\Orchestrating a brighter world NEC

Retail Banking Fraud Analytics

Mitigate Risks and Prevent Frauds with Ease

Introduction

Fraud detection and prevention are important for banks catering to retail clients/customers to prevent losses and build customer trust. In retail banking, frauds could originate from various sources such as customers, people pretending as customers, hackers or external criminals. However, the most prominent of the frauds involve fake/stolen credit and debit cards. According to a recent study by Nielson, losses from fraud involving cards used for payment worldwide reached $27.85 billion in 2018 and are projected to rise to $35.67 billion in five years and $40.63 billion in 10 years.

Analysis of transactions and activities such as purchasing, accounts payable, POS, sales projections, warehouse movements, employee shift records, returns, store-level video and audio recordings, and other data across your company can help you to identify fraudulent activities and develop suitable priorities for management and investigation.

Retail Fraud in Numbers*

2.81 B
Credit Card Users
World-wide

368.92 B
Purchase
transacations for
goods and services
World-wide

$32.39 B
Global
Payments
Fraud

NEC's Retail Banking fraud analysis enables Retail Bankers to combat card fraud by analysing huge volumes of historical and current transaction data to understand buyer motivation and identify anomalies (suspicious activities that deviate from the norm). By applying deep learning and AI algorithms, the solution extracts numerous attributes for each transaction and analyses millions of data points to keep the sales secure and transparent. Our solution helps reveal hidden patterns that a human-led interaction would have found difficult. When an anomaly is detected, the platform can either block a user or a transaction, or send an alert to an employee to investigate the activity further. Our fraud detection and prevention engine is capable of self-learning, thereby becoming more accurate and powerful after every single transaction they inspect.

*Nielsen Report 2020

Fraud Types

Outside the Store Fraud

Lost or stolen cards – Here a customer finds a lost card and doesn't try to return it, or steals it from another customer at a retailer's location.

Account takeover – Here a cardholder unwittingly gives their account information, such as their card number or home address, to a criminal, who then contacts the cardholder's bank, reports a lost card and change of address, and obtains a new card in the soon-to-be victim's name.

Counterfeit cards – Cloning a card from another and then using the clone to make purchases

Never received – Here a new or replacement card is stolen from the mail and never reaches its rightful owner.

Fraudulent Applications – Here a criminal uses someone else's name and information to apply for and obtain a credit card from a bank.

Inside the Store Fraud

Malware – Criminals install malware on a POS system software

Multiple imprint – Here a single transaction is recorded multiple times on an older credit card imprint machine

Collusive retailers - Employees conspire with criminals to defraud.

Card-not-present Fraud(CNP)

This type of fraud involves internet, phone and mail-order transactions or activity. The actual fraud occurs after criminals steal card information by using hacking, phishing or skimming techniques.

Web and Mobile based Frauds

This type of fraud involves internet, phone and mail-order transactions or activity. The actual fraud occurs after criminals steal card information by using hacking, phishing or skimming techniques.

Retail Fraud - Business Impact

Loss of Billions of Dollars resulting in Rise of Bottom Line

Dissatisfaction of Genuine Customers

Delayed Operations

Misutilized Workforce

Opportunity Lost(Cost)

Solution Overview

Problem Statement

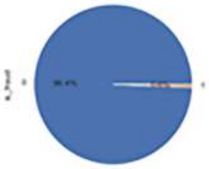
- Digital/cashless transactions have led to increasing in fraudulent activities, causing an increase in losses for financial institutions and card issuers.
- BFSI is seeking new techniques and solutions to detect & combat card frauds.

Solution

- Classification Models such as Logistic Regression, Decision Tree, Random Forest, Deep Learning etc. to predict the precision of a transaction being fraudulent.
- Can be used either in-real time monitoring by the bank or after a fraud complaint by a customer.
- ML/DL techniques can detect fraud transactions with precision based on the previous transactions of a customer and can easily learn the complex hidden patterns in transaction data in real-time for fraud detection.

Outcomes

- Detect and predict suspicious transaction as fraud and non-fraud, thereby safeguarding the interest of genuine customers.
- Analyse customer transaction behaviour and determine fraud patterns.
- Beneficiaries: Vigilance Department of Banks and NBFCs, CC provider companies

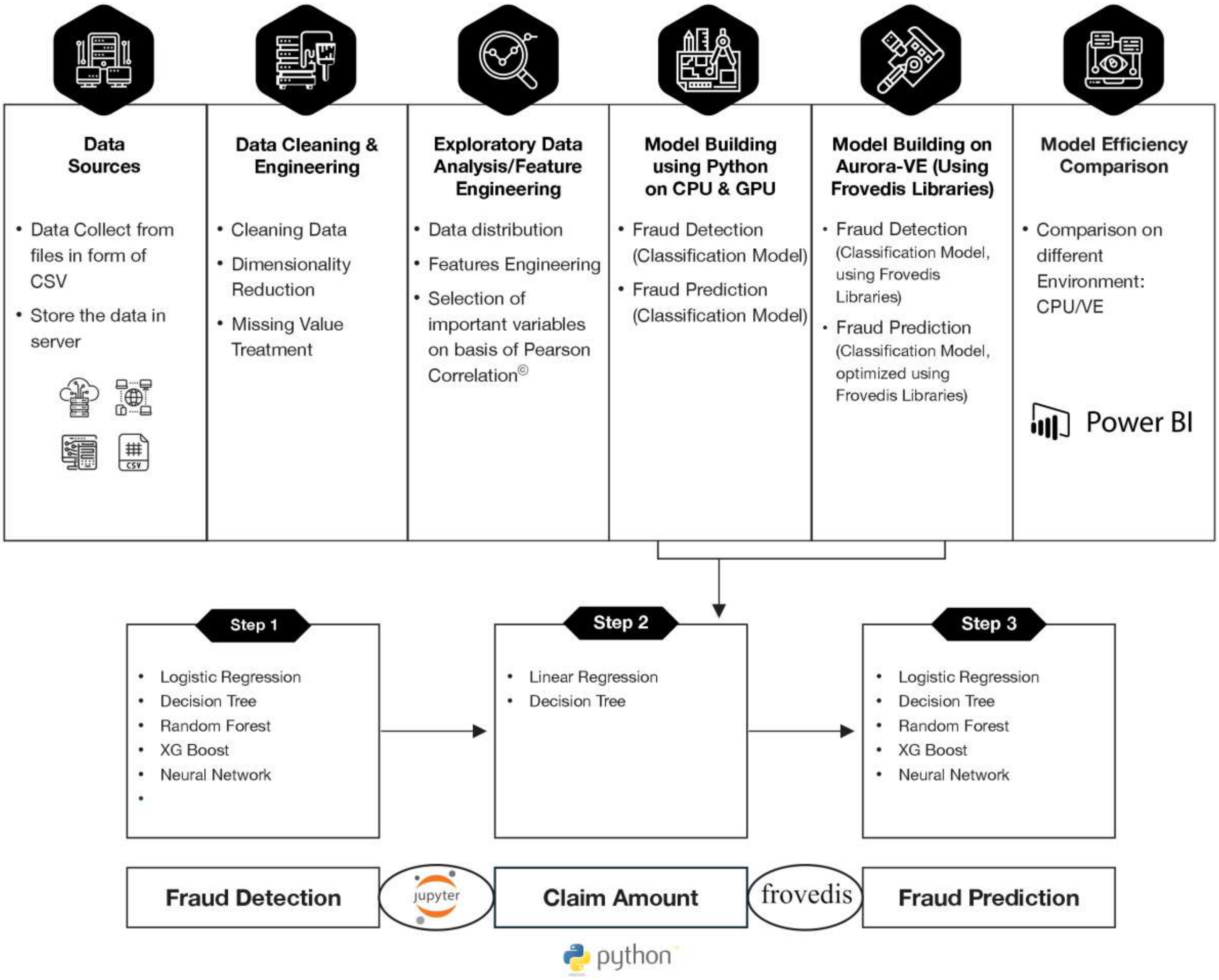


Accuracy & Performance Parameters

✓ Accuracy Parameters

Confusion Matrix

Solution Flow



Data Sources

- Data Collect from files in form of CSV
- Store the data in server

Data Cleaning & Engineering

- Cleaning Data
- Dimensionality Reduction
- Missing Value Treatment

Exploratory Data Analysis/Feature Engineering

- Data distribution
- Features Engineering
- Selection of important variables on basis of Pearson Correlation©

Model Building using Python on CPU & GPU

- Fraud Detection (Classification Model)
- Fraud Prediction (Classification Model)

Model Building on Aurora-VE (Using Frovedis Libraries)

- Fraud Detection (Classification Model, using Frovedis Libraries)
- Fraud Prediction (Classification Model, optimized using Frovedis Libraries)

Model Efficiency Comparison

- Comparison on different Environment: CPU/VE

Step 1

- Logistic Regression
- Decision Tree
- Random Forest
- XG Boost
- Neural Network
-

Step 2

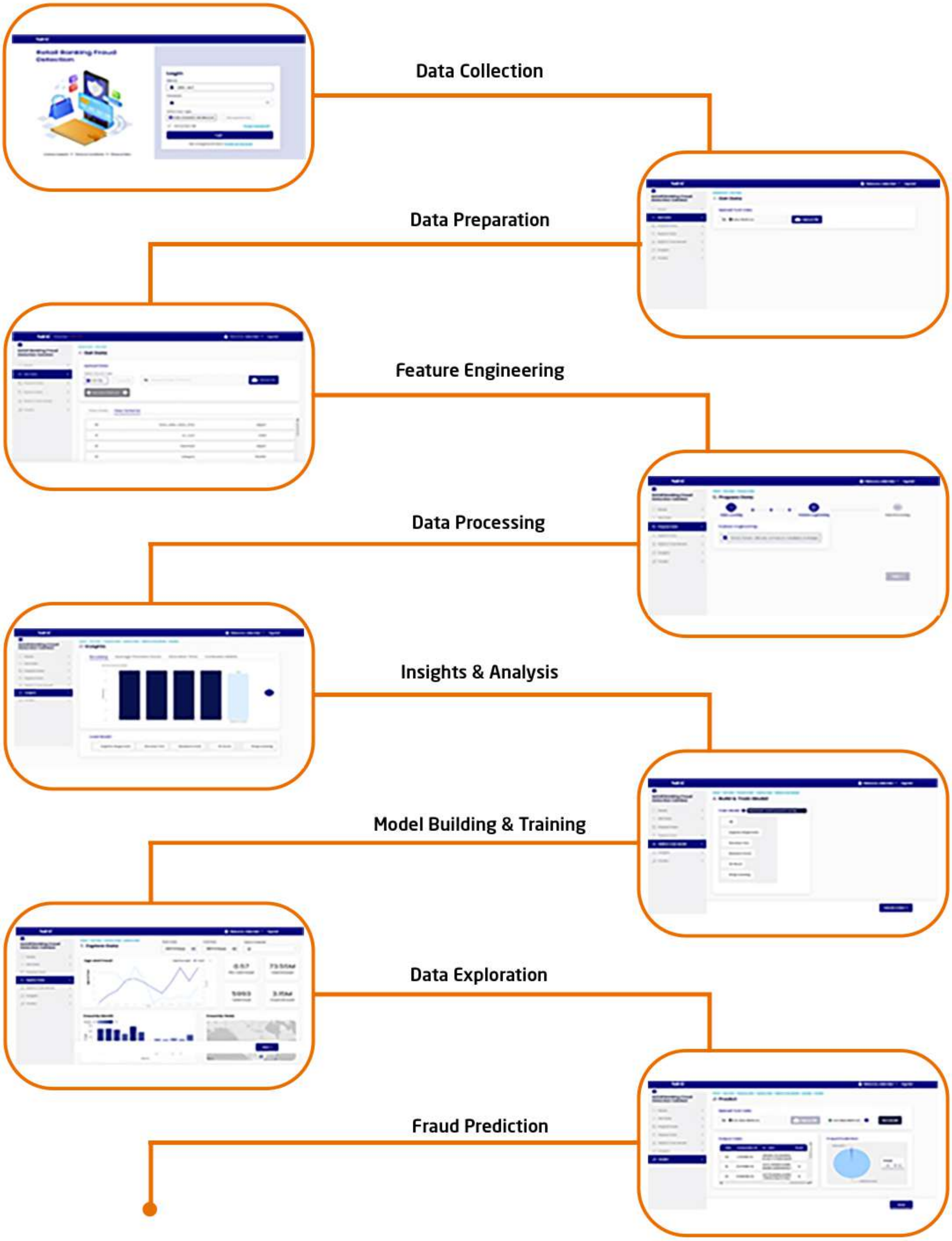
- Linear Regression
- Decision Tree

Step 3

- Logistic Regression
- Decision Tree
- Random Forest
- XG Boost
- Neural Network

Fraud Detection | **Claim Amount** | **Fraud Prediction**

How the Platform Works?



Data Collection

Data Preparation

Feature Engineering

Data Processing

Insights & Analysis

Model Building & Training

Data Exploration

Fraud Prediction

Why NEC?

We at NEC possess deep expertise in the design and implementation of retail fraud detection solution that leverages the most innovative big data techniques including predictive analytics, Artificial Intelligence (AI), data modelling, and Machine Learning (ML). We have expertise in designing and implementing Enterprise ready AL/ML solutions with industry leading accuracy. We enable models to operate on live data streams and model re-training on the go. Our mission is to minimize fraud rates and increase profits by lowering costs for retail frauds in your organization.

Capabilities on Technology Stack

Core business experience combined with domain and technical expertise with Cutting-edge tools and technologies.

Skilled Workforce

In-house business & domain experts

- Data Stewards
- Data Scientist
- Big Data Engineers
- Architects
- Consultants & Data Analysts

Domain Expertise

Solving Complex Data Challenges

Myriad of Successful Analytics Projects

Dedicated Analytics Research Labs

Work for Solutions for Societies

Robust Partner Ecosystem

Strong Partnerships & Alliances Across Data Platforms and Analytics Solutions

Technology Partners

hadoop · CLOUDERA · APACHE Spark · HIVE · kafka · STORM · APACHE nifi · APACHE HBASE

elasticsearch · talend · Informatica · Greenplum · denodo · logstash · tableau

Power BI · pentaho · Qlik · kibana · RStudio · python · R · SPSS · sas

theano · GUROBI OPTIMIZATION · Azure · aws · torch · Caffe · TensorFlow · PostgreSQL

Contact us for more information:

marketing@india.nec.com

in.nec.com