Fraud Detection in Customer Transactions Using Dimensionality Reduction and Clustering

Anim Ohene
College of Science and Technology
Temple University

Henry Nguyen
College of Science and Technology
Temple University

Businesses and banking institutions have serious concerns about identifying and stopping fraud in consumer interactions. Fraudulent operations can cause large financial losses and harm to a company's reputation, including identity theft, account control, and unlawful transactions. The intricacy and sophistication of deceptive strategies keep changing as technology develops and digital transactions proliferate.

This study aims to solve the difficulties in detecting fraud in consumer transactions and analyze more efficient strategies for successfully preventing fraud. Financial institutions may limit financial losses, safeguard their brand, and improve customer contentment by creating effective fraud detection procedures. Effective fraud detection also helps keep financial systems secure and reliable, which is advantageous to both consumers and institutions.

The issue is how to quickly and efficiently detect fraudulent activity in customer transactions. Phishing schemes and pretexting are two common strategies used by fraudsters to fool people into giving personal information or committing fraudulent acts without realizing it. These techniques bypass security measures by preying on people's weaknesses and manipulating their minds to conduct fraud discretely. To detect sophisticated fraud schemes, traditional fraud detection approaches generally rely on rule-based systems (flag suspicious activities if the amount exceeds the limit) and manual review procedures, which may not be reliable, efficient, or flexible enough.

While supervised machine-learning algorithms may be efficient in detecting fraudulent transactions, a more nuanced approach such as unsupervised learning, may prove more effective in detecting fraud. Unsupervised tasks such as dimensionality reduction and clustering algorithms may be applied to transform the dataset into a lower-dimensional space while retaining the important information, only then using the clustering technique to reveal hidden structures in the scope of fraud transactions. To start, obtaining a dataset representing fraudulent transactions is necessary. Features may include the time length of the transaction, amount of money, product, type of transaction, and binary values for the target variable(isFraud). After preprocessing the data, statistical tests such as mutual information gain may be used to assess dependencies between features and target variables with the aim of selecting the top 2 or 3 features to be used in the clustering task. This selection of 2 or 3 features is made so orderly and comprehensible visualizations can be made of the selected original features. Subsequently, apply a dimensionality reduction technique such as Principle Component Analysis (PCA) to reduce the dimension of the selected features. It is well known that correlation does not imply causation, however, performing the clustering task between features highly correlated to the target variable may allow for relevant pattern recognition and meaningful data to be structured. After clustering, desired insights are, ranges of susceptibility to fraudulent transactions, suggestions to be made to susceptible groups, etc…

For the clustering task, algorithms such as k-means, k-means++, and agglomerative clustering may be fitted on the given feature set. K-means is a clustering algorithm that randomly initializes cluster centroids, classifies samples as members as part of its cluster based on their distance to its centroid in relation to other cluster centroids, relocates the cluster centroid to its center of mass, and repeats the process until the centroid center of mass remains the same. Similar to k-means is k-means++ which mitigates unfavorable clusters by initializing cluster centroids in a more structured way. Lastly, Agglomerative clustering is a form of hierarchical clustering that initializes each sample as a cluster,

merges the nearest two clusters into a new cluster, and repeats until one cluster remains. Now, Optimization techniques such as the Elbow Method for finding the optimal amount of clusters, as well as different distance parameters of agglomerative clustering will be used in obtaining proficient clusters.

Finally, the clustering algorithms will be evaluated, based on the integrity of the clusters. One particular metric to be used is the silhouette score, which measures the association of a sample to its cluster as opposed to its attraction to another cluster. That is, silhouette scores assign values that range from -1 to 1, where -1 may be interpreted as a possible misclassification of a sample to a cluster, and 1 as a sample being assigned to its correct sample. After performing evaluation metrics, a bar plot will be made to compare the different clustering algorithms used and their silhouette scores, in selecting the most appropriate clustering algorithm for the given task. In addition, after partitioning the selected features, the class ratio of target variables in the clusters will be taken.

The Timeline of the project is to first obtain a fraud transaction dataset, befitting the use case. This is followed by the data pre-processing phase. Utilize PCA to reduce the dimension of the selected features with the highest mutual information. Next is to fit the data to the clustering algorithms. Subsequently, the optimization techniques and the visualization of the clustering will be seen. Afterward, the models will be evaluated and compared. After performing the evaluation metrics the most appropriate model will be chosen to further gain insights, into, ranges of susceptibility to fraudulent transactions, and the suggestions to be made to the susceptible groups.

References:

Abdallah, Aisha, et al. “Fraud Detection System: A Survey.” Journal of Network and Computer Applications, vol. 90–113, 1 June 2016, https://doi.org/10.1016/j.jnca.2016.04.007.

Vasan, K. Keerthi, and B. Surendiran. “Dimensionality Reduction Using Principal Component Analysis for Network Intrusion Detection.” Perspectives in Science, vol. 510–512, 1 Sept. 2016, https://doi.org/10.1016/j.pisc.2016.05.010.