MACHINE LEARNING FOR FRAUD DETECTION

PROF. GAUTAM R. DESIRAJU
PROFESSOR, SOLID STATE AND STRUCTURAL CHEMISTRY UNIT
INDIAN INSTITUTE OF SCIENCE (IISC), BENGALURU, KARNATAKA
EXPERTISE: CRYSTAL ENGINEERING, SUPRAMOLECULAR CHEMISTRY

“Sorting through overly hyped and overly generalised label of machine learning is a key to any successful consideration and implementation of a new fraud analytics solution”.

Detection strategies are shifting from analysing siloed transactional activity to instead making better use of data and analytics, building holistic understandings of customer activity.

By bringing together cross-product and cross channel data and applying nimble machine learning analytics that iteratively optimize results, business can understand the context of transactions and make better decisions.

Progressions in AI technology can streamline workflows and eliminate antiquated dependencies.

Two key advancements in particular can serve to bottle human creativity, drive employees towards more strategic work, and reduce operational bottlenecks.

These trends are: workforce augmentation (doing more complex tasks) and operational machine learning (doing complex tasks more quickly).

Workforce augmentation: organizations are searching for ways to augment their existing workforce by using technology.

The basis for augmentation is in the technological architecture of a system.

More evolved systems can better automate the “janitorial tasks” of data science, like cleaning data and combining data from different sources.

These integrated automation tools drive workers towards increasingly creative and advanced tasks, like analysing data and building predictive models.

Work force augmentation refocuses the data science on interesting work like analysing simulations and iterating on multiple models.

Operational Machine Learning: As a basis for operationalization, organizations are considering their complete risk workflows and dependencies, and seeking ways to optimize them.

OML overcomes the dependency on manual coding from IT, signalling an evolution in the ability to look at more data, from more sources, and make better predictive decisions with less uncertainty, benefits are speed and reliability.

Organizations can significantly accelerate the time to deployment in mission-critical systems, because now what they code, and test is what they deploy.

The most effective OML can inject real-time analytics into their operational routine.

With data science techniques embedded into a tightly coupled with the real-time transactional workflow, running through machine learning models, business intelligence is generated at a higher resolution.

How to bring machine learning in?

Solving a narrow problem: organizations with a narrow problem want ML technology that can be "additive". They seek an incremental journey that solves for one problem at a time. By layering new technology onto their existing stack, they seek to minimize disruption while also measurably improving or existing.

Answering the call for transformation: The call for transformation often comes from a large market force, such as an immediate compliance need or a government directive.

Alternatively, there may be an urgent but broad need to modernize.

Organizations with a mandate for change seek a solution that can solve for cross-functional pains, from those of fraud teams to marketing team to the warehouse.

Working with Existing Systems: For organizations who have already invested significant resources in legacy fraud detection, the choices for bringing in machine learning are whether to complement, supplement, or replace what they have. Machine learning technology can provide flexibility for organizations with existing systems.

For example, a large organization can have different systems detecting different types of fraud across multiple business units and use cases. The right vendor can deploy fraud detection for a single business unit or use case, then expand into others as its value becomes clearly expressed. Because machine learning is better when it ingests more data (assuming it can ingest omni data from omnichannel), a system's orchestration layer gains increasing cross-visibility as it expands, and its detection became even more accurate. The other benefit is that an implementation team can capture and cross-pollinate domain expertise across the organization as they deploy the system into new areas.

Future Proof against Future Fraud:

Whether an organization is solving a narrow problem or answering a call for transformation, it must consider whether a new system is future-proofed against new fraud. The need to think long-term is particularly keen for organizations searching for a short-term solution, because while narrow problems carry the temptation for narrow solutions, a point solution will become obsolete as fraudsters target new vectors.

By focusing instead on platforms with proven blueprints for multiple use cases and business units, an organization can target the two qualities of a future-proofing risk system: fraud detection with both expansive boundaries (beyond existing use cases and business units) and expansive inputs (Omni data ingestion of any orchestration layer, e.g. Data lakes or internal and external data).

Existing solutions either served issuers or merchants, but not both. To operationalize the system, the processor first deploys the issuer solutions.

The units may take cognizant to adopt solutions for merchants as well.

The function is to sit inside the core of the network between the issuing bank and merchant acquiring functions and scores all transactions (not just PIN debit), providing both issuers and merchants with real-time fraud scoring.

The capabilities among machine learning systems differ in a range of ways. Is the system purpose-built to mitigate fraud at an enterprise scale? Is it optimized to handle mission critical applications at high availability and low latency, processing 100% of the transactions? How quickly can it build, train, and deploy models?

Today businesses have a weapon that is uniquely theirs to leverage: machine learning capabilities, together with computing power, that can ingest any kind of data at speed and at scale. It is clear that the winners in this game will be the organizations who break down data barriers, so they can arrest the proliferation of new and unknown fraud and create seamless customer experiences.

By building a complete view of customer behaviour across fragmented interactions, and by connecting this intelligence at speed and at scale, an organization can reduce risk and increase revenue in one fell swoop.

But not all machine learning platforms are created equal.

Here are the key capabilities to look for in a machine learning system in our platform.

360° Vision:

Data is the fuel for a machine learning engine. To be effective, a platform needs to be able to take in all data from all sources, so it can ingest every kind of signal that the customer is providing, no matter the channel or the use case.

Many platforms can only take in data from certain sources or channels. For instance, a platform might look at transactional data but not device data.

These single channel, single use case platforms can be breached. It takes a platform with omni data and omnichannel capabilities to keep pace with today's fraudsters.

To get a complete view of every transaction, an organization needs a platform that can instantly ingest every kind of data, whether it's coming from an internal system, like your Account Management System, or external data sources, like enrichers.

Many sources, one story:

Transactional data<--->online session data—customer data----user device data—third party data

Agile Models:

Multiple models are important because fraudsters behave differently depending on where they are and what they're doing. A global model, for example, won't reflect the nuances of fraud patterns unique to a specific region.

Platforms that can only run one model will use a generalized view to look for specialized behaviours, which results in lower fraud detection rates and higher false positives.

A platform with multiple models must also be able to score orders at scale, without compromising on the response time, by taking all the different input streams from these multiple models and translating them into one single storyline or risk profile that a human reviewer can then evaluate.

Agility means giving the power back to the data scientists, with an integrated environment that lets them adapt to new fraud and deploy models quickly, without having to depend on external resources.

Beyond multiple models, can the platform support custom models? In the rush to buy a machine learning platform, an organization runs the risk of purchasing a "one size fits all" model, with point solutions for single use cases. But every business is different, and every model should be different too. Consider a platform with a flexible and agile architecture, developed by data scientists with domain expertise in specific industries. Custom models that are built with domain expertise in fraud science, specifically for financial services, produce more power and more insight by taking into account the unique fraud patterns that banking and payments face.

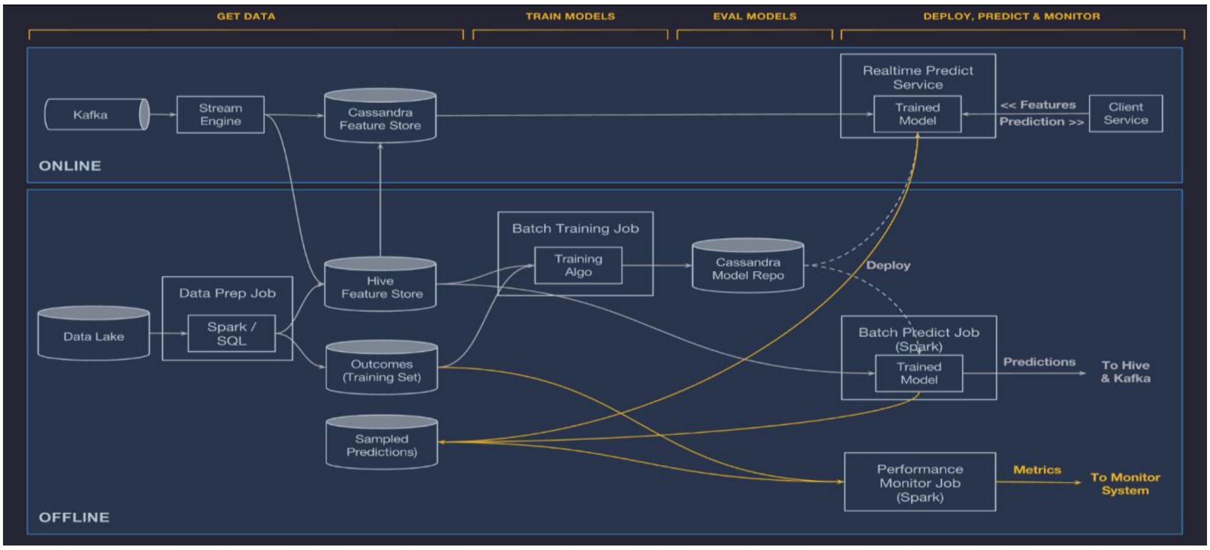
Explainable Logic:

It's hard to decipher the machine logic in systems that use neural network algorithms.

These systems that make decisions inside black boxes lack transparency around their decisions, which creates two serious problems.

First, there's a control problem, because humans can't manage and improve a system they don't understand. Second, there's a regulation problem, because an organization can't audit or validate the decisions that happen inside a black box.

Compare that to a platform that does Whitebox processing to provide clear, human-understandable reasons for its decisions. Certain machine learning platforms predict patterns using an algorithm called Random Forest, which is made of tens of thousands of decision trees. A Whitebox system can take the few top-most factors from this ensemble of decision trees, then weigh and communicate them to the human in a simple way.



.

What to do in case of a credit/debit card fraud

The moment you come to know that a suspicious transaction has been done on your credit/debit card, inform the card issuer immediately. One should lodge a formal complaint with the bank and ideally call up the customer care number to block the card or the account immediately.

How to file a complaint

If you a fraud related to net banking, ATM transactions, or any other online transaction happens, you have to raise a complaint. But, before filing a written complaint with the bank or the card issuer, make sure you have at least these following documents with you:

* Bank statement of the last six months of the concerned bank
* Make a copy of SMSs received related to the alleged transactions
* Take copy of your ID proof and address pro ..

What you should do

Having informed the bank, as per the RBI rules, the resolution has to be over within 90 days. Banks have to credit or reverse the unauthorised electronic transaction to the customer's account within 10 working days from the date of notification by the customer. Credit card frauds are known to be more common in case of their usage abroad.

LEGALITY

In any fraud - the primary offense is always CHEATING wherein there is a victim or victim(s) , there is a perpetrator (accused) and the victim undergoes financial loss due to action of the accused - the financial loss may be due to (a) False information provided by the accused (b) Accused availing goods, services from the Victim but not paying for the same intentionally (c) Accused giving information which is false to cause the victim to part with money or any item of monetary value.

Under Indian Penal Code -regardless of Rs. 25000/- or Rs. 25 Crores - the offense is always Section 420 (Cheating)

The secondary offense - is the additional offenses committed to facilitate the cheating for instance (a) Forgeries of various kinds (465,467,468)(b) Impersonations of various kinds (c) Theft/Breach of trusts of various kind (381,406,409) (d) Corruption by public servants etc (Sec 7, 13 of PC Act) which are always added in most cases to the primary offense.

So Fraud is just a combination of Cheating with offenses facilitatiing the cheating.

Maximum Punishment for any kind of Fraud is 14 years. This includes all sections and all offenses. Regardless of whatever may be the fraud - the maximum term for imprisonment is always 14 years.

The minimum could be anything including Time served - for a few months also. It depends on the Judges discretion.

For huge amounts - other acts like Protection of Depositors Act of Various States, Money Laundering (PMLA) etc are also imposed.