INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 8, Issue 1 - V8I1-1423)
Available online at: https://www.ijariit.com

Jocata Grid: To study Artificial Intelligence (AI) used for fraud detection and reduction in False Positive

Sahil Sharad Patil
sahils1314@gmail.com
University of Westminster, London, England

"Artificial intelligence is one of the most profound things we're working on as humanity. It is more profound than fire or electricity"

-Sundar Pichai

ABSTRACT

Fraud detection in today's arena presents numerous challenges since fraud instance being present in all sources and walks of life. Technological innovations have always proven boon for Financial Crime and Compliance Industry with the ascent of big data and man-made consciousness, new freedoms have emerged in utilizing progressed AI models. With renewed promises to fight frauds and other financial crimes, it is imperative to look at intelligent solutions that can prevent and detect internal frauds. With regulators encouraging the use of advanced technologies like analytics, machine learning (ML) and other forms of artificial intelligence (AI) in managing FinCrime risks. We summarize our findings in the research for reduction in False Positives and to increase efficiency of fraud detection and conclude by deriving key values created and captured from our analyses.

Keywords: *Fraud, Financial Crime, Big-data, False Positive, Artificial Intelligence.*

1. INTRODUCTION

1.1 Artificial Intelligence

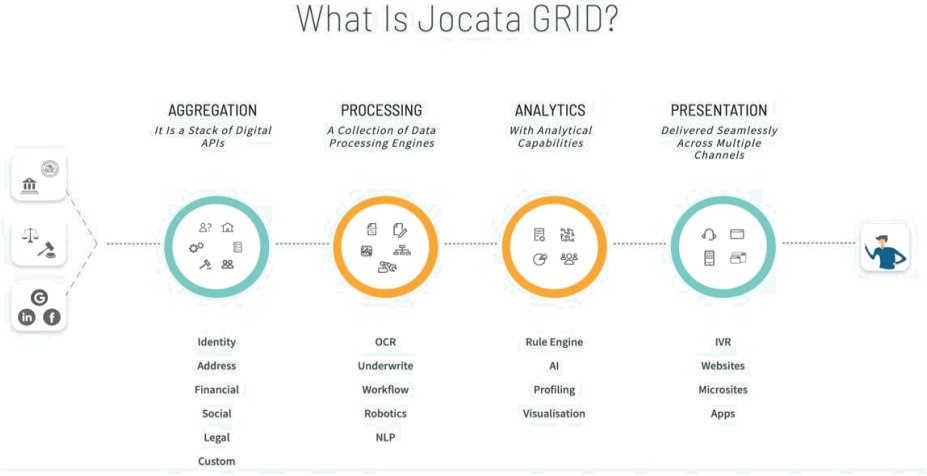
McKinsey defines AI "as the ability of a machine to perform cognitive functions we associate with human minds, such as perceiving, reasoning, learning, and problem solving" (McKinsey, 2018, p.1). Two main branches of artificial intelligence pervade. The first is machine learning, encompassing a range of algorithms falling into three learning techniques: supervised, unsupervised and reinforcement. Machine learning algorithms are different from traditional programmatic algorithms, rather than receiving direct commands, they use data and past computations to take decisions, detect patterns and make predictions.

With new data and patterns algorithms are able to adapt and learn overtime (McKinsey, 2018p.1). The second branch is deep learning. This more sophisticated type of artificial intelligence "can process a wider range of data resources, requires less data pre-processing by humans, and can often produce more accurate results than traditional machine learning approaches" (McKinsey, 2020, p6.).

1.2 Jocata Financial Advisory Service

Jocata GRID is a sophisticated enterprise ecosystem technology platform that strives to provide an integrated real-time view of business, risk, operations and compliance. It is designed as a multi-layered stack of technology capabilities that help financial institutions in their digital transformation initiatives, with each layer solving a specific challenge.

Although the individual feature sets of the GRID are mapped to discrete products, its architecture allows for them to be deployed separately or all together or in specific combinations, depending on your solution requirements. The GRID plugs into your backend systems through a secure interface, and brings you the benefits of Jocata's cutting-edge software while substantially reducing upfront costs for training, setup, and infrastructure. (Jocata Grid,2010)



(Source: Jocata Grid. 1)

3. OBJECTIVE

The Objective of this study encompasses use of AI Technology to:

- Analyse issues rosining in Real Time Fraud detection
- Reduction in False Positive
- Study Value created and value captured with use of Artificial Intelligence for Jocata

4. TYPE OF RESEARCH

This is type of Applied research.

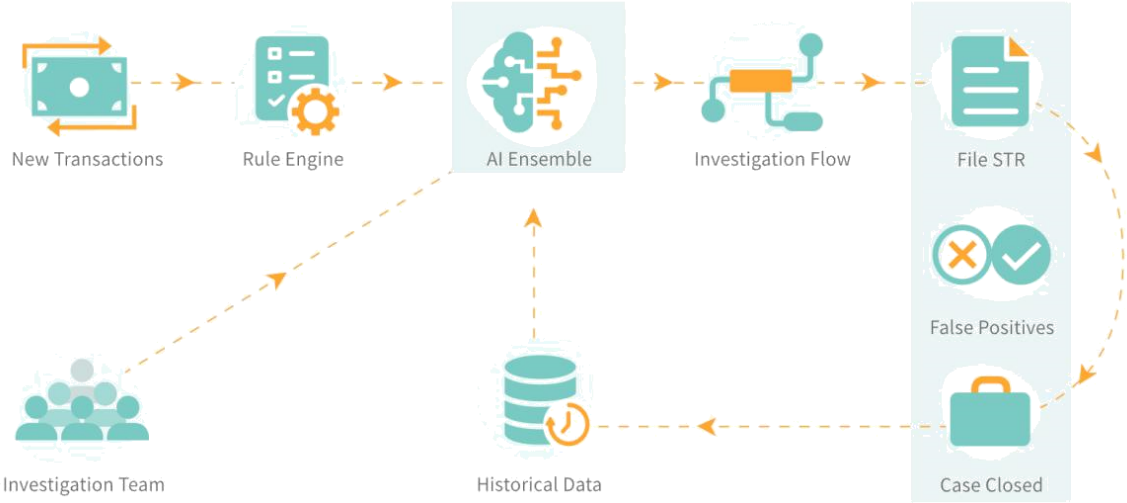
Applied research "aims at finding a solution for an immediate problem facing a society, or an industrial/business organisation, whereas fundamental research is mainly concerned with generalisations and with the formulation of a theory (John Dudovskiy).

5. ISSUE IN TECHNOLOGY

The current issues and challenges faced in technology leading to Financial Crime and Compliance are numerous out of which few identified are considered for study:

- Extremely High False Positive
- Missing insights from unstructured data
- Lack of insight from analytics
- Outdated rule-based detection
- Delayed alert Mechanism leading to increased fraud

The current system flow below shows lower closure of False positive cases and closure of case as Fraud/Not a fraud/Not eligible with normal transaction allowing multiple cases generated for same account based on the Customer Identification Number, Credit card number, debit card number and multiple dimensions of deposits and withdrawals from non-base locations.

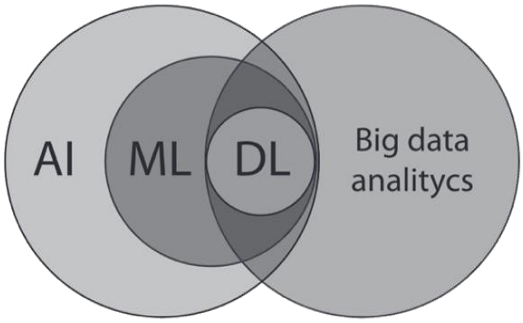


(Source: Jocata Grid. 2)

6. TECHNOLOGY REVIEW

Artificial Intelligence major head, one of its parts is Machine learning:

- A branch of artificial intelligence that aims to teach computers how to perform tasks with data without the use of explicit programming.
- ML uses numerical and statistical approaches inclusive of artificial neural network to encode learning in models



(Compiled by researcher)

- Supervised learning is a machine learning approach that's defined by its use of labelled datasets. These datasets are designed to train or "supervise" algorithms into classifying data or predicting outcomes accurately. Using labelled inputs and outputs, the model can measure its accuracy and learn over time. The algorithm "learns" from the training dataset by iteratively making predictions on the data and adjusting for the correct answer. While supervised learning models tend to be more accurate than unsupervised learning models, they require upfront human intervention to label the data appropriately. In supervised learning, the goal is to predict outcomes for new data. You know up front the type of results to expect. Supervised learning models are ideal for spam detection, sentiment analysis, weather forecasting and pricing predictions, among other things. (Julianna Delua, March 2021)
- Since organized crime tactics are so clever and adaptable, defensive efforts based on a single, one-size-fits-all analytic methodology will fail. Expertly developed anomaly detection approaches that are optimal for the situation at hand should be supported by each use case. As a result, both supervised and unsupervised models are critical in fraud detection and must be integrated into complete, next-generation fraud tactics. A supervised model is one that is trained on a large number of correctly "labelled" transactions, which is the most frequent type of machine learning across all fields. (Ashesh Anand, September 2021)

7. SOLUTION TO HOW THE ISSUE CAN BE SOLVED/FIXED

Within artificial intelligence (AI) and machine learning, there are two basic methodologies: supervised learning and unsupervised learning. The differentiating factor is one uses labelled data to help predict outcomes, while the other does not. Nonetheless, there are some distinctions in two approaches, and key areas in which one outperforms the other.

The issue can be fixed using supervised AI Models for False Positive reduction and fraud detection

(a) AI has emerged as a significant tool for avoiding financial crimes due to its increased efficiency
(b) When fraud is suspected, AI models may be used to reject transactions altogether or flag them for further investigation, as well as rate the likelihood of fraud, allowing investigators to focus their efforts on the most promising instances
(c) Enhanced rule based matching techniques with data accuracy, use of Fraud intelligence data base to evaluate risk of fraud, thereby data enrichment
(d) Behaviour/ profile-based rule modelling can significantly help in reducing false positive which will indeed suppress repetitive alerts and will trigger high risk alerts in the system.
(e) False positive reduction modelling: Each transaction is assigned to one of two categories: fraud or non-fraud. In order to discover patterns that best reflect lawful activities, the models are trained by consuming huge quantities of labelled transaction information. Innovation in existing data set and use of various new technology of AI to captivate and detect maximum fraudulent transaction and money laundering activities
(f) Risk assessment is vital part when considering reduction of false positive as it impacts the number and quality of alerts, if at all any suspected fraud missed out in false positive case can lead to regulatory authority intervention to the financial institution and may be penalised for the same.
(g) Instance of case of detection and interdiction, the output of many algorithms is a score that predicts the risk level associated with a situation. However, users have to be clear about what is being predicted. In many cases, the algorithm will detect anomalous transactions (i.e., those that are different from an expected benchmark), but an anomalous transaction does not necessarily mean a problematic transaction. If the analysis is not conditioned properly, the lack of apparent anomaly can be problematic. (Yang Bao, Nov 2020)

8. FINDINGS

Evaluation of technology based on Criteria to evaluate A New Technology (Vera Solution, October 2019)- Jocata in FinCrime and False Positive reduction

Criteria for evaluation	Observations
Features	System integrates seamless and easy of fraud detection with use of human intervention and technology, this also has analytical tool function to check the data use and enhances better predictability of fraud. The amount of clean, relevant training data used in the development of a supervised model is closely connected to model accuracy.
Security	AI to detect fraud has aided businesses in improvising internal security and simplify corporate business operations (Ashesh Anand, September 2021). The data used for monitoring is protected and governed by financial institutions with the Jocata software provider as the data involves financial transaction, history of individual, source of income

	and much more personal data. Handling this data securely can be challenging based on the servers of institutions. Breach of data security can impose fine and lead to issues in financial environment. Thus, it is mandatory for software provider and the financial institution to have data security maintenance agreement in place.
Privacy	Using behavioural analytics, machine learning is used to analyse and predict behaviour at a granular level across all aspects of a transaction. The data is tracked using profiles that describe the habits of each user, merchant, account, and device. With each transaction, these profiles are updated in real-time, allowing analytic features to be computed that provide accurate forecasts of future behaviour. The profiles include information on both financial and non-financial transactions. Non-monetary transactions include address changes, requests for duplicate cards, and recent password resets (Ashesh Anand, September 2021) Financial transaction data aids in the development of patterns that may indicate an individual's average expenditure velocity, the hours, and days when they tend to transact, and the time duration between geographically dispersed payment sites. Profiles are extremely beneficial because they provide an up-to-date picture of activity, which can aid in the prevention of transaction abandonment.

(Compiled by researcher)

9. VALUE CREATION AND VALUE CAPTURE FOR USING AI FOR JOCATA

Benefits of Machine Learning in Fraud Detection and false positive reduction:

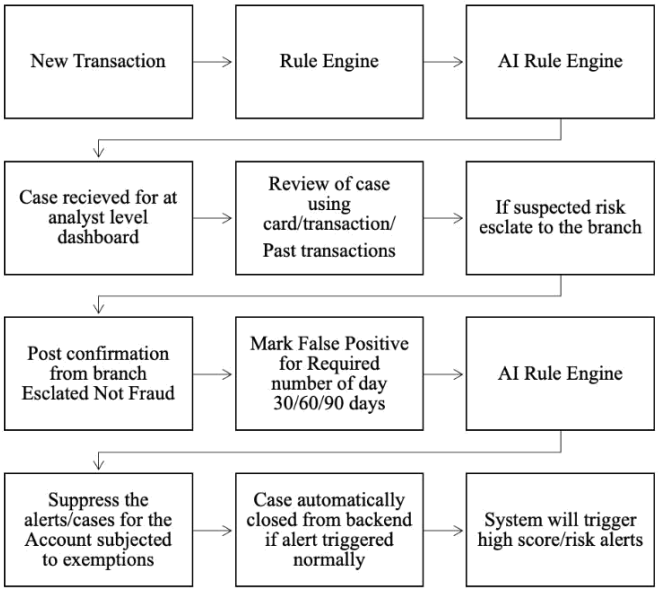
- Faster & efficient detection
- Increased Accuracy
- Better Prediction & classification
- Reduced financial & reputational loss
- Reduced sophisticated fraud across channels
- Reduced false positives
- Regulatory compliance
- Enables real-time employee or internal fraud prevention and protects financial institution against core-banking frauds like customer, and account level frauds.

Value Creation and Value Captured

Value Creation Value creation refers to the total additional benefit created in transforming the input to output	**Value capture** Value capture refers to your ability as a business to 'capture' that value yourself, as your retained profit.
• Value created by technology are increase in compliance and security of financial transaction of the financial institution • Reduction in human interference in the process of FinCrime and Compliance • Improvisation in quality of alerts due to reduced false positive • Labelling of rules so that alerts are processed accurately • We tried assessing AI maturity level • Value created using evaluating need for AI Rule engine • Value created by assessing industry readiness • AI aids cost efficiency for the system implementation • Overall process improvement	• Financial rewards in form of increased revenue to the organization • This technology provides add on security with data maintenance • Financial penalties can be avoided if the technology is placed in the financial institution • Since the financial penalties are not levied on organization it will also foster and increase brand image of the financial institution • Value captured by competitive edge using ML since technology aided • Value captured using risk assessment at all stages

(Compiled by researcher)

10. PROPOSED SOLUTION FOR FALSE POSITIVE FRAMEWORK



(Compiled by researcher)

11. FUTURE RESEARCH DIRECTIONS

I believe that it would be a fruitful for future research to combine the knowledge and expertise from both the financial crime and machine learning domains to develop more powerful and adaptive learning models for value offerings. In particular, I believe that the following interdisciplinary challenges deserve vital attention to such problems for integration of supervised learning in fraud detection and reduction in false positives. The research could have a positive influence on future similar academic research of FinCrime and Compliance management.

12. RECOMMENDATIONS

- It's the responsibility of the Governments to use their regulatory authority to ensure that financial institutions have acceptable risk profiles to prevent large-scale defaults, and customers are not using financial institution to commit financial crimes. Financial Institution must comply with regulations requiring them to know their customers, uphold customer privacy, monitor & prevent money laundering and other fraud.
- Machine learning-based behaviour profiling and detection of anomalous activity –hybrid model that combines a traditional rule-based platform with an ML-based customer behaviour profiling and anomaly detection platform can improve the quality of fraud detection in financial institutions by behaviours based on static scenarios, flagged up for threshold violation. In fraud detection algorithms, from a data protection perspective, with focus on the intrusiveness of the data collection, processing, and transfer and storage of data securely.

13. LIMITATIONS

The research limits to the financial crime and compliance challenges faced in Artificial intelligence and Machine learning in India and limits to Jocata software only. The software being used at National level presently across banking and financial institutions in India.

14. CONCLUSION

- The goal of this research is to reduce the number of false positives in internal fraud detection by contributing to existing fraud detection framework used by Jocata
- Fraud is adversarial, Machine-learning techniques work best when patterns are stable, fraud detected previously can be stored in data set to understand techniques and transaction pattern thereby allowing to make decision for reduction in false positive for account/customer.
- False positive should work on account level basis and not on transaction basis so one account multiple transaction should only trigger one single case/alert and works on account basis
- The research results can be applied in FinCrime and Compliance domain development by financial institutions.
- Value created by Artificial intelligence technology for Jocata is improvised efficiency and process
- Value captured by AI for Jocata is increased revenue for the organization and reduced penalties from government bodies.

15. REFERENCES

[1] McKinsey. (2018). An Executive Guide to Machine Learning 2018. McKinsey & Company,[online] Availableat:https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/An%20executives%20guide%20to%20AI/An-executives-guide-to-AI.ashx. [Accessed: 04 Dec. 2021].

[2] McKinsey. (2020). The state of AI in 2020. McKinsey & Company. [online] Available at: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020. [Accessed: 04 Dec. 2021].

[3] Julianna Delua. (12th March 2021) IBM Supervised V/s unsupervised Learning: What's the difference? Available at: https://www.ibm.com/cloud/blog/supervised-vs-unsupervised-learning#:~:text=Supervised%20learning%20is%20a%20machine,accuracy%20and%20l earn%20over%20time [Accessed: 23rd Dec. 2021].

[4] Vera Solution, 10 Criteria to evaluate When Choosing a New Technology https://www.verasolutions.org/10-criteria-to-evaluate-when-choosing-a-new-technology/?locale=en [Accessed: 23rd Dec. 2021].

[5] Ashesh Anand. (21stSeptember 2021) How is used in Fraud Detection? https://www.analyticssteps.com/blogs/how-ai-used-fraud-detection [Accessed: 25th December. 2021].

[6] Yang Bao, Gilles Hillary, Bin KE. (24th November 2020). Artificial Intelligence and Fraud detection.

[7] Nenad Milojevic and Sridjan Redzepagic (27th November 2020).Prospects of Artificial Intelligence and Machine Learning Application in Banking Risk Management. UDK: 336.77.067.

[8] Sundar Pichai. (2020) Artificial Intelligence Available at: https://www.forbes.com/sites/robtoews/2020/03/28/12-thought-provoking-quotes-about-artificial-intelligence/?sh=7b5c45e27d26 [Accessed: 02nd January 2022].

[9] C. R. Kothari (2008) Research Methodology: Methods and Techniques [ISBN: 9386649225] (16th January 2018). The key to reducing False Positives in fraud detection systems Available at: https://www.synectics-solutions.com/our-thinking/reducing-false-positives-in-fraud-detection-systems [Accessed: 5th January. 2022].

[10] Galina Baader and Helmut Krcmar (December.2018) Reducing false positives in fraud detection: Combining the red flag approach with process mining (IJAIS) Available at: https://www.sciencedirect.com/science/article/pii/S146708951630077X

[11] John Dudovskiy. Business Research Methodology, Applied Research Available at: https://research-methodology.net/research-methodology/research-types/applied-research/ [Accessed: 5th January. 2022].

[12] Barney, J. B. (1999). How a firm's capabilities affect boundary decisions. MIT Sloan Management

