# Securing Tomorrow: Navigating Innovation and Ethics in Credit Card Fraud Detection

Aditya Krishna

2024-10-25

Credit card fraud is a consumer's worst nightmare. From housing, to vehicles, to the grocery store, credit determines most of the purchases of the average consumer. Millions of people around the globe check their credit scores and work to keep their credit history perfect to save money on large purchases like mortgages and personal loans. However, with the rise of e-commerce, a very small percent of consumers will fall victim to credit card fraud, and it can ruin peoples' lives if they are not aware. With billions of transactions daily, no company can dedicate a human resources to find fraudulent transactions. To combat this, credit card companies look towards fraud detection algorithms to sift through the transactions to alert consumers and the company to potential fraudulent transactions. Researchers around the world have started applying ML techniques to improve this process. This paper examines "A machine learning based credit card fraud detection using the GA algorithm for feature selection," by Emmanuel Ileberi, Yanxia Sun, and Zenghui Wang, which utilized a different approach to solving credit card fraud with ML. While their research might have improved fraud detection, it also brings awareness to issues like consumer data collection and privacy, algorithmic bias, and consumer trust in credit card providers.

The paper begins by acknowledging other researchers' attempts at solving credit card fraud. They all used the same dataset based on European cardholder data and the researchers used logistic regression (LR), decision tree (DT), support vector machine (SVM) and random forest (RF), and many others. While they all had decent results, they all failed to have high accuracy levels, the metric that the authors determined as the best indicator of model success. To solve the low accuracy, the authors chose to use a special feature selection algorithm called a Genetic Algorithm (GA) based feature selection. A genetic algorithm is a type of evolutionary algorithm (EA) that solves optimization problems. This algorithm is based of off biological evolution. EAs have three attributes: population (all the possible solutions), fitness (measure of "success" of a solution), and variation (represents the "mutations" of each solution). A very important choice for EAs is the fitness measure as it determines how the feature selection will determine what is optimal. The authors referenced another study that used a GA-based FS and determined that RF is best as it solves the overfitting issue with normal decision trees. Credit card fraud, although extremely scary and important to prevent, is very rare in the billions of transactions that happen daily. As a result, datasets regarding credit card fraud are extremely skewed, so the authors have to be aware of overfitting throughout the

algorithmic process.

To implement GA, they divided their data into train and test data and computed the fitness of all the features using RF. If the desired fitness has been met, designated by $q$ (optimal fitness score), you have found the optimal feature subset and feature selection is complete. The GA returned 5 different vectors containing features that it determined were optimal.

Next, the authors used the 5 different vectors to train the data on 5 different types of ML algorithms: decision trees (DT), random forest (RF), logistic regression (LR), naive Bayes (NB), and artificial neural network (ANN). After standard data pre-processing, including data-normalization using the min-max scaling equation, the authors trained each of the algorithms on each of the vectors of selected features. For each model, the same testing process for each vector is conducted until the desired results are achieved. To evaulate each model, the authors used the following metrics: accuracy (AC), recall (RC), precision (PR), F1-score (F-measure), and area under the curve (AUC). Accuracy is simply the precent of correct predictions. Recall is the percent of correct positives out of all positives. Precision is the percent of correct positives out of predicted positives. F1-score is a metric that balances precision and recall. Finally, AUC is a metric that measures a model's ability to distinguish between classes with 1 being perfect, .5 being a completely random model, and 0 being it incorrectly selects the class every time.

The results had many takeaways. First, for each vector of selected features, the RF model usually performed in accuracy, precision, and AUC while the NB and LR methods underperformed consistently. To verify these results. the authors trained the same types of models on a randomly chosen feature vector and the full feature vector to bolster the strength of their choice in feature selection. The ten models trained on the control vectors heavily underperfomed compared to the feature selection which strengthened their hypothesis that feature selection would aid in ML fraud detection. Next, the authors compared their results to the papers they used as inspiration and the accuracy of authors' best models outperformed by an average of 2.7%. Their final results concluded that GA-based FS improved all the standard ML algorithms and they intend to use more datasets to validate their framework.

While preventing credit card fraud is very important for all consumers, it should never come at the cost of data privacy. A consumer should be entitled to privately purchase anything without worrying about their data being leaked. PII (personally identifiable information) is always collected on every transaction at every bank worldwide. This data must never be leaked when allowing public research solely to reduce the cost of doing the research in house.

Another potential ethical consideration is the algorithmic bias involved with feature selection. While the names of features besides Time and Amount were removed from the dataset, the features included have the possibility to be some immutable characteristic of a consumer. This could lead to certain groups of people having their transactions scrutinized at a disproportionate rate which is extremely unethical. Ensuring that feature selection algorithms are unbiased in their choices is a difficult task, but it must not be overlooked as a credit card provider should equally trust all transactions by all consumers without explicit cause.

While the previous ethical consideration will cause a degradation in the trust of the consumer, it will also degrade the trust of the credit card providers as well. Companies are obligated

to provide the best services to their customers or else they will lose business. A company must be able to protect their consumers against unethical and illegal activities like identity theft, skimmers, and card-not-present (CNP) transactions where a majority of fraud occurs. With the rise of e-commerce, companies should bolster their security to be able to protect themselves and their consumers ethically and financially.

In conclusion, credit card fraud is a complex issue to solve with serious finanical, ethical, and security implications. Consumers need to be protected from illegal activity online while being able to freely spend their hard-earned money without fear of scrutiny from their credit card provider. Providers also need to be able to protect their assets while not unfairly discriminating against any of their customers. This complexity requires intelligent minds from the ML and ethical communities to produce a fair and execellent solution to a worldwide problem.

References

Ileberi, E., Sun, Y. & Wang, Z. A machine learning based credit card fraud detection using the GA algorithm for feature selection. J Big Data 9, 24 (2022). https://doi.org/10.1186/s40537-022-00573-8