**

The challenge of detecting fraudulent credit card transactions is significant, as it ensures that customers are not charged for items they did not purchase. The main challenges involved in credit card fraud detection include enormous data processing, imbalanced data, data availability, misclassified data, and adaptive techniques used by scammers. To tackle these challenges, the following strategies can be employed:

Fast and simple models: The model used for detection should be simple and fast enough to detect anomalies and classify them as fraudulent transactions quickly

Handling imbalanced data: Imbalanced data can be addressed using various methods, such as oversampling or undersampling techniques, to balance the distribution of fraudulent and non-fraudulent transactions

Data privacy: To protect user privacy, the dimensionality of the data can be reduced, and a more trustworthy source can be found to double-check the data, at least for training the model

Interpretable models: Making the model simple and interpretable allows for easier adaptation to changes in scamming techniques, enabling quick deployment of updated models

By implementing these strategies, credit card companies can effectively detect and prevent fraudulent transactions, ensuring that customers are not charged for items they did not purchase.

References: <https://www.infosysbpm.com/blogs/bpm-analytics/machine-learning-for-credit-card-fraud-detection.html>

How can machine learning help in credit card fraud detection?

The digital payments market is soaring as the world shifts towards online and card-based payment methods at a faster rate. With such a shift comes the growing issue of cybersecurity and fraud, which is more common than ever.

Enhancing credit card fraud detection is a priority for all banks and financial organisations. Thanks to machine learning (ML), credit card fraud detection is becoming easier and more efficient.\* ML-based fraud detection solutions can track patterns and prevent abnormal transactions.

Common credit card fraud techniques

Credit card fraud rose by a whopping 46% in 2021 when digital transactions became the norm. The US has been a significant contributor to this statistic. This means that the modi operandi of credit card fraudsters have also witnessed change. The various ways in which fraudsters can commit credit card fraud include:

Creating counterfeit credit cards using legitimate credit card information

Creating and using new credit card accounts under someone else's name

Stealing an existing credit card holder's account

Skimming shoppers' credit cards while swiping and making fraudulent copies

Manipulating the payer into making multiple credit card transactions against the same invoice/purchase

Committing card not present (CNP) fraud, that is, making transactions without physical possession of the credit cards via phone or email

Taking over cardholders' accounts via email phishing and deceptive text messages

How can machine learning help with credit card fraud detection?

Machine learning models can recognise unusual credit card transactions and fraud. The first and foremost step involves collecting and sorting raw data, which is then used to train the model to predict the probability of fraud[2]. The solutions offered by machine learning for credit card fraudulent detection involve:

Classifying whether credit card transactions are authentic or fraudulent using algorithms such as logistic regression, random forests, support vector machines (SVMs), deep neural networks along with autoencoders, long short-term memory (LSTM) networks, and convolutional neural networks (CNNs)

Predicting whether it is the cardholders or the fraudsters using the credit cards through credit card profiling

Using outlier detection methods to identify considerably different transactions (or 'outliers') from regular credit cards transactions to detect credit card fraud.

The benefits of using machine learning for credit card fraud detection

Machine learning (ML) models are much better than conventional fraud detection models. They can recognise thousands of patterns from large datasets. ML offers an insight into how users behave by understanding their app usage, payments, and transaction methods. Some of the benefits of fraud detection using ML are as follows:

Faster detection

A machine learning model can quickly identify any drifts from regular transactions and user behaviours in real time. By recognising anomalies, such as a sudden increase in transactional amount or location change, ML algorithms can minimise the risk of fraud and ensure more secure transactions.

Higher accuracy

Conventional fraud detection techniques cause errors at the payment gateways that sometimes result in genuine customers being blocked. With sufficient training data and insights, ML models can achieve higher accuracy and precision, reducing these errors along with the time required to be spent on performing manual analysis.

Improved efficiency with larger data

Once an algorithm picks up different transactional patterns and behaviours, it can efficiently work with large datasets to separate authentic payments from fraudulent ones. The models can analyse huge amounts of data in seconds while offering real-time insights for improved decision-making capabilities.

How can Infosys BPM help?

Our ML-based fraud detection solutions and management services help clients protect themselves from malicious practices by leveraging excellent expertise and insights into fraudulent transactions. Our analytical skills, combined with our technology, can help protect your organisation's revenue and brand image.

We offer retail and e-commerce fraud management solutions that include:

eCommerce fraud management

PoS fraud management

Product counterfeit fraud management

For organisations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed organisational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive yet modular suite of services is doing exactly that. Equipping organisations with intuitive decision-making automatically at scale, actionable insights based on real-time solutions, anytime/anywhere experience, and in-depth data visibility across functions leading to hyper-productivity, Live Enterprise is building connected organisations that are innovating collaboratively for the future.

References :

1. Basic idea of the problem: <https://www.geeksforgeeks.org/ml-credit-card-fraud-detection/>
2. Some gyst of the topic: <https://towardsdatascience.com/credit-card-fraud-detection-using-machine-learning-python-5b098d4a8edc>
3. Another approach of this detection by GA Algorithm: <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00573-8>
4. Companies Approaches: <https://www.infosysbpm.com/blogs/bpm-analytics/machine-learning-for-credit-card-fraud-detection.html>
5. Datasets: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>
6. Reviews: <https://link.springer.com/article/10.1007/s44230-022-00004-0>
7. Articles related to it : <https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=12455&context=theses>