Dynamic Risk Profiling: A Risk-based Approach to Managing Fraud
About the Author

Kothai Manoharan

Kothai has over seven years of experience in the Banking, Financial Services, and Insurance (BFSI) domain. She is currently a domain consultant in the Delivery Excellence and Risk Management team in the Retail Banking and Cards group at Tata Consultancy Services (TCS). She holds a Master's degree in Business Administration with a higher diploma in Software Engineering.
Abstract

As banks and financial institutions grow significantly in size and revenue, they face an increased risk of fraud. The growing momentum and intensity of fraudulent activities is a challenge for the payments industry, exposing organizations to huge financial losses. Though banks and financial institutions have mitigated fraud related to paper-based processing by moving to electronic banking, fraudsters are now targeting mobile and other emerging payment processing techniques. They take advantage of loopholes and weak controls in the current systems. Technology can play a significant role in the protection of customer and organizational assets, and enable constant vigilance and diligent action against fraud.

This paper outlines a basic theory and technological framework for dynamic profiling of accounts using Big Data. It highlights the key activities involved in dynamic risk profiling, and how it helps organizations counter fraud. The paper also provides a robust method that organizations can use to upgrade the payment system environment and fight fraud proactively.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td><strong>Dynamic Risk Profiling</strong></td>
<td>6</td>
</tr>
<tr>
<td>Importance of Identifying Fraud Patterns</td>
<td>6</td>
</tr>
<tr>
<td>Technology is a Double-edged Sword</td>
<td>6</td>
</tr>
<tr>
<td><strong>Leveraging Big Data Analytics Framework for Risk Profiling</strong></td>
<td>7</td>
</tr>
<tr>
<td>Identification and Definition of Different Classes of Risk</td>
<td>7</td>
</tr>
<tr>
<td>Implementation of Risk Behavior Analysis</td>
<td>7</td>
</tr>
<tr>
<td><strong>Advantages of Leveraging Big Data Framework for Dynamic Risk Profiling</strong></td>
<td>10</td>
</tr>
<tr>
<td>Conclusion</td>
<td>11</td>
</tr>
</tbody>
</table>
Introduction

Globalization, technological advancements, and product innovation have led to significant changes in the financial landscape, including the rise of increasingly complex fraud risk profiles. The widespread use of new technologies has led to a plethora of new, fraudulent activities. Sophisticated execution of fraud with the help of state-of-the-art technologies makes the task of forestalling fraud attempts more challenging than ever before.

A reactive response to fraud is no longer good enough. Today, the focus has shifted to assessing an organization’s role in inadvertently allowing fraudulent activities by not closing the gaps in its risks and control structure. As per Basel II guidelines, every bank needs to follow certain risk standards, and build robust risk management and technological frameworks to mitigate fraud risk. The thrust is on maintaining the integrity of customer data by curbing identify theft and data leakage.

Figure 1. shows the wide range of crimes that financial institutions and their customers. Robust compliance programs and comprehensive risk management policies with well-defined protocols for preventing, detecting, and responding to fraud help organizations stay one step ahead of defrauders. Adopting a zero-tolerance approach towards fraud needs to become a part of every organization’s corporate culture and agenda. Stemming the tide of illicit financial transactions and meeting regulatory mandates should also be part of the organization’s mission and value statement. Institutions that face moderate to high risks need a rigorous automated system based on dynamic risk profiling systems that proactively identify, alert, assess, and monitor the risk.

Figure 1: Various types of crimes that financial institutions and their customers are susceptible to
Dynamic Risk Profiling

Today’s complex and evolving financial environment calls for robust methodologies and strategies to cover a wide spectrum of risk categories, and create and manage dynamic risk profiles. Profiling should go beyond the creation of a fraudster’s profile to include comprehensive details of the fraud committed.

Financial institutions need to arrive at a thorough understanding of key risk categories, and gain a more holistic and dynamic view of a person’s behavior across these categories. Dynamic risk profiling (DRP) provides an effective means of achieving this goal.

DRP is the process of identifying an account profile as being fraudulent based on the predefined classification rules. It involves continuously monitoring the transactions of such profiles and updating the rules and traits that classify these counterfeit profiles on a real-time basis. Based on its activity patterns, the account may be added to a 'list of defrauders'. Continually updating the definition of a fraudulent individual's profile is also a critical part of the profiling activity.

DRP leverages analytics to consolidate data from a range of sources, and explore the patterns in the acquired data to enable quick and effective decisions on countering fraudulent attempts. It is a ‘plug and play’ concept which can fit within the organization’s framework for risk mitigation and management. This enables organizations to cope with risk at a complex level of operations in a cost effective and efficient manner. Identifying patterns in an individual's fraudulent activities is one of the key activities undertaken in DRP.

The Importance of Identifying Fraud Patterns

Successful fraud perpetration is based on certain key determinants. The fraudster’s personality and other personal factors can play a dominant role in the execution of fraud. In other instances, environmental factors such as opportunities available in the system or lapses in the control mechanism may dominate. In both cases, it is imperative to determine a pattern and create a profile either for the fraudster or for the fraud attempt itself.

Typically, an attempt at financial crime is influenced by three factors — a need that cannot be shared with others (pressure), a perceived opportunity for illicit gains (opportunity), and personal rationalization of the act (justification). The common perception of a fraudster has always been that of a devious and covetous individual. But in reality, a person with no criminal history might commit an act of deceit if swayed by any of these three factors. Such an individual negates the traditional behavioral definition or profile of a fraudster.

Technology is a Double-edged Sword

Identifying patterns in the types of fraud committed or attempted and the behavior of fraudsters has become difficult with the advent of new product types and technology. Fraudsters increasingly use a large array of techniques to tamper with an organization’s control framework. But by investing in dynamic risk profiling, an organization reinforces its resistance to such activities.

Due to the huge amount of data available on fraudulent accounts and fraudsters, dynamic risk profiling
requires a technological framework with capabilities for data optimization, text and data mining, predictive analytics, forecasting, and so on. It should also be able to help businesses make decisions quickly to enable early recognition and containment of fraudulent attempts.

Leveraging Big Data Analytics Framework for Risk Profiling

Predictive analytics fueled by Big Data provides the right technological framework to contain the threat of fraud in today's digital environment. Analytics helps in effective and accurate decision making by providing insights into real-time and high frequency information, which is usually hidden and difficult to discern.

Below, we outline the structure and relevant focus areas of our recommended technology framework for dynamic risk profiling.

Identification and Definition of Different Classes of Risk

The very first activity in dynamic risk profiling is to list the risk classes and the rules for cataloging them. It involves these steps:

- The rules can be built as characteristics of the account or account holder. These can be location, types of transactions, threshold on transaction value, value of each transaction, type of product selected for effecting a transaction, and so on.
- These traits are assigned real-time weightage on a scale of 0-10 to tag the account to different classes of risk.
- Risk classes are created based on the product of the trait's severity, and its weightage.

Implementation of Risk Behavior Analysis

After the risk classes have been created, the organization can implement risk behavior analysis with these steps:

- Create risk clusters for accounts or profiles in similar risk classes.
- Identify the expected behavioral pattern for the risk cluster based on the history of activity in the cluster and the real-time transactions in the accounts.
- Compare the actual behavior in an account with the identified pattern for the risk clusters to identify variations.
- Redefine the risk classification traits on a dynamic basis based on this gap analysis of behavior and identification of high-risk accounts or activities.
The process of building a technology framework for profiling high risk accounts can be complex. Large volumes of data need to be handled during the profiling exercise. This calls for the power of Big Data and three different models of analytics—predictive, descriptive, and decision models. Figure 2 illustrates the technology ecosystem of the proposed framework for dynamic risk profiling.

The framework consists of four key layers:

**Ingestion Layer**

Data from multiple sources is imported into this layer and standardized for use across the framework.

For instance, discrete data belonging to financial institutions (FIs) may be downloaded from the front-end banking platform. These FIs might have the history of the customer and transactions processed in the account in the form of SWIFT messages or mass files of transactions.
Management Layer

In this layer, data is altered, processed, and manipulated based on pre-defined rules, while maintaining its quality, integrity, and security.

For instance, for a particular account, the database of the FI can provide details on both the history of the customer and the 'know your customer' (KYC) information using correlation techniques. This method collates and combines data from multiple data sources for a given account at any point in time.

Analytics Layer

This layer involves the use of data mining rules or algorithms using predictive and descriptive analytics techniques.

Predictive analytics models can be built by integrating predictive analytics with data mining techniques. The models are based on predictors—variables that are identified, measured, and used to predict the behavior of an account or entity. The risk class identified for a cluster is the output of the predictive model, which uses business rules based on the database, company policies, customer behavior, and the expectations of the FI performing the risk profiling.

Descriptive analytics can be used to create a model for grouping accounts based on forensic and real-time data.

Real-Time Stream Processing Layer

This layer generates action triggers or alerts based on the application of decision analytics or decision engineering techniques.

A decision model can be used to create decision logic based on Big Data, the outcome of the predictive modeling, and the decisions that go into predictive and descriptive analytics. The model takes the key data elements, along with the relationship between elements, and predicts the outcome of the decisions. As a decision model is an axiomatic system, any number of rules can be built based on the forensic and real-time data of any number of accounts or set of accounts.

Decision engineering based on machine learning techniques can be used for generating triggers or alerts. This makes the system robust and dynamic, and facilitates the creation of dynamic risk profiles for accounts.
The Advantages of Leveraging a Big Data Framework for Dynamic Risk Profiling

With the capability of supporting and testing different variations in data and information, the proposed Big Data framework for DRP enables swift detection of patterns in fraudulent attempts. Here are a few other benefits of leveraging this framework:

**Effective prediction and countering of fraud:** Predictive analytics employed in the Big Data DRP framework enables high probability prediction for proactively identifying and countering fraud. It enables organizations to continuously and comprehensively track the latest fraud trends, customers and their behavior, and any likely attempt at fraud. They can do all these without compromising the performance of their systems or affecting genuine customers.

**Secure management of sensitive data:** Efficiently handling the process of storing, processing, and transporting highly sensitive data is a priority of the DRP framework. Data can be flagged against perpetrators without compromising the safety of the data being stored, monitored and transported. A large volume of customers and stringent security requirements can be served easily with this built-in feature of the framework.

**Easy modifications to existing technology framework:** The DRP framework employs Big Data for predictive analysis and ensuring continued relevance. The ease of updating or adding to the technological framework precludes the cost of building a new system from scratch.

**Creation of customized risk management plans:** The DRP framework makes it easy to create personalized risk management plans and solutions for various accounts and account holders based on the risks they face.

**Simplification of analytical processes:** A DRP solution with an underlying technological framework frees investigators and data analysts from tedious work, while simplifying the process of visualizing and drawing insights from the data.
Conclusion

Leveraging Big Data and analytics helps in developing next-generation applications and services that create value and security for the customer. When used innovatively, they increase the efficacy of businesses, while reducing their operating costs.

Successful deployment of the proposed framework depends on the organization’s commitment towards adding value and building a culture that promotes risk intolerance. The buy-in and involvement of senior management, high level of usability, and the availability and integrity of data and sources used are other key success factors. The ecosystem should also be designed to be sensitive and flexible enough to adapt to new regulations, changes to existing law, and the ever-changing endeavors of fraudsters.

A scalable, secure, and cost-effective plug-and-play Big Data component can reduce false positives, thereby reducing the risk management cost and fraud-related losses for companies. The framework helps institutions to move from monitoring fraud attempts to anticipating and preventing them. Big Data makes it relatively easy to pinpoint fraudulent attempts in a sea of legitimate transactions.
About TCS Business Process Services Unit

Enterprises seek to drive business growth and agility through innovation in an increasingly regulated, competitive, and global market. TCS helps clients achieve these goals by managing and executing their business operations effectively and efficiently.

TCS’ Business Process Services (BPS) include core industry-specific processes, analytics and insights, and enterprise services such as finance and accounting, HR, and supply chain management. TCS creates value through its FORE™ simplification and transformation methodology, backed by its deep domain expertise, extensive technology experience, and TRAPEZE™ governance enablers and solutions. TCS complements its experience and expertise with innovative delivery models such as using robotic automation and providing Business Processes as a Service (BPaaS).

TCS’ BPS unit has been positioned in the leaders’ quadrant for various service lines by many leading analyst firms. With over four decades of global experience and a delivery footprint spanning six continents, TCS is one of the largest BPS providers today.

Contact

For more information about TCS’ Business Process Services Unit, visit: www.tcs.com/bps
Email: bps.connect@tcs.com

Subscribe to TCS White Papers

Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

IT Services
Business Solutions
Consulting