Use of AI Algorithms to solve Societal Problems

Chakradhar Reddy Donuri

E949F496

Technology has helped communities across the globe tackle the most urgent issues and solve social problems. By offering rapid technical progress, artificial intelligence (AI) aims to provide answers to the economic, security, and society-related questions we are all addressing today. There's no doubt that AI is in the process of transforming the environment as we know it.

Intelligence can be built in three ways. They are

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

In Supervised Learning, The data used and the desired output are given in the algorithm. For example, if we give a set of colors and then train them to recognize a specific color which is the required output then they follow the data and display the required output.

In Unsupervised Learning, some random data are given to the algorithm, and it is trained to find the most repetitive data collection. For Instance the e-commerce website.

In Reinforcement Learning, the algorithm interacts with the changing world and provides feedback on incentives and sanctions. For instance, if we take a self-driving car, if the data is the road, it stays on the road and if it turns right or left

In this paper, we are going to discuss the algorithms used to find Fraud Detection for safer banking.

Fraud detection solutions operated by systems based on artificial intelligence (AI) will significantly enhance safety across the banking sector. By rising the accuracy of fraudulent activity alerts, banks dramatically reduce the time and expense of security breaches and maintain a reputation for the brand

AI-based fraud detection systems function better when taught by a person and with knowledge and example of what to do and what not to do should be taught in a similar way as a person. AI systems, however, are learning more scalable than human counterparts. AI-enabled fraud detection systems are implementing and learning to recognize new trends and forms of fraud by ingesting continuous volumes of data.

Let's look at several ways banks can use AI-based technologies to prevent fraud.

Anomaly detection

The most growing and basic layer of fraud detection is anomaly-based fraud detection. This type of smart model includes an ML-based algorithm to control the continuous stream of transactional data coming in. It is designed to operate exactly as an person does when conducting bank transfers, mortgage loans, and more. Most banks are demanding that anomaly detection be used. AI-based algorithms can identify any unusual activity by monitoring the customer's usage in real time, and detecting any deviation from previous usage patterns.

The model algorithm based on AI is programmed with an alarm system to instantly alert the bank of any deviations from the 'normal' sequence. If fraud is detected, the system will automatically reject the application and in real time warn the bank workers via an app. The AI-based model is trained by observations of purchasing habits to 'comprehend' whether or not the variance detected is a fraud, and on a scale. These AI-enabled applications helped Visa Inc. deter annual fraud estimated at $25B, the company announced in June 2019.

Predictive analytics

Predictive analytics provides an added level of sophistication from anomaly detection. Bank data experts mark vast volumes of transactions as fake or genuine and then execute those transactions to train the AI model. The model uses the knowledge to identify fraudulent transactions quickly.

For example, a fraudulent transaction warning may be provided based on the buying habits and location data of the consumer for a product or service which a consumer has purchased online. The program can flag an object that has never been purchased before but may not be indicative of fraud in and of itself. However, the AI solution will also test the location of a customer supplied with the site of purchase through geo-location data to determine the probability of fraud.

Predictive analytics may also be used as fraudulent to discourage operation from transactions that have been incorrectly flagged. Via its Decision Intelligence and AI Express systems, MasterCard has used predictive analytics to reduce by 50 percent the rate of transactions being reported incorrectly as fraudulent and to deter further fraud. Decision Intelligence uses sophisticated AI algorithms to calculate, rate, and learn from each transaction and to give the card issuer a predictive rate. The scoring is based on smart analysis of large-scale behavioral trends, combined with real account use (location, time, and form of purchase) to accurately detect fraudulent activities.

The fraud detection software based on predictive analytics is used to identify fraud through many digital platforms. These may include payment processes for online transactions and the use of geo-locational data to identify anomalous user activity within banking apps.

Accurate data analysis

This approach to risk-based analytics improves fraud detection through the identification of complex and secret trends. With greater availability and accessible data, AI algorithmic models are the most efficient. The complexity of AI algorithms detected

fraudulent activity increases with the amount of data the more knowledge the model has as sources, the better the ability to identify the variations, patterns, and similarities between multiple data behaviors.

AI-based fraud detection tools take into account several data points not only to identify a fraudulent transaction but also to explain why a customer's account may have been fraudulently compromised. Factors accommodated by AI algorithms include the location of customers and the main contextual data points of each transaction, just to name a few.

AI algorithms can work with real-time and historical bank transactions to block or isolate legitimate transactions from fraudulent transactions, without impacting the customer experience. For banks, this automated method may become more efficient as AI algorithms can allow a more granular analysis of available data to predict the future state as new transactions capture information.

Conclusion and Future Work:

Fraud detection is a complex problem that involves a tremendous amount of preparation before throwing algorithms about machine learning into it. Nevertheless, it is also an activity for the benefit of data science and machine learning, meaning that the money of the consumer is secure and not easily abused.

Future work will require a comprehensive tuning of the algorithm Random Forest. Having a data set of non-anonymized features would make this especially interesting because it would allow one to see what different factors are most relevant for detecting fraudulent transactions to generate the feature value.

References:

[1] L.J.P. Anton Vaisburd is a Data Scientist at SoftServe, Journal of Machine Learning Research

[2] Capitalizing AI for Safer Banking, ULB, Credit Card Fraud Detection , Kaggle