

IBM –NAAN MUDHALVAN - APPLIED DATA SCIENCE

Project name: Credit Card Fraud Detection

Phase 2: Innovation

INTRODUCTION :

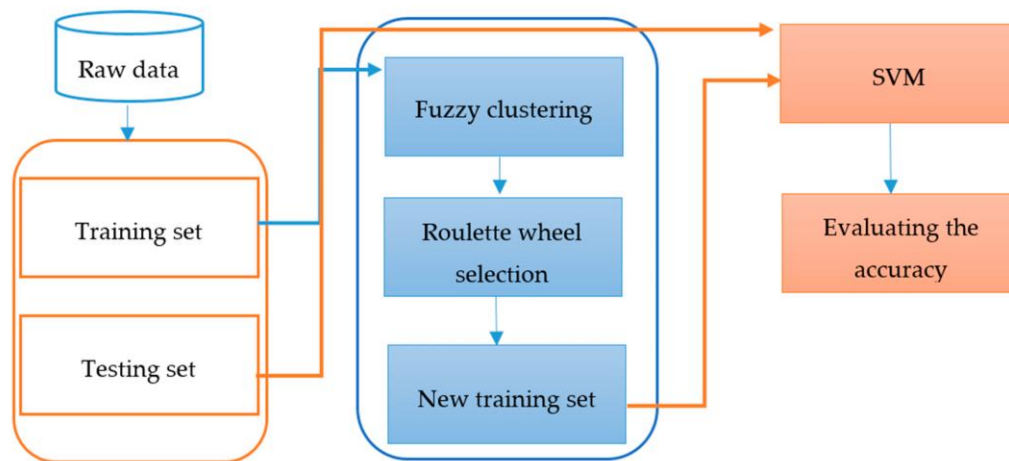
Fraud detection and prevention tools involve risk mitigation by monitoring and reviewing user actions. Device fingerprinting, social media lookup, and data enrichment are part of the fraud detection and transaction fraud detection tools. I hope you got a good intuition about isolation forest algorithm and how it achieves high anomaly detection performance reducing swamping and masking by leveraging the subsampling technique.

- Certainly, advanced techniques like Isolation Forest, One-Class SVM, and ensemble methods can be very effective for improving fraud detection accuracy.
- Isolation Forest is great at isolating anomalies, while One-Class SVM can be used to model the normal behavior and detect deviations. Ensembles, such as Random Forest or boosting, can combine multiple models for enhanced performance.
- If you have specific questions about implementing these techniques or need more information, feel free to ask!
- **Advanced Fraud Detection Techniques**User
Consider exploring advanced techniques such as anomaly detection algorithms (e.g., Isolation Forest, One-Class SVM) and ensemble methods for improved fraud detection accuracy.
- Certainly, using advanced techniques like Isolation Forest, One-Class SVM, and ensemble methods can enhance fraud detection accuracy. These methods work well for anomaly detection in fraud detection systems.

Isolation Forest: It's effective at isolating anomalies by creating a binary tree structure. Anomalies are isolated closer to the root, making them easier to detect.

One-Class SVM: This algorithm is suitable for one-class classification, making it useful for detecting anomalies in imbalanced datasets, which is common in fraud detection.

Ensemble Methods: Combining multiple models can improve accuracy. Techniques like Random Forest or Gradient Boosting can be used to create an ensemble of models for more robust fraud detection.



To implement these techniques:

Data Preprocessing: Ensure your data is well-preprocessed and features are properly engineered.

Model Selection: Choose the appropriate anomaly detection algorithm(s) and ensemble methods for your dataset. Experiment with different algorithms to find the best fit.

Hyperparameter Tuning: Fine-tune the hyperparameters for each algorithm to optimize performance.

Cross-Validation: Use cross-validation to assess the models' generalization and avoid overfitting.

Monitoring and Updating: Continuously monitor the performance of your fraud detection system and update it as new data becomes available.

Remember that fraud patterns can change over time, so a robust and adaptable system is essential.

One-class SVM (SGD) – Builds on the one-class SVM algorithm using Stochastic Gradient Descent (SGD). Isolation forest – Uses decision trees to continuously split or divide the data to eventually isolate anomalous data points.

AE Reconstruction Error Distribution

