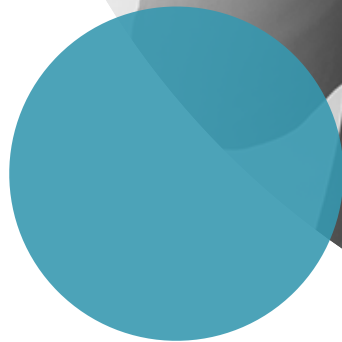# Leveraging AI & Machine Learning in Designing Anti Money Laundering (AML) Framework

Perspectives from Indian Banking Industry

wipro

1.0 Introduction

Know-Your-Customer (KYC) and anti-money laundering (AML) are in the limelight globally since some large banks were hit with hefty penalties in 2012. Regulators in the United States and Europe have imposed $342B in fines on banks since 2009 for misconduct, including violation of AML rules, and that is likely to top $ 450B by 2023. Despite several analytical platforms, tools and applications being available for AML transaction monitoring, there has been an increasing incident of penalties levied on the banks in India and abroad for non-compliance with the AML guidelines[1].

In 2016, the Reserve Bank of India (RBI) had imposed INR 270M in fines on 13 Indian banks for violating KYC norms and 8 other banks were advised to put appropriate measures in place, and had reviewed from time to time to ensure strict compliance of KYC requirements[2]. As of August 2019, RBI has imposed INR 265M in fines on banks for non-compliance with its directions relating to opening/ operating of accounts and end-use monitoring of funds. This has triggered a flurry of initiatives across the banking sector to boost compliance both in India and abroad.

Most of the financial institutions (FIs) rely on a system of rules and procedures targeted for acquiring knowledge about their customer and their activities. However, money launderers have come out with alternatives to cover their activities, that a traditional rule-based system might not be capable enough to detect. It results in non-detection/ non-reporting of the suspicious transactions; leading to non-compliance with the AML/KYC regulations. This may result in both financial and reputation loss. Therefore, it is of utmost importance for banks to establish a reliable set of controls, allowing them to identify monetary activities and transactions even when the money launderers are using the best of their ability to circumvent the rules. One of the promising ways is to use an AI & ML driven AML transaction monitoring system.

2.0 Traditional process – Anti-money Laundering (AML) transaction monitoring

The traditional process performs routine scans for transactions based on pre-defined rules and flags that meet the criteria of those rules for the purpose of further investigation. These rules generally fall in the following categories of scenarios:
• Anomalies in behavior
• Transaction patterns
• Hidden relationships
• Credit, debit and bank cards
• High risk entities

Alerts generated out of these rules are then investigated by a bank's operations team, which is set up for conducting a detailed review/ investigation. Based on the outcome of the investigation, they are either closed considering false positives or reported as suspicious transactions.

[1]https://www.reuteINRcom/article/us-banks-regulator-fines-idUSKCN1C210B
[2]https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=37618

2.1 Drawbacks of the traditional AML transaction monitoring

- **Increased operational cost**

  Per industry estimates, as much as 90 to 95% of the alerts generated by the traditional AML system are false positives[3]. This requires substantial workforce to analyze such alerts and take subsequent action. Each alert needs careful analysis, as any non-compliance in identification and reporting of the suspicious transaction can lead to huge financial and reputational loss to the bank. Thus, there is a need for adequate staffing depending upon the bank's size and volume of alerts generated.

- **Lack of AML system capability to detect new scenarios**

  Considering the fast evolution and new number of ways / techniques emerging for money laundering by fraudsters, there is an urgent need to constantly evaluate the transactions and external factors and identify new scenarios. Any delay in the detection mechanism would result in the system's inability to detect the suspicious transaction; thus resulting in non-compliance of the regulatory prescribed guidelines.

- **Identification of new scenarios**

  These are identified based on the human analysis of the past events. This requires strenuous manual work, yet there are chances that some scenarios are missed out or not completely captured due to lack of robust data analysis.

Despite the efforts taken by the banks, the level of undetected suspicious transaction remains high. Thus, to overcome various shortcomings, banks are evolving from the traditional approach towards advanced approaches involving AI & ML enabled technology for transaction monitoring and complying with the stipulated AML guidelines.

3.0 Contemporary fraud risk models: Leveraging AI & ML

AI & ML facilitate continuous advancement of computing through exposure to new scenarios, testing and adaption, while employing pattern and trend detection for improved decisions in subsequent (though not identical) situations. Also, ML includes techniques, approach and tools that produce actionable insights from the data that can be used by an investigator for further investigation, which can lead to reporting a suspicious transaction or identifying a new fraud pattern. This enables the capability to update the rules to identify and monitor suspicious transactions on a real time basis.

[3]https://www.acfcs.org/wp-content/uploads/2019/12/AI-and-FinTech-Richards-RegTech-Consulting-LLC-ACFCS-Seminar-December-5-2019.pdf

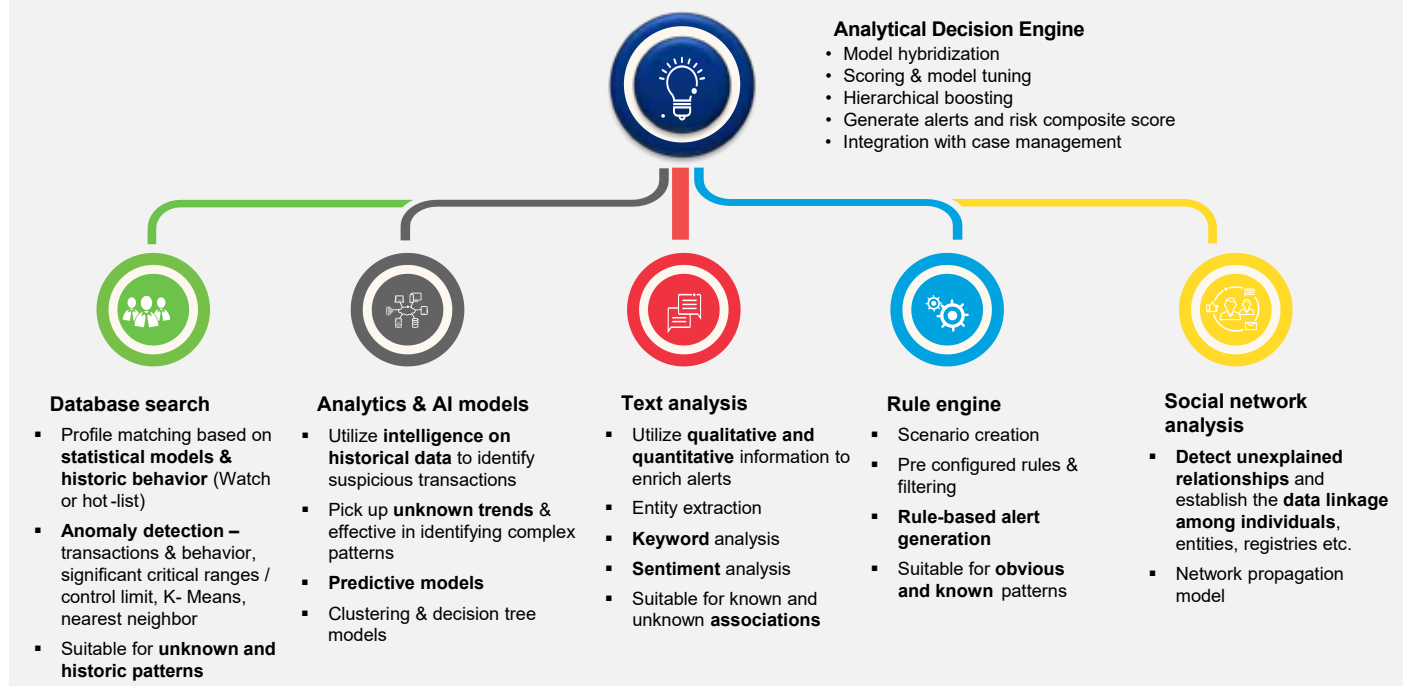**Contemporary Fraud Risk Models : Leveraging AI & ML**

Analytical Decision Engine
- Model hybridization
- Scoring & model tuning
- Hierarchical boosting
- Generate alerts and risk composite score
- Integration with case management

Database search
- Profile matching based on **statistical models & historic behavior** (Watch or hot -list)
- **Anomaly detection –** transactions & behavior, significant critical ranges / control limit, K- Means, nearest neighbor
- Suitable for **unknown and historic patterns**

Analytics & AI models
- Utilize **intelligence on historical data** to identify suspicious transactions
- Pick up **unknown trends** & effective in identifying complex patterns
- **Predictive models**
- Clustering & decision tree models

Text analysis
- Utilize **qualitative and quantitative** information to enrich alerts
- Entity extraction
- **Keyword** analysis
- **Sentiment** analysis
- Suitable for known and unknown **associations**

Rule engine
- Scenario creation
- Pre configured rules & filtering
- **Rule-based alert generation**
- Suitable for **obvious and known** patterns

Social network analysis
- **Detect unexplained relationships** and establish the **data linkage among individuals**, entities, registries etc.
- Network propagation model

Figure 1: Proposed fraud risk model

4.0 Research Methodology and Case: A consultative approach adopted by 3 MNC banks

This case elucidates the AML and fraud risk deployment story of 3 reputed multinational banks that have been carrying out consumer banking activities perinstructions by the RBI. These banks had faced huge reputational and financial impact on account of non-compliance with financial crime guidelines. Due to restrictions in usage of customer data, privacy and confidentiality clauses, we have not illustrated the exact implementation details of the proposed approach. However, we have shared a holistic view within the permissible level of disclosures.

In this paper, we illustrate, through case studies, how a global IT and consulting firm efficiently incorporated AI & ML enabled fraud score and financial crime prevention models for three multinational banking clients, and achieved compliance with guidelines stipulated by the RBI.

4.1 Business Challenges

- All these banks had legacy source as well as financial crime detection systems.
- The source systems were either outdated or not helpful for analytics or decision sciences.
- The need of the hour was to build a host of efficient AML, fraud detection and deterrence models, including externally available data to reduce the lead time.
- The top management of all three banks was interested to build capacity to effectively manage data & insights, and produce quality insights for management.

4.2 Solution Deployed

Considering the fast evolution and new number of ways / techniques emerging for money laundering by fraudsters, there is an urgent need to constantly evaluate the trans actions and external factors and identify new scenarios. Any delay in the detection mechanism would result in the system's inability to detect the suspicious transaction; thus resulting in non-compliance of the regulatory prescribed guidelines.

Adopted Approach:

- **For obvious and known patterns:** Configured a set of pre-defined rules and scenarios
- **For unknown and historical patterns:** Devised profile matching and anomaly detection techniques
- **For complex patterns:** Data scientists have built predictive models using pools on historical data and decision trees

- **For known and unknown associations:** Extensively used social network and text analysis, streamlined the alert and the case management system

4.3 Business Benefits

The new system provided greater flexibilities with limited resources to support the end-to-end financial crime transaction monitoring process.

Easy navigation, money laundering patterns analysis with several pre / custom-built visualization and identity relationship and resolutions patterns, integrated case management and reporting, rules repository, online rules definition capability etc. enriched the operations.

4.4 Advantages

Easy navigation, money laundering patterns analysis with several pre / custom-built visualization and identity relationship and resolutions patterns, integrated case management and reporting, rules repository, online rules definition capability etc. enriched the operations.

- **Reduce false negatives:** An unsupervised ML model does not need large historical datasets and can find unusual transactions that are not obvious to human analysts. The technique can adapt and change to newer patterns as and when they emerge.

- **Reduce false positives:** ML algorithms probed in auto closing the false positives. Once the alert is generated, ML can then be used for understanding the customer
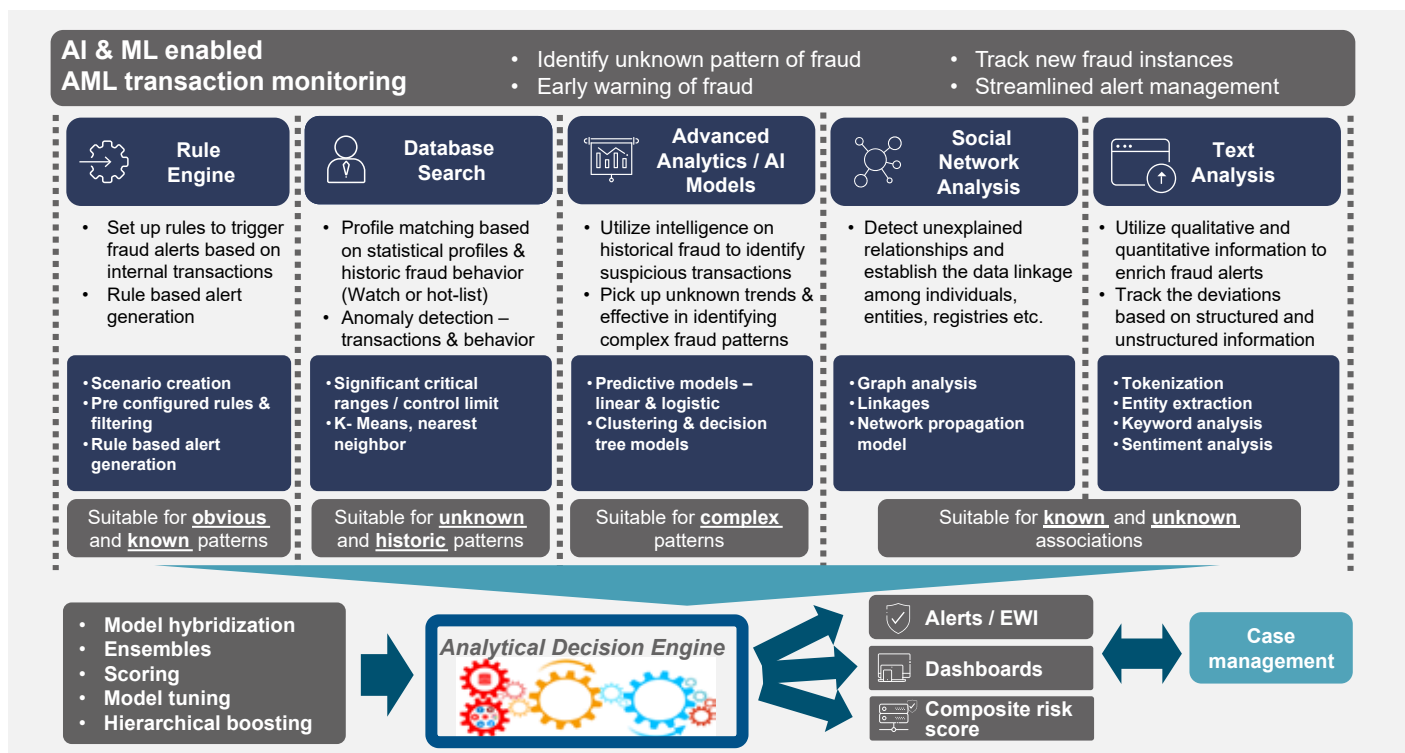
Figure 2: Deployed AI & ML enabled financial crime management system at the respective banks

risk profile and the risk alert score. As per the revised grid, in case the alert risk score is below the defined threshold; then the alert gets addressed in auto-pilot mode.

• Prioritize alerts:

The newly devised models helped in prioritizing the workflow queues for the transaction monitoring system so that the alerts could be acted on more efficiently, and in a timely manner.

• Increase effectiveness and efficiency:

The continuous learning process (by the scorecards) helped in incorporating any new pattern of fraud into the monitoring system on a timely basis and thus increased the effectiveness and efficiency of AML transaction monitoring and regulatory compliance.

4.5 Challenges faced during implementation process

• Huge amount of data:

ML algorithms were trained by using large amounts of data. The more accurate the results expected, the more number of parameters needed to be fed, which in turn needs larger amount of data. Lack of quality historical data would influence the outcome of the ML algorithms.

• Complexity:

ML is a relatively new technology, with some techniques like neural networks relatively unknown. In the present case, the data scientists of the consulting firm knew the model parameters and the data that were fed into the neural networks. However, in general banks have had a hard time in understanding how the system could arrive at the conclusion. The operations of the neural networks are invisible to humans and thus it restricts the usage especially for areas where verification of the process is important.

- **High performance hardware:**
  ML requires tremendous amount of data for the purpose of training and building the algorithm. To handle such data, ML needs to be equipped with high processing power. To achieve efficiency and reduce time consumption, multi-core high performing processing units were used that consumed a lot of power and were costly.

5.0 Conclusion and Recommendations

Across the world, regulators are holding financial institutions answerable for the magnitude of failures in management of financial crime. Averting money laundering is no easy feat, not with both the criminal environment, and product and service risks posing as main hindrances[4]. Risk managers and data scientists with limited practical research experience might not foresee the challenges in implementing a sturdy financial crime management system and protocols in combating modern day techniques of fraud risk and money laundering adopted by hackers and criminals.

One, these issues become intensified in the context of adaptation of a machine learning enabled risk management system, fraud prediction models and scorecards.

Two, in response to a RTI filed in 2020, the RBI stated that the total number of frauds reported by scheduled commercial banks and select FIs during Financial Year 2019-20 was 84,545 and the amount involved therein was INR 1,85,8 Bn. However, RBI did not have any information about the number of bank employees involved in fraud cases and the amount involved. Irrespective of the predictive power of these models, it is essential to have a control mechanism over internal stakeholders (including staff, contract employees etc.) as a major proportion of such crimes happen due to lapses in internal systems; including staff.

Three, it is high time financial institutions reconfigure their alert and transaction monitoring programs to identify the rudimentary to super-complex, multi-dimensional money laundering and terrorism finance methods that are defeating today's rules-based detection scenarios. Adopting an actor-centric hybrid threat finance (HTF) model can cut compliance costs, reduce risk, improve regulatory relations, and increase the usefulness of suspicious activity reports[5] .

Four, it may be too idealistic to ask financial institutions to balance two roles (execution of a seamless and lightning-fast customer resolution versus having a dynamic financial crime and anti-fraud management process in the background). It is an arduous task to meet compelling customer demands, provide 24*7 surveillance, deploy advanced cyber forensics, and at the end of the day save money and retain customers.

---

[4]https://www.theasianbanker.com/updates-and-articles/what-banks-must-do-to-prevent-money-laundering
[5]Thomson Reuters Anti-Money Laundering Insights Report 2019

Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**