

Fraud Detection using Data Analytics

<https://medium.com/@SivaMakani/fraud-detection-using-data-analytics-5037cf4244e>

One need not be in Police/Crime department to detect the Fraud, instead can be a **Data Analytics Specialist**.

Fraud is a big problem for many businesses and can be of various types: Inaccurate credit applications, Fraudulent transactions both offline and online, Identity thefts and false insurance claims. These problems plague firms of all sizes in many industries. Some examples of likely victims are credit card issuers, insurance companies, retail merchants, manufacturers, business-to-business suppliers and even services providers. A predictive model can help weed out the "negatives" and reduce a business's exposure to fraud.

Predictive modelling can also be used to identify high-risk fraud candidates in business or the public sector. Mark Nigrini developed a risk-scoring method to identify audit targets. He describes the use of this approach to detect fraud in the franchisee sales reports of an international fast-food chain. Each location is scored using 10 predictors. The 10 scores are then weighted to give one final overall risk score for each location. The same scoring approach was also used to identify high-risk check kiting accounts, potentially fraudulent travel agents, and questionable vendors. A reasonably complex model was used to identify fraudulent monthly reports submitted by divisional controllers.

Fraud is an adaptive crime, so it needs special methods of intelligent data analysis to detect and prevent it. This method exists in the areas of Knowledge Discovery in Databases KDD [1], Data Mining, Machine Learning and Statistics. They offer applicable and successful solutions in different areas of fraud crimes.

Use-case for Theft Detection:

Consider a Theft happen in a reputed Jewellery Palace where there is no CCTV surveillance. It is incurred to be huge amount of loss but unfortunately the owner of the Jewellery Palace doesn't want to report to Police department/Media to not to lose the reputation in public. Fortunately, the owner gets to know about Data Analytics specialist and contacted him to resolve this case. And this is how the Data Analytics specialist worked on this case.

Step 1: Understand the requirement (Here the requirement is to find out the culprit).

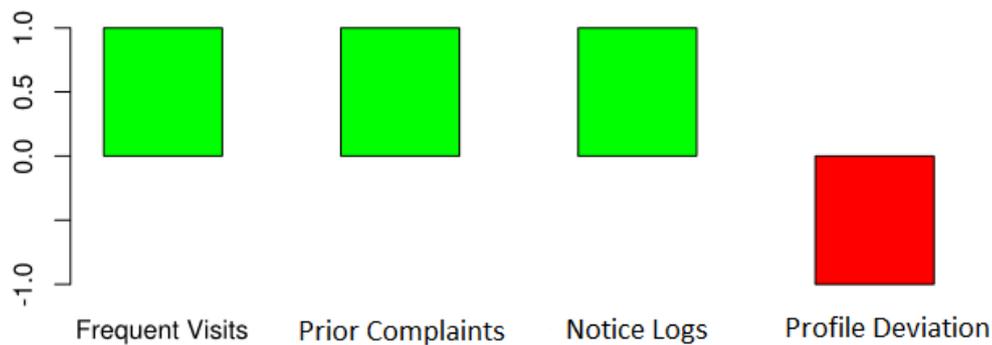
Step 2: Collect Raw Data as much as possible (Collect all the data relevant to the case like Number of Employees, Name of the Employees, Location details, Date and Time, Employee Time Deviation etc.,).

Step 3: Fine Tune the data with any Clustering techniques if required (Tune the Data in proper format which is understandable to the compiler by using Clustering Algorithms such as K-Means Clustering Algorithm).

Step 4: Import/Load the tuned Data to perform the Prediction mechanism by using Data Visualization techniques to convert the Data into Tree map visualization.

Step 5: Set multiple decision factors such as Employee Login time and Logout time, Number of Hours spent, Number of prior complaints about each Employee, Employee Location Deviation inside Palace, Frequent visit to same compartment, Vehicles of Employee, Number of Vehicles entered, Frequent visit of same vehicles, Time spent by each vehicle owner, Flow Profile Deviation and much more.

Generate behavioural Patterns based on the decision factors using statistical and Data Visualization techniques.



Employee Behaviour->Normal Behaviour/Expected Behaviour v/s Current Behaviour

The same Behavioural Pattern should be generated to all employees and all together generate a **Tree map** for easy visualization in finding the culprit.



Based on all decision factors, the Data Analytics specialist predicted that the culprit is Employee 6 and reported to owner of Jewelry palace.

Hence, one need not be in Crime Department for Theft Detection, instead can be a **Data Analytics Specialist**.

..... Siva Makani