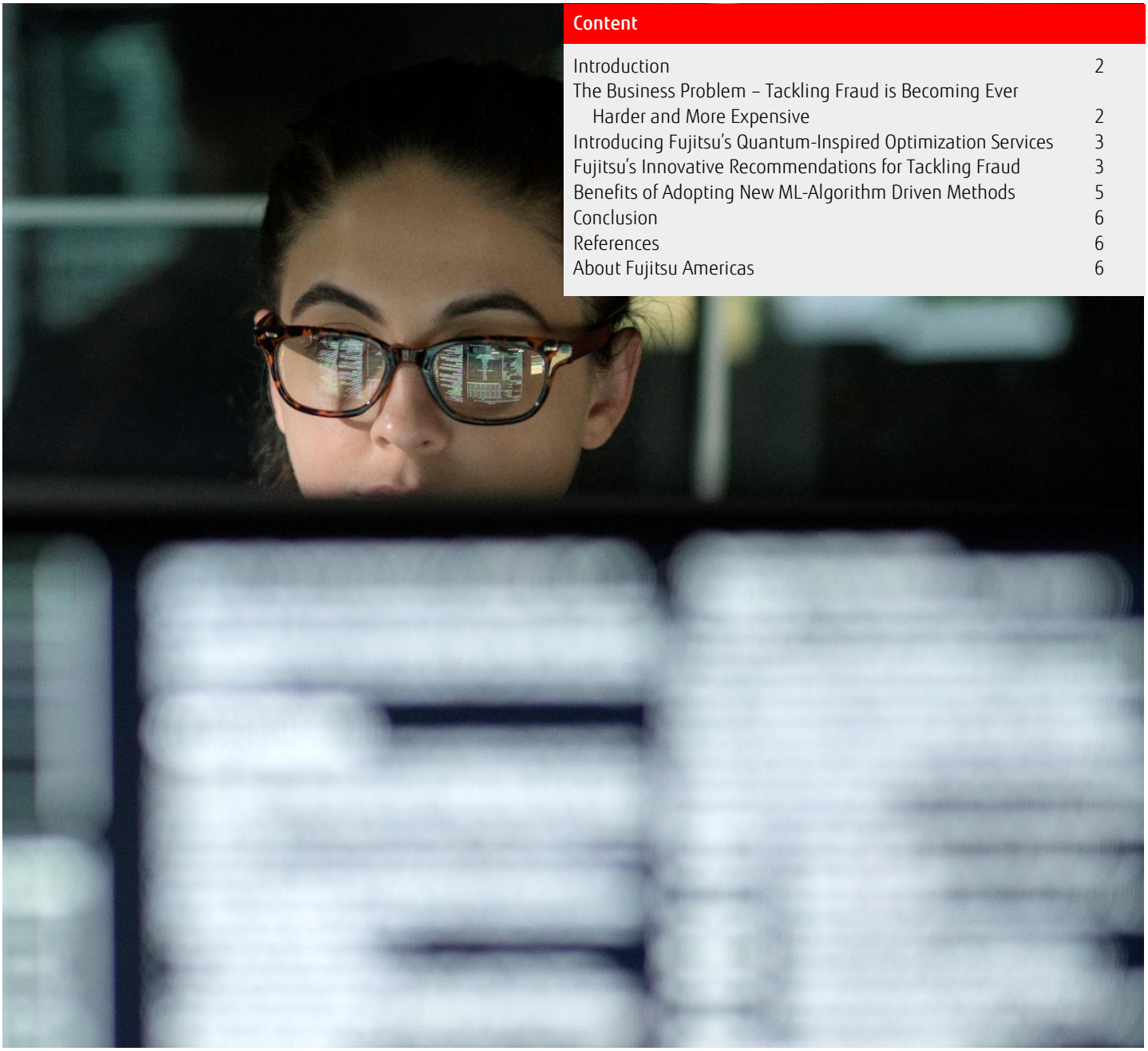
FUJITSU

White paper

How to Improve Fraud Prevention & Detection Leveraging Machine Learning & Quantum-Inspired Optimization Techniques

Written by : Thierry Kahane, AI & Analytics Practice Leader for North America at Fujitsu
Debarttasharan Dey, Senior Data Scientist at Fujitsu



Content

Introduction

In recent months and years, the banking & finance sector has dramatically expanded the adoption of new technologies and platforms used by consumers for B2C digital banking, eCommerce and peer-to-peer payments. This is great news for customers, but it has had an unfortunate side effect: increased potential for fraud. As a result, fraud detection and fraud prevention have further grown in importance in this industry.

This increased emphasis on combating fraud is not an overreaction; sellers stand to lose a staggering US$130 billion to online payment fraud between 2018 and 2023[1]. Additionally, the US transaction value in the mobile POS payment segment is projected to reach US$358 trillion (39.1% growth) in 2020, coming from about 50 million users. This is expected to grow to 75 million users by 2024[2], further increasing the risk of fraudulent transactions. In 2018, there already were close to 700,000 account takeovers (ATOs), which was a growth of close to 100% compared to 2017, resulting from the continuing shift of a larger portion of financial services to online and mobile channels[3].

According to the 2019 AFP Payments Fraud & Control Survey, payment fraud continues to soar, and a record 82% of organizations reported incidents in 2018[4]. In the credit cards eco-system, the card issuers, merchants, acquirers of card transactions from merchants and acquirers of card transactions at ATMs experienced gross fraud losses of $27.85B in 2018, an increase of 16.2% from 2017. This number was projected to rise to $35.67 billion in five years and $40.63 billion in 10 years, an increase of 45%.[5]

It is no wonder that large financial institutions are constantly looking for better approaches to contain these costly threats that are constantly growing and evolving. In this article, we will explore some of these approaches and suggest several ways to improve their effectiveness and efficiency of by leveraging the power of machine learning combined with quantum-inspired optimization provided by Fujitsu's proprietary Digital Annealer.

The Business Problem – Tackling Fraud is Becoming Ever Harder and More Expensive

There are two components to combating fraud – fraud detection and fraud prevention:

- Fraud detection refers to the ability to recognize or discover fraudulent activity
- Fraud prevention refers to measures taken to avoid or reduce fraud from happening

Both these approaches are used in tandem, achieving the common goals of minimizing the risk of exposure to a fraudulent event and the materiality of the losses due to fraud. However, as the complexity and size of this problem continues to explode, companies have moved from the old rule-based fraud detection systems to approaches using machine learning (ML), especially to detect fraud in high-volume activities such as credit cards and payment systems.

The rule-based model is the standard approach to fraud detection. It relies on expert judgement and detection systems, based on rules determined by analyzing historical data and experiences. Such rule-based engines are expensive to maintain and manage, since the rules have to be continuously updated based on the discovery of new fraud cases and findings from security experts. Also, it is important to realize that fraudsters can learn about the business rules that block transactions through trial and error, and devise ways to get around those rules to commit fraud.

In contrast, the ML-based fraud detection model takes into account subtle and hidden events in user behavior that may not be evident, but still signal possible fraud. ML allows for the creation of algorithms that process large datasets with many variables and help find these hidden correlations between user behavior and the likelihood of fraudulent actions. Another strength of machine learning systems compared to rule-based ones is faster data processing and reduced reliance on manual work. For example, ML algorithms fit well with behavior analytics used in helping reduce the number of verification steps. However, building an effective ML-based fraud detection system presents companies with its own set of challenges.

Most financial institutions are facing a scenario such as the one described below when considering the implementation of a new ML-based fraud detection model for their payment platforms:

- **Objective:** improve the ability to tackle fraud in payment systems leveraging the large numbers of data points available on their customers, while facing a rapidly evolving fraud activity. In such scenarios, it becomes imperative for companies to detect and respond to new fraud patterns quickly in order to remain ahead of the curve and protect their clients.

- **Challenges:** one of the hardest challenges is selecting a robust set of features that serve as critical predictors of fraud from the very large set of attributes associated with customers and transactions. Selecting the right features / critical predictors from a massive range of possible predictors becomes a NP-hard problem. Solving this problem poses major challenges for the traditional feature selection method called RFE (Recursive Feature Elimination) due to its complexity and size. As a result, banks are only capable of solving this problem for smaller feature sets.

- **Solution:** when constructing a fraud detection model, it is imperative that the most important features are leveraged for accurate classification. ML algorithms such as Neural Networks can be augmented with quantum-inspired feature selection to help determine the most important features, thus classifying fraud more effectively and accurately. Leveraging its proprietary quantum-inspired Digital Annealer, Fujitsu can help implement such a state-of-the-art fraud detection model, which dramatically increases the speed of conducting high-quality critical feature selection.

Introducing Fujitsu's Quantum-Inspired Optimization Services

Fujitsu has developed a proprietary quantum-inspired processor called the Digital Annealer, which is a truly novel computing architecture. This digital chip was purpose-built to solve large, complex combinatorial optimization (CO) problems more efficiently. These problems occur any time the maximum or minimum solution from a large but finite set of permutations or combinations has to be found. Feature selection can be expressed as a CO problem, similar to the traveling salesman problem or knapsack problem, which are two of the most commonly known examples of CO problems.

To address these large CO problems, our teams develop QUBO (Quadratic Unconstrained Binary Optimization) models, which enable a much more efficient solution to a variety of combinatorial optimizations. Challenges like feature selection for use in driving machine learning algorithms can be restated as QUBOs to be solved by leveraging Fujitsu's quantum-inspired optimization services.
For more information, please access our recent whitepaper on this topic called "Why executives are adopting quantum-inspired computing solutions right now " (http://marketing.us.fujitsu.com/rs/407-MTR-501/images/quantum-inspired-computing.pdf) or visit our dedicated webpage (https://www.fujitsu.com/global/services/business-services/digital-annealer/index.html).

Fujitsu's Innovative Recommendations for Tackling Fraud

» Recommendation #1

Apply product & fraud specific pre-processing steps before Using ML algorithms for fraud detection

It is vital for banks to be able to identify fraudulent transactions rapidly and correctly so that customers are not charged for goods and services they did not purchase. Fraud detection is essentially a pattern recognition problem, but of a very challenging nature. For credit cards, every cardholder has certain spending behaviors, which gradually establish his or her profile. These behavioral patterns change over time due to personal or seasonal variations. Very often, unusual transactions will be legitimate transactions. Every cardholder's activities generate a huge number of possibilities, which in turn lead to an exponential rise of new behavioral patterns and attributes. Therefore, it is impossible to identify consistent and stable patterns across all of the transactions generated by each customer.

Additionally, banks capture a vast multitude of monetary, non-monetary and device attributes related to their customers' transactions. These immense amounts of data make proper pre-processing and data-cleansing a crucial first step. Even after extensive pre-processing of the datasets, which includes removing any redundant variables through the feature selection step, the data will typically still be very imbalanced, with the vast majority of transactions being legitimate. This has led banks to increase the adoption of advanced ML algorithms like XGBoost and neural networks to detect fraud even in these highly imbalanced datasets.

Pre-processing should be based on product specific fraud events – An example for online payments: the crucial step of pre-processing of the data should take into account product specific fraud events. For example, in the case of payment systems, banks will capture vast amounts of monetary, non-monetary and device attributes about their customers. Proper pre-processing should be take into account the investigation of any past fraud events. To catch fraudulent events effectively, the crucial data cleansing pre-processing steps will include: creating relationships between payer and payee; creating distance metrics between payee and payer; matching the phone number area code between payer and payee; matching state location; evaluating transfer memos by calculating the number of characters; calculating the ratio of amount transferred to available balance; creating variables to capture device attributes like model name, model type and screen resolution; etc.

» Recommendation #2

Conduct Feature Selection Using Quadratic Optimization vs. Traditional Recursive Feature Elimination Method

Companies typically encounter a wide variety of issues when building fraud detection algorithms. As noted, they often they deal with high-dimensional datasets and these datasets are highly imbalanced. An acceptable ML model should have both a low level of false positives and of false negatives (you do not want to bother "good" customers, but at the same time you need to catch "bad" actors). In such a scenario, identifying the right set of critical predictive features becomes a crucial step in the development and use of these ML algorithms.

a) Traditional Method: Feature Selection Using RFE

The traditional approach consists of using Recursive Feature Elimination (RFE), which is a wrapper feature selection method that works recursively, removing redundant features and building a model based on the remaining attributes. It uses model accuracy to identify which features contribute most to predicting the target variable. This works well if you have 10 features, from which you want to select the top-three critical predictors. In that case, it will have to run through 120 combinations to select the best subset of three features with the highest accuracy level. In reality though, especially in the world of fraud detection in payment systems, banks gather thousands of variables to evaluate customer behavior. Running traditional wrapper functions in a Monte Carlo simulation environment is not feasible when dealing with these high dimensional datasets.

When dealing with these very large potential feature sets, the challenge consists in eliminating insignificant and unimportant features, whose contribution to the predictive model is almost zero. Banks deploy feature selection steps to identify the most significant features from an initial set of possible predictors. When the number of possible features grows, this becomes a combinatorial optimization problem, which is very challenging to tackle. Suppose a bank wants to run a logistic regression with a feature set of 48 variables to detect fraud on its digital payment platform. Additionally, this bank would like to run the logistic regression with only the top 10 critical predictors and remove the remaining redundant predictors. The number of possible combinations will be about 6.5 billion, meaning that the bank will have to test over six billion combinations individually to find the best one. It is not feasible to test so many permutations systematically with traditional computing approaches.
Such traditional techniques work well only when dealing with a small set of predictor variables. For much larger sets of variables, Fujitsu recommends conducting feature selection using QUBOs to build powerful ML algorithms to detect fraud as explained below.

b) Superior Method: Feature Selection Using QUBOs

Suppose that from the original set of n features, we want to select a subset of K features to use in making decisions about fraud. The number of possible subsets of size K is given by combinatorial function C(n,K). This search space will typically be very large. Therefore, we recommend focusing our search on areas where the best subset of features is likely to be found. QUBO-powered feature selection enables much more rapid searches on much larger search spaces, which can be done interactively, as opposed to the traditional methods, which require hours or days of computation[6].

Solving this QUBO equation with the Digital Annealer, we can select features that are both independent and influential. Compared to traditional methods, for which compute power and memory would need to scale exponentially with a growing number of independent variables, the QUBO formulation scales linearly. This scaling advantage, combined with the hardware acceleration provided by the Digital Annealer, will provide significant performance improvements over traditional methods.

» Recommendation #3

Include Social Network Analysis in Fraud Detection Efforts

Social networks constitute an important element in the analysis, detection and prevention of fraud, which is especially true given the accelerated adoption of social media platforms and features. Fraud is often committed through illegal setups and leveraging multiple accomplices. When traditional techniques fail to detect fraud effectively, social network analysis can provide new insights by helping to investigate how people interact with and influence each other. These so called suspicion-by-association' approaches assume that valuable insights can come from such analysis because fraudulent influences often run through perpetrators' social networks.

However, online social networks often consist of millions of interconnected parts reflecting the size and complexity of most real-life networks. Therefore, technology companies and banks have started using graph theory to extract meaningful statistics and insights from these networks. Graph theory, informally referred to as graph clustering, is an example of unsupervised machine learning. Executing a graph clustering analysis for a large network becomes a NP-hard problem, which is often successfully tackled by using meta-heuristic techniques, exploring subsets of the solution space. Fortunately, graph clustering analysis can also be reformulated as a QUBO (Quadratic Unconstrained Binary Optimization) problem, which can enable banks to tackle much larger networks much more effectively and rapidly, to find the answers they seek [7].

Benefits of Adopting New ML-Algorithm Driven Methods

Machine learning is being used more intensively in the fight against fraud, helping companies to be more efficient and accurate in detecting fraud across digital channels. Advances in technology and ML algorithms are helping banks and companies to more accurately pinpoint fraudulent activity today in a way that previously would have been impossible, thus protecting the organization's reputation and giving customers a safer and more seamless experience.

Large financial services companies are seeing real benefits from adopting these newer approaches powered by ML and other new technologies. Typically, companies see significant improvements such as a reduction in false positives in the range of 50-70%, which improves the customer experience. Additional benefits include improved authorization rates, increased fraud detection accuracy and reductions in missed fraud as high as 80%.

Generally, banks experience the following tangible benefits from moving to these methods:

1. Scalability- ML algorithms and models become much more efficient and accurate with increasing volume of data, whereas for rule-based models the cost of maintaining these fraud detection models escalates as transaction volume increases. The ML models are much better at picking out the relevant patterns across multiple predictors spread across large datasets.

2. Speed - With advances in real-time processing, ML techniques are being deployed to enable real-time decision making. Advances in in-memory and real-time streaming technology has allowed for real-time scoring mechanism based on ML algorithms, enabling decisions in seconds.

3. Accuracy – ML models are much more effective than rule-based algorithm in discovering non-intuitive and extremely subtle patterns, which might be hard to detect, even for an experienced fraud analyst.

4. Continuous Learning - ML models are much more efficient in adapting to changing behavioral patterns of customers and fraudsters. When building ML models, one must be mindful of the changing threat landscape. The real world is dynamic with fraudsters constantly changing their tactics. Continuous improvement is an essential part of the ML operating mode, with newer datasets and features used for retraining to increase the quality of ML models and to keep pace with the evolving threats.

5. Flexibility – Using ML techniques enables a better balance between catching bad actors while not disturbing good customers. The right way to maintain that balance is to continuously evaluate and include new data from multiple vendors and partners, and find unique features that identify and protect the real customers behind the digital identities.

Conclusion

As we outlined in this article, fraud in financial services is continuing to grow at an accelerated pace resulting from the movement to online banking and other online financial activities. Therefore, financial institutions need to continue to adopt fresh approaches and technologies to stay ahead of the curve and protect their customers' assets as well as their own reputations. The good news is that these exciting innovations can be and are being adopted right now by financial institutions. These enable banks to continue serving legitimate customers and ensure the safety of their transactions across digital channels and platforms, while catching bad actors and preventing their fraudulent activities as early and quickly as possible.

For more information about this solution or the Fujitsu Digital Annealer, please visit www.fujitsu.com/global/digitalannealer or contact the author at thierry.kahane@fujitsu.com.

References

1. https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report
2. https://www.statista.com/outlook/331/109/mobile-pos-payments/united-states
3. https://feedzai.com/blog/fighting-fraud-and-financial-crime-with-a-single-customer-view/
4. https://www.prnewswire.com/news-releases/payments-fraud-jumps-to-record-high-82-of-businesses-impacted-survey-finds-300825669.html
5. https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1164.pdf
6. Milne A., Rounds M., & Goddard P. (2017). Optimal Feature Selection in Credit Scoring and Classification Using a Quantum Annealer.
7. Baesens B., Veronique V.V. & Wouter V. (2015). Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection.

About Fujitsu Americas

Fujitsu America, Inc. is the parent and/or management company of a group of Fujitsu-owned companies operating in North, Central and South America and Caribbean, dedicated to delivering the full range of Fujitsu products, solutions and services in ICT to our customers in the Western Hemisphere. These companies are collectively referred to as Fujitsu Americas. Fujitsu enables clients to meet their business objectives through integrated offerings and solutions, including consulting, systems integration, managed services, outsourcing and cloud services for infrastructure, platforms and applications; data center and field services; and server, storage, software and mobile/tablet technologies. For more information, please visit: http://solutions.us.fujitsu.com/ and http://twitter.com/fujitsuamerica

Contact
FUJITSU AMERICA, INC.
Address: 1250 East Arques Avenue Sunnyvale, CA 94085-3470, U.S.A.
Telephone: 800 831 3183 or 408 746 6000
Website: www.fujitsu.com/us
Contact Form: http://solutions.us.fujitsu.com/contact

Have a question? Email us at: AskFujitsu@us.fujitsu.com