CREDIT CARD FRAUD DETECTION

INTRODUCTION:

Fraud detection is critical in keeping remediating fraud and services safe and functional. First and foremost, it helps to protect businesses and individuals from financial loss. By identifying potential instances of fraud, companies can take steps to prevent fraudulent activity from occurring, which can save them a significant amount of money. Fraud detection also saves users a lot of headaches and instills trust in them when they know these protections are in place.

FEATURES ENGINEERING FOR FRAUD DETECTION

Feature engineering for fraud detection
When constructing a credit card fraud detection algorithm, the initial set of features (raw features) include information regarding individual transactions. It is observed throughout the literature, that regardless of the study, the set of raw features is quite similar. This is because the data collected during a credit card transaction must comply with international financial reporting standards (American Institute of CPAs, 2011). In Table 4, the typical credit card fraud detection raw

The Feature engineering strategies for credit card fraud detection was an essential framework in creating features to analyze credit card transaction data.

1.A more compressive way for feature creation is to derive some features using a transaction aggregation strategy.

2.The derivation of the aggregation features consists in grouping the transactions made during the last given number of hours, first by card or account number, then by transaction type, merchant group, country or other, followed by calculating the number of transactions or the total amount spent on those transactions.

3.When aggregating customer transactions, there is an essential question on how much to accumulate, in the sense that the marginal value of new information may diminish as time passes. Indeed, when time passes, information loses their value, in the sense that customer spending patterns are not expected to remain constant over the years. In particular, Whitrow et al. define a fixed time frame to be 24, 60, or 168.

MODEL TRAINING FOR CREDIT CARD FRAUD DETECTION:

Training a credit card fraud detection model involves several steps. Here's a high-level overview of the process:

1.*Data Collection and Preprocessing:*

- *Data Collection:* Gather historical transaction data, including both fraudulent and legitimate transactions.
- *Data Preprocessing:* Clean the data, handle missing values, and encode categorical variables. Split the data into training and testing sets.

2. *Feature Engineering:*

- Create relevant features from the transaction data, as discussed in the previous response.

3. *Model Selection:*

- Choose an appropriate machine learning algorithm for fraud detection, such as Logistic Regression, Random Forest, Gradient Boosting, or Neural Networks.

- Consider ensemble methods for improved accuracy and reliability.

4. *Model Training:*
   - Train the selected model(s) using the training data.
   - Utilize techniques like cross-validation to tune hyperparameters and avoid overfitting.
5. *Model Evaluation:*
   - Evaluate the model's performance using the testing dataset.
   - Metrics like accuracy, precision, recall, F1-score, and area under the ROC curve (AUC-ROC) are crucial for fraud detection tasks.
   - Given the class imbalance (fraudulent transactions are usually a small portion of the data), focus on metrics like precision and recall, which provide a better understanding of the model's performance.
6. *Adjust Thresholds:*
   - Depending on the business requirements and the cost associated with false positives and false negatives, adjust the classification threshold to balance precision and recall.
7. *Monitoring and Updating:*
   - Continuously monitor the model's performance in a production environment.
   - Regularly update the model with new data to keep it relevant and accurate.

Tips and Best Practices:

- *Imbalanced Data:* Address class imbalance using techniques like oversampling, undersampling, or using algorithms that handle imbalanced data well.

- *Anomaly Detection:* Consider using anomaly detection techniques like Isolation Forest or One-Class SVM in addition to traditional classification algorithms. These methods are well-suited for detecting rare events.

- *Explainability:* For regulatory compliance and understanding the model's decisions, consider using explainable AI techniques to interpret the model's
- *Validation Set:* Apart from the training and testing sets, maintain a validation set for fine-tuning the model during the training process.

Remember, the effectiveness of the model heavily depends on the quality of data, feature selection, and the chosen algorithm. Regularly updating and monitoring the model are essential to adapt to evolving fraud patterns.

EVALUTION FOR CREDIT CARD FRAUD DETECTION:

Credit card fraud detection evaluation

A credit card fraud detection algorithm consists in identifying those transactions with a high probability of being fraud, based on historical fraud patterns. The use of machine learning in fraud detection has been an interesting topic in recent years. Different detection systems that are based on machine learning techniques have been successfully used for this problem, in particular: neural networks (Maes, Tuyls, Vanschoenwinkel, & Manderick, 2002), Bayesian learning (Maes et al., 2002),

CONCLUSION:

Maes and his team proposed using Bayesian and Neural Network in the credit card fraud detection. Their results showed that Bayesian performance is 8% more effective in detecting fraud than ANN, which means that in some cases BBN detects 8% more of the fraudulent transactions.