Deep Science Publishing
https://doi.org/10.70593/978-81-988918-1-5_8

DeepScience
Open Access Books

Chapter 8: A deep dive into credit card networks, fraud detection, and artificial intelligence - driven risk assessment

8.1 Introduction

Credit cards are often regarded as the most convenient and universal payment method. Therefore, it is not surprising that the credit card network industry is a multi-trillion-dollar market, responsible for more than 25% of the GDP of many developed countries. Today, the main players in the credit card network industry are Visa, Mastercard, and AMEX. These companies provide payment processing solutions, by putting in place a system that connects consumers, merchants, banks that support consumers, banks that support merchants, and companies that secure the credit card network (Chen & Zhang, 2021; Gupta & Singh, 2022; Kim & Lee, 2023).

More concretely, when a customer decides to pay for a purchase with a credit card, he/she presents the credit card to the merchant, who in turn sends the credit card information to the payment processor. The processor contacts the customer's bank, and this bank verifies that the card is not reported lost or stolen, that the credit limit is not exceeded, and that the customer has enough money to pay for the purchase. If these checks are ok, the merchant receives the confirmation and the transaction is completed. Then, the funds are moved from the customer's bank to the merchant's bank. This all happens in a matter of seconds. The fact that this entire system works smoothly is the result of years of technological innovation and work that many professionals dedicated to this purpose (Li & Wang, 2020; Narayan & Bannigidadmath, 2020).

8.2. Understanding the Structure of Credit Card Networks

Credit card networks have become one of the key enablers of contemporary retail and e-commerce, and the question of network design has come back to the forefront, driving discussions about various economic issues regarding the network. Annual credit card transaction volume is more than 10 trillion dollars in the United States alone, and is poised to grow further due to growing consumer preference. In marketplaces and online stores, credit card acceptance is the most popular and oftentimes the only option. Meanwhile, concerns about payment system security and the impact of payment security measures are well understood in the industry. Ensuring that credit card networks validate transactions while minimizing fraud is critical for the smooth operation and growth of not only any single card network, but also of the payment sector as a whole. The credit card industry's specific environment is interesting from the perspective of information security and risk mitigation, as money and identity data are at high risk of theft.

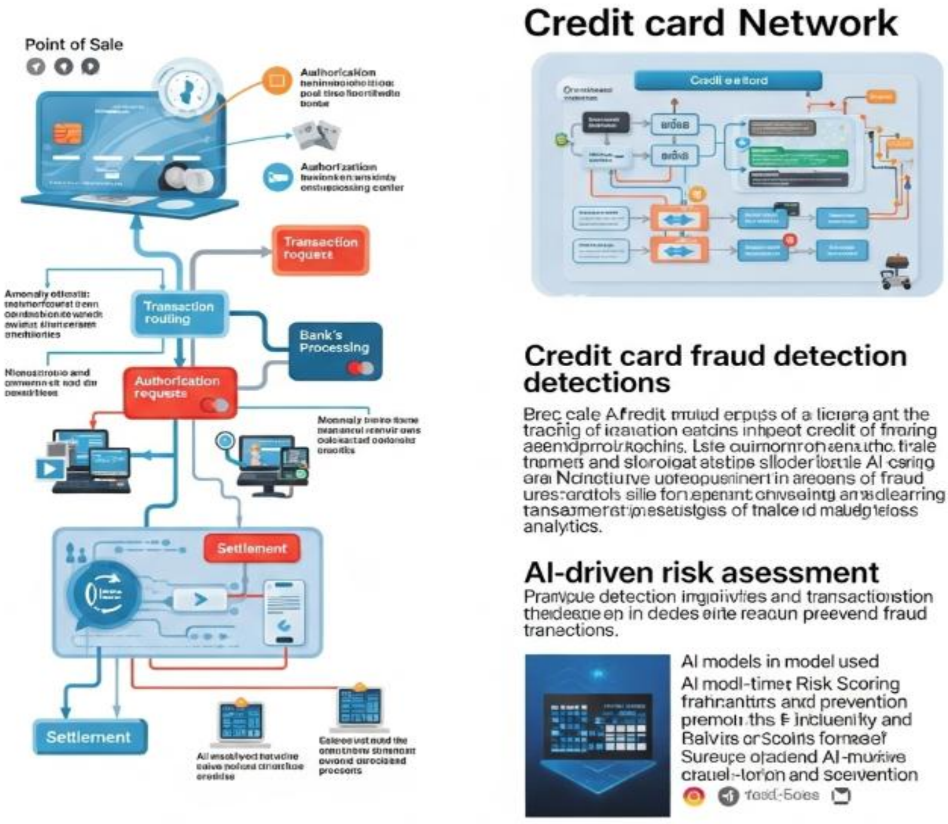

Fig 8.1: Detect Credit Card Fraud with Machine Learning

Credit card networks may be generally described as the intermediaries between merchants and customers. The networks make sure that payment is initiated and completed, while banking relationships involving credit allow consumers delay the deduction of their purchase amounts from their accounts. Although significant time delays between the actual transaction date and the clearing date of the transactions are an established feature of the system, for consumers these electronic transfers are almost instantaneous. From the perspective of banks, credit card transactions involve a considerable amount of service work, because they process the transfer of credit between parties. Many questions arise from the structure of credit card networks.

8.2.1. Major Players in the Network

The credit card network primarily involves two major parties, being the cardholder and the merchant. The cardholder is the person in perspective, and is generally believed to initiate a transaction by presenting his/her credit card through an electronic means of payment, for example, point of sales terminal or mobile wallet, or other means, for example, via online shopping. The transaction is initiated to purchase and pay for goods or services offered by the merchant. The merchant generally possesses a merchant account opened with a financial institution to facilitate receiving credit card payments and has a credit card acceptance arrangement with merchant acquirer to credit his/her account, generally upon availability, with the value of the cardholder transaction minus the processing fees. Payment networks provide a platform for transmitting credit card transaction details between the merchant and cardholder bank. Merchant acquirers are financial institutions that manage relationships with cardholders by opening merchant accounts for merchants. Acquirers typically use services provided by payment processors, who act as intermediaries between merchants, acquirers, and payment networks, for transaction processing.

A merchant acquirer is typically a financial institution that acts as an intermediary between merchants and cardholder banks by receiving cardholder transaction authorization requests upon receipt of transaction requests with the payment networks and then forwarding them through payment networks to the cardholder bank for transaction approval or decline. Merchant acquirers may arrange the support provided by payment processors to merchants for the transaction approval infrastructure. Payment networks have relationships with acquirers for facilitating credit card acceptance arrangements with merchants and receiving from acquirers the approval or decline messages for credit card transactions initiated by cardholders for completion of transactions initiated for merchants. Subsequently, the merchant acquirer debits the account of the cardholder bank and later credits the account of the merchant, typically, after deducting processing fees.

8.2.2. Transaction Flow and Processing

The first step initiating a credit card transaction process occurs when a consumer purchases goods or services with a merchant at the merchant's store location. Following this event, the merchant sends a transaction authorization request including the purchase amount for the goods or services and card details such as number, expiration date, and card verification value code via the merchant's bank into the network, and the acquirer completes and forwards the request to the card issuer via the card network. The card issuer then verifies whether the transaction can be authorized based on various parameters, such as cardholder credit limit, temporal and geographic validity, and whether the cardholder has reported that card as compromised, and sends back an authorization reply via the card network to the acquirer and finally to the merchant. Upon receiving the reply, which typically responds with an approval or decline code, the merchant and the cardholder either complete the transaction or abort it. In some cases, instead of checking the transaction authorization immediately, some merchants, especially those operating in online environments, request the storing of cardholder details until the actual settlement is subsequently performed.

The second major step is the settlement: if the transaction has been authorized, after the merchant processes the transaction, it forwards a settlement request through the network to the card issuer, which transfers the transaction amount, minus applicable fees, to the acquirer, whereupon the acquirer pays the merchant. Most issuers allow their customers to defer payment up to 1 month from the date of the transaction without charging any interest on the amount owed; if the customer fails to pay the full debt in the month following a transaction, typically, the issuer charges interest starting from the date of transaction. Monthly statements of account, listing transactions and the amount owed, are sent by the issuer to all cardholders.

8.3. Types of Credit Card Fraud

Credit card fraud is a broad classification that describes multiple illicit acts. Several of the merchant and company losses due to credit card fraud are due to chargebacks, or cardholders denying that they approved a transaction. A chargeback can occur for legitimate transactions as well. For example, if a company receives a returned item from a buyer, but does not refund the buyer or cancel the transaction, the buyer may request a chargeback. Some banks enforce strict time limits on how long a cardholder has to dispute a transaction or they may refuse to process a chargeback. Chargebacks negatively affect merchant relationships with credit card companies due to the costs incurred from processing. In addition, companies face the costs of the items that are returned but not re-sold. As a result, credit card companies may revoke a merchant's ability to accept credit cards if the company has an excessive number of chargebacks.

Due to the risk of chargebacks, credit card companies, banks, and merchants are incentivized to reduce fraudulent transactions. In the vast majority of cases, credit card fraud incidents come from two sources: card-not-present and card-present transactions. CNP fraud is when the cardholder is not present during the transaction process. Most frequently, this means that a card is swiped during a telephone or Internet transaction. It includes payment by telephone for goods and services as well as e-commerce or mail-order purchases. There is an increased risk of fraud in such transactions, as the merchant cannot verify that the person asking for the transaction is in possession of the card. Causing additional issues with CNP fraud, many merchant fraud detection systems rely on the billing address and not the shipping address during verification. This is unsafe, considering that a fraudster can easily purchase items for shipment to another address without being detected.

8.3.1. Card-Not-Present Fraud

A card-not-present (CNP) transaction occurs when the cardholder does not present a physical card to a merchant in an electronic transaction over the Internet, telephone, or mail. The card issuer authorizes a CNP transaction by publishing software security standards. The Merchant gets the card authentication data, passes it together with other transaction information to the acquirer, who, in turn, passes everything to an issuer to check that the data is authentic, prevents fraud, and clears funds. Alternatively, a risk-based authorization method screening for certain unusual transaction characteristics, in tandem with a common risk-rule test, could be implemented to flag certain high-risk CNP transactions for manual review. In this manner, CNP fraud prevention can balance the sometimes-conflicting goals of fraud detection and customer service. The merchant is liable for any CNP fraud if the issuer agrees to not bear the loss, for example, if the merchant did not take reasonable precautions to prevent fraud or the cardholder failed to pay a bill because of unauthorized charges on the account. Fraudulent CNP transactions totaled $46.5 billion in 2022, accounting for 79% of global card fraud losses. CNP represents a "perfect crime" that "is easily perpetrated and very difficult to prevent," and consumer doubts about security are the main impediments to larger volumes of global e-commerce. The main methods for preventing CNP fraud losses include: risk-based business rules, CNP insurance, and "execute, measure, and optimize." The "execute, measure, and optimize" method "allows for quick testing of a fraud detection model in a live environment with real cash-flow impact." The model is also "retuned continuously as market conditions change and customers adjust behavior as a response." The "execute, measure, and optimize" method can also be executed in tandem with PCI compliance without impacting service levels or customer satisfaction.

8.3.2. Card-Present Fraud

This section provides an overview of credit card fraud that occurs in a brick-and-mortar setting where a physical card is presented, but it is not an authorized use of that card by the actual issuer-identified cardholder, which is the relevant definition as there are many other types of fraud that can occur in such card-present settings. For example, card-present fraud is distinct from unauthorized but legitimate card usage that is a crime like shoplifting, or the display of counterfeit cards to the transaction manager, which could lead to various forms of asset loss without necessarily being considered a card-present fraud. The definition for card-present fraud used in this paper is intended for capturing only actions indicating that the actual cardholder is not the impartial at-the-counter user, such as identity theft, skimming, or cloning.

The section's limit on definition extends only so far as modulating one's actions with regard to the credit account legitimizing the physical card in question, as opposed to just performing an unauthorized transaction. In other words, some definitions would insist that card-present fraud is always related to unreported cards or otherwise invalid cards issued in the name of a real user; others would broaden its scope to all actions that steal money from merchants or retailers via false seeking legitimate facilitation. The restriction to only account-infringements is the more widely accepted one. After examining fraud in a card-present setting in generality, the section provides an in-depth look at how this fraud type is detected, how detectors might be evaded, and how data science methods can improve the ability of detectors to recognize actual fraud.

8.3.3. Account Takeover

Many merchants encourage new customers to create an account by offering some type of incentive or discount. This makes sense for most large merchants who can afford to acquire and manage customer data for marketing-strategy purposes. However, once a customer sets up an account with a merchant, that account could compromise the individual even further than their credit card alone. This is because the customer account often contains personally identifiable information that is valuable to friends, family, or business associates of the customer. This data can include sensitive information like the individual's Social Security number, passport number, driver's license number, bank account details, or even credit card numbers and expiration dates.

That's why it is crucial to have proper detection mechanisms in place to prevent account takeover breaches. Cybercriminals may exploit account vulnerabilities and takeover accounts through a variety of methods, such as email phishing, credential stuffing, web scraping, session hijacking, and password spraying. Once a hacker gains access to a customer's account, they may use that account to make fraudulent purchases — using the personally identifiable information stored in that account to impersonate the customer in an online transaction — or illegally access the user's sensitive data for other nefarious activities.

Account takeover can also be detrimental to merchants, especially e-commerce websites. If a breach occurs and consumers lose trust in a merchant due to a security flaw or if a hacker uses compromised customer credentials to go on a spending spree, the merchant can suffer significant losses. Because of this, merchants likely want to train their internal teams and spend time and resources implementing and optimizing detection mechanisms to thwart account takeover.

8.4. Impact of Fraud on Financial Institutions

Credit card networks and banks providing credit cards suffer adverse effects from card fraud. The increasing ease of executing frauds such as clear-cut low-tech card-not-present frauds, as well as the fraudulent use of existent but unwittingly reactivated accounts, or dormant accounts primed for easy takeovers, makes these two institutions both concerned and attentive to consumer losses along with their expenses devoted to prevention and dispute resolution. The decision-making problems addressed in the present essay.

Network-financed monitoring and assessing of credit card transaction risk has been limited effectively and correctly to card transactions, in contrast with paradoxical benefits from other transactions. Furthermore, time lags in using excess consumer payment capacities to pool fund availability for card exposures serve to annually generate large cost penalty estimates, representing the principal excess preventive expense, often approximated at approximately 1.5 billion dollars per year for the industry. In terms of direct gross fraud costs, these are highly problematic to estimate. Net direct fraud losses suffered by all parties are approximated at 85 percent of approximate gross losses amounting to 753-827 million dollars in 1995.

If too low a threshold cutoff first-pass transaction risk criterion, representing what network security systems use, is imposed to flag excessive incoming alerts by posturing market systems, consumer impatience at transaction delays will detract from the enthusiasm for using credit cards. Improvements in reputation mediated by enhanced accuracy of fraud detection systems geared to fraud reduction have been shown to be positively correlated with the false negative rate and negatively correlated with the false positive rate, thus giving rise to a benefit from brand name equity preservation and enhancement. Moreover, research has uncovered that merchants consistently underestimate their fraud risk exposure but overestimate the loss of revenue from warning good consumers of high Lie-Sim tests by switching to non-capital intensive information data-gathering, mitigation, and resolution procedures or machines using reputation heuristics.

8.4.1. Financial Losses

Criminals using stolen, lost, or counterfeit cards can commit serious financial fraud. Credit card fraud, especially card-not-present fraud, is among the fastest growing types of fraud, in terms of percentage growth and absolute dollar losses. Global card fraud losses reached $28.59 billion in 2019, of which $20.57 billion was incurred by the card issuers and $8.02 billion was suffered by merchants. Moreover, 23% of actual data breaches were caused by financial gain motives, while the cost of cyber-related crimes is estimated to be up to $600 billion each year, a number comparable to the GDP of the 20th-poorest countries in the world, which protect more than 700 million people.

Similar estimations were made regarding lost cards and acts of card fraud. Based on their analysis on financial incidents, global cyberattacks were predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2016. E-commerce crime was projected to reach $4 trillion in the next few years. Based on their analysis of historical trends, CNP fraud losses are expected to exceed $130 billion by 2023. In summary, many have attempted to estimate the financial losses associated with unauthorized use of credit cards and the expected explosive future growth of credit card fraud. Data-driven technological advancements in fraud detection systems are believed to help mitigate these losses and increase the level of protection against credit card fraud, which will benefit not only issuers and acquirers but also customers.

8.4.2. Reputation Damage

One of the most damaging repercussions of successful fraudulent activities is a loss of consumer trust, generated by the initial incident and perpetuated by a pattern of failing to protect consumer interests. Banks and financial institutions are in a business where trust is paramount. For many consumers, their credit card account is an extension of their financial portfolio. With that trusted asset comes an enormous willingness of people to use their credit cards for all sorts of purchases, easily evidencing the positive effects of brands in this space. But trust, once breached, can take a long time to repair. Ongoing reports of data breaches and failures to detect are a negative for banks. Banks invest heavily in marketing to increase brand awareness, brand perception, offering loyalty programs and the like. When something happens to jeopardize that trust, usually a scandal, there is an erosion of that brand image overnight and the cost to restore it can be exorbitant. Moreover, different banks are often compared against each other, so any brand damage for one bank could lead to negative effects for the entire banking system.

A strong commitment to information security and protecting the consumer from fraudulent losses can revive trust in the consumer's bank. Banks provide guarantees that customers won't be held responsible for unauthorized transactions. In some cases, having measures in place for their customer transactions would prove a bank's commitment to authentication. It would help refine their brand attributes over time. Brands are sensitive to long-term negative changes on the product attribute levels because they can be costly and complicated to overcome. Tactics that a bank could implement for protecting transaction accounts would be to put systems in place with additional steps or alerts to alert the consumer of the transaction and possibly considered a risk indicator.

8.5. Traditional Fraud Detection Methods

The traditional credit card fraud detection has been done using two categories of methods: rule-based systems and behavioral analysis. The advantage of those methods is that they are easily explainable. However, they frequently miss recent patterns hiding unknown fraud types and therefore need to be frequently updated manually. We will first briefly introduce these traditional methods before continuing to AI-driven systems.

The basis of a rule-based fraud detection system is a set of rules, defined by humans, coding their intuition or understanding of fraud. In other words, these rules use transaction attributes, other than transaction amount, date, time, or geographical location, to check for unusual or suspicious transactions. Some fraud detection rules check that the transaction is of high dollar amount and occurs within a short temporal interval or an attempt to use different cards at the same merchant. In addition, the merchants at which the validation is performed, as well as the merchants at which the purchases are being made, are considered unusual if they are not simply from different countries, or have the same general characteristics, such as date/time of the transaction, amount, and type of purchased item.

Although rule-based fraud detection systems are fast and cheap to implement, the downside is that manually implementing rules to be as generic and flexible as possible is a daunting task. Updating the rules is also difficult since fraud solutions are usually based on the type of transactions that were previously identified as fraudulent. Furthermore, rule-based fraud detection approaches are unable to identify unknown transactions that are fraudulent, which is the most important goal of such systems. The reason is that using historical data to create the rules needed for detection prevents the detection of new fraudulent activities and any anomalies.

8.5.1. Rule-Based Systems

A rule-based fraud detection system relies on rules constructed by a team of fraud experts, which reflect that team's know-how derived from their experience with discovering fraudulent transactions in the past. Such fraud detection systems have the advantage of being both easy to understand and explain: if a transaction triggers one of the rules, it is instantly classified as a fraudulent transaction based on that rule. Additionally, rule-based systems are easy to maintain and manage. The drawback of rule-based systems is that their ability to detect new fraudulent patterns is limited. Fraudsters are creative. Consequently certain transactions that are not identified by any of the rules might be fraudulent. That can be a large volume of transactions because rule-based systems are commonly configured so that they generate only a small number of false positives. Moreover, the existing rules may or may not be tuned to the specific behavior of a given transaction type. Moreover, because not all fraudulent patterns are sufficiently obvious, experience with uncovering past fraudulent activity may fail to account for all the cases that experts might consider when developing rules, leading to false negatives. Despite these limitations, rule-based systems remain important due to their ease of configuration.

The rules described above are really more like heuristics than true rules. A true rule would contain a formal specification of the conditional distribution of fraudulent versus valid transactions along with a way of setting a threshold on it. Such a specification is rarely possible due to the fact that, for typical transaction types, the conditional distribution as a function of the transaction features is extremely complex. In simple transaction types, one can get away with simplistic rules of the form "if feature A then fraudulent". However, for ids like credit cards, a rule of that type, which uses only one feature, would produce too many false positives. However, the business of explicitly requesting threshold values instead of distilled rules is the preferred model of modern systems rather than asking for rules.

8.5.2. Behavioral Analysis

Behavioral analysis employs unsupervised and/or semi-supervised techniques to determine user operations from static and/or dynamic data parameters. Unsupervised and/or semi-supervised models applied on dynamic data can discover new states representing relevant user behavior, calculate the change rate from previously established knowledge, estimate the probabilities of behavior at any point in time; and use the results for on-the-fly risk evaluation. In addition, unsupervised and/or supervised models can characterize the data records by clustering and can detect label-corresponding abnormal deviations via supervised methods. These methods extract recurrent transactions, sort them, calculate the user transaction's total duration and the average and maximum timing differences, identify the days of the week and the operating times, build user transaction histograms axis-aligned on these parameters, extract the histogram modes and H-function moments, learning user profiles based on a statistical-dynamic analysis instead of a purely dynamic analysis.

User profiles describe the routine behavior of a user for a certain range of time. In practice, the histogram modes during the non-incremental data profile building phase represent the most typical state of a user during the profile-building phase, and during the operational phase, represent what the operations must stick to. The statistical distance between the user-histogram and behavior-histograms determines the behavioral risk index. Theoretically, user profiles continue to be built while the user debit card is managed. Nevertheless, the profile improvement process takes time, involving a simile of the user identity inspired by the old truism that practice makes perfect.

8.6. Emergence of AI in Fraud Detection

Over the last few decades, intelligent systems have increasingly been utilized to enhance the productivity, efficiency, usability, and business value of information systems in a variety of domains. In particular, with the evolution of machine learning, large-scale data access, and computing resources, there have been significant strides in the development of software tools for sophisticated machine learning methodologies. Application of these intelligent tools to data-rich fraud detection domains has uncovered both new techniques and problems, particularly emerging in the area of credit card fraud detection for the prevention of revenue losses in the banking and finance sector.

Smart payment platforms and subsequent commerce growth have led to substantial credit card transaction data availability. Credit card networks collect massive credit card usage data and outsource fast and reliable fraud detection to specialized service companies offering fraud prevention solutions. The volume of legitimate transactions presents ample opportunity for fraudsters to think creatively and continually update their tactics in an ever-evolving cycle; therefore, fraud detection systems must continually update their models for these shifts, imposing a heavy burden. Traditional fraud detection methods have only been moderately successful as machine learning algorithms employed as pattern recognition techniques have focused on building models based on past data of detected fraudulent chains of events that are stored in the banks' databases.

Several issues have posed unique challenges to the task of credit card fraud detection. The ratio of genuine transactions and fraudulent activity is extremely imbalanced, with a small percentage of all transactions actually being of fraudulent nature. Another is the fact that massive amounts of credit card transactions need efficiently be evaluated in real-time. This calls for fast computation time for the application of the fraud detection models while factors such as changeability and high dimensionality further complicate the problem. Yet another is the need for a robust fraud detection algorithm that can deal with noise in the data, particularly changes in the purchase patterns and use of mobile usage of transaction data for small value of debit card credit transactions.

8.6.1. Machine Learning Algorithms

Fraud detection has been a longstanding challenge across multiple industries. Many methods have been used to identify fraudulent behavior and the corresponding prediction tools have evolved from traditional rule-based systems to modern artificial intelligence (AI)-driven solutions. The associated machine learning (ML) algorithms use sophisticated data pattern-recognition techniques to identify new fraud signs, their speed of detection protecting stakeholders and customers from bigger impacts. These methods leverage both existing fraud knowledge and newer less supervised or even unsupervised approaches to identify anomalies in the data. The associated methods range from traditional outlier detection, statistical processes or rule-based transaction monitoring systems, to more modern machine learning-based techniques like decision trees, support vector machines, random forests or neural networks.

Statistical-based approaches generally focus on the development of mathematical relationships that describe the statistical characteristics of normal behavior or relationships between multiple variables. Outlier detection then searches for transactions that deviate significantly from this norm. Such methods commonly include spectral analysis, regression model residual analysis, Bayesian frameworks, extreme value theory, or principal component analysis to create a lower-dimensional representation and cluster the transactions to highlight possible anomalies. Such methods can leverage unsupervised learning approaches to cluster transactions based on variable similarities. These methods then highlight transactions in small anomaly clusters with low expected sizes or low expected members compared to similar members in different clusters. Current trend of this area is to use more advanced data science methods with dimensionality transformation, such as t-distributed stochastic neighbor embedding, latent semantic analysis or autoencoders to automate the clustering methods. These advanced automation capabilities have led to increasing attention on the associated reinforcement learning frameworks to develop semi-supervised anomaly detection, thus lowering the need for labeled data.

8.6.2. Anomaly Detection Techniques

Anomaly detection is a category of machine learning algorithms that has been around for a long time. In fraud detection, anomaly detection is used to determine whether a transaction is an outlier from some normal profile. Sometimes, anomaly detection is called one-class classification because it learns from a distribution of labels for only one example. It is different from typical supervised classification in that there are very few examples with non-regular labels. In contrast to supervised classification, it often works better in the unsupervised configuration, where no label is even provided.

Anomaly detection works on the assumption that fraudulent activity is rare or not representative of the normal distribution of credit card transactions. This is especially true for the early phase of a new payment method: A large number of transactions will be labeled as legitimate because there is little or no fraud. Consequently, in a credit card dataset, given the vast number of consumers, shops, and transactions, chances are that outliers in a profile may not be detected, even disproportional or disproportional to the number of legitimate transactions. Anomaly detection can be performed at various levels of credit card transaction profiles, either jointly or separately: consumer, shop, merchant category, geographic area, transaction type, and card issuer. It can also be performed for modifying parameters, for example: time of day, day of week, or centralized online access history behavior.

8.7. Benefits of AI-Driven Fraud Detection

AI and machine learning make it cost-effective for credit card networks to detect more fraud without increasing false-positive rates. AI technology offers significant accuracy benefits that lead to improved profit margins as networks address more fraud. AI also enables networks to identify stolen cards and conduct at-risk transactions in real time, allowing the issuance of significantly fewer new cards for affected customers and, thus, greater end-user satisfaction. Because of an AI approach to fraud detection, customers incur lower transaction costs, which drives customer loyalty and increases usage. Current challenges such as evolving consumer behaviors and emerging payment ecosystems limit network margins. These converging factors require that credit card networks have smarter tools for fraud detection. Current payments models use a rules-based approach that identifies previously defined threats and falls short of recognizing new risks, is costly, is incapable of processing data in real time, and is inaccurate. To provide better security against current and emerging threats, payment networks are turning to AI systems capable of processing batch data in seconds or milliseconds, with results that achieve a higher accuracy level than rules-based systems. AI technology used as part of a more extensive fraud detection system is substantially more accurate than traditional rules-based systems, leading to more precise decision-making and profitable results. The processing speed and accuracy achieved by AI systems reduce transaction-blocking occurrences, allowing greater network speed and efficiency, from card authorization to settlement. AI-driven multivariable models deliver significantly greater accuracy levels, compare fraud and non-fraud characteristics, and monitor broader variables. These end-to-end, near-real-time solutions often analyze thousands of model variables to create a model capable of predicting acceptable approval rates.

8.7.1. Increased Accuracy

AI-driven risk assessment tools are based on machine learning methodologies that outperform traditional techniques. AI leverages the promise of deeper and more robust data verification, allowing the detection of even very small changes in the financial behavior of users. Consequently, the increasing amount of data processed, coupled with advanced technology, produce intelligence that generates higher detection of prediction rates and reduces false alarms, increasing response efficiency. The increasing use of AI has proven that machine learning-based algorithms detect almost twice as many fraudulent credit card applications as traditional rules, more accurately identify malicious merchants compared to blacklisting-based systems, and more deeply inspect transactions by flagging those transactions that are cutoff from a merchant's historical activity patterns such as defaulting a previous payment or repaying a loan at an unexpectedly high rate. Because it is unrealistic to expect traditional blacklists to constantly and forever detect new, customizable credit card payment fraud methods, leveraging AI in the form of machine learning algorithms provides a more intelligent and accurate response. However, beyond just fraud detection, these state-of-the-art systems reduce costly delays and generally improve overall transaction management processes for all parties involved. Multinomial Logistic Regression, Random Forests, and Gradient Boosting Machine methods differentiate between risk-based classes more effectively than traditional decision-tree-based classifiers.

8.7.2. Real-Time Processing

Fraud detection has been a well-recognized application domain of AI technology for fifty or more years. Since machine learning has been available, the focus of research, applications, and publications has accelerated greatly. The application area has also been extended beyond just credit cards but includes online banking, e-commerce, and corporate fraud as well. The detection problem is usually posed as searching for hidden patterns or structures in datasets that are considerably skewed in favor of "normal." For credit card data, many million transactions occur every day but only a small percentage of those are fraudulent. Various specific machine learning methods are used including case-based reasoning, Bayesian inference, neural networks, genetic algorithms, support vector machines, and most commonly, decision trees, along with the more classical statistical modeling techniques.

The increasingly instant character of transactions, particularly in the area of online, phone, and text transactions where the likelihood of approval and income is very sensitive, has led some networks and major banks to begin to include active intelligence in their basic transaction processes. Hence they would assess risk in real time during the transaction. These neural net-based systems usually assess transactions in an aggregate with a multiple credit risk score parameterization.

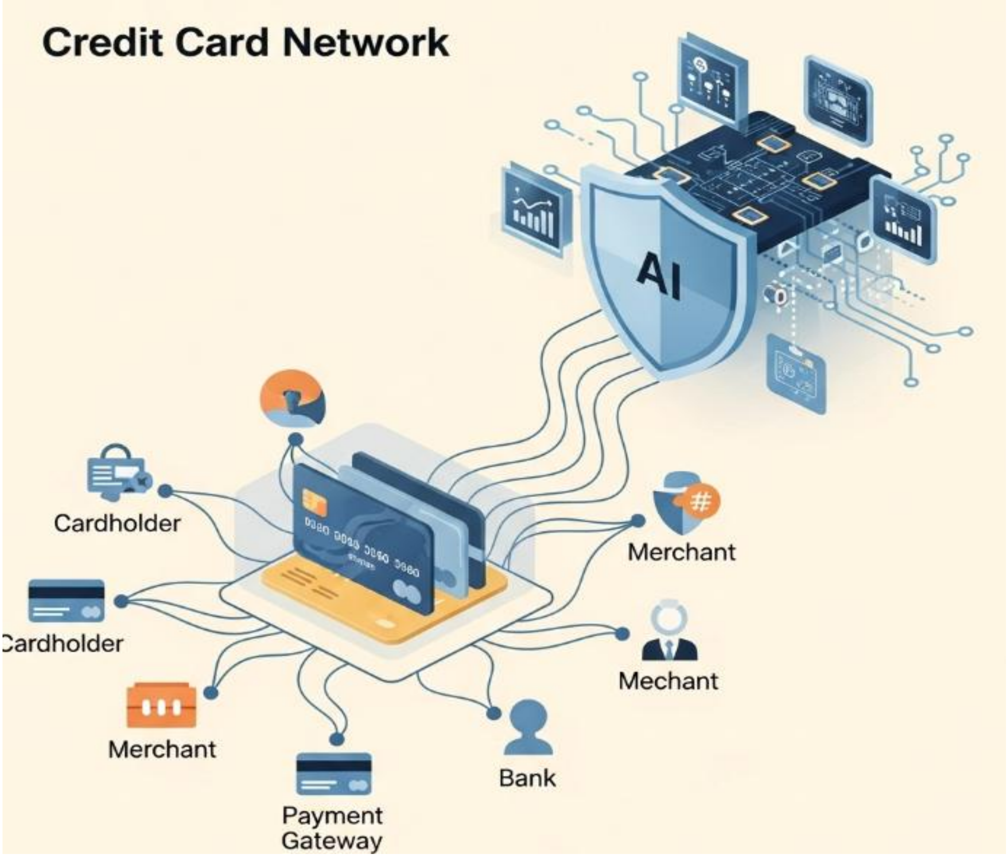

Fig 8.2: credit card fraud detection

Those scores can include, or be formulated from, previous credit performance based on history, previous five-year charge-off experience, risk-based reward points relationship, and risk-adjusted pricing gross margin identification. Neural nets have been implemented to signal the transaction for further manual processing if required.

8.8. Challenges in Implementing AI Solutions

The success of AI solutions is heavily dependent on large amounts of pertinent data. The technology needs large averages of labeled samples for each set of features of interest, which is relatively easy to gather for problems such as image classification, where hundreds of thousands of labeled objects can be retrieved. Example AI solutions in fraud detection also use these labeled data averages, compared with small samples reflecting unique company circumstances, relationship types or customer behavior. Users expect AI solutions to account for organization-specific parameters, while designers rely on large labeled data for model training. What makes unique AI solutions viable? First of all, companies need to share anonymized information to help create groupwide models. There are currently no joint solutions viewable by other participants in the transaction monitoring space. All models made available use internal bank transaction monitoring data only. Consortium joint models would eliminate the high false alert ratios currently faced by banks. Purchasing behavior by industry segment would also allow consortium members to share responsibility for unique algorithms and reduced risk exposure.

Algorithm bias is a well-documented phenomenon that occurs when an algorithm produces results that are systemically prejudiced due to erroneous assumptions in the machine learning process. All AI algorithms suffer from some degree of algorithm bias, which can be introduced at any stage of the machine learning process. Biases are inevitable in any type of model since the world today is still not perfectly fair. Algorithmic fairness is the property of algorithms ensuring responses are impartial and variations are the result of chance rather than bias. Many credit card acquiring companies are presently in a process of outsourcing their credit fraud detection operations to external suppliers. AI-driven solutions are able to continuously enhance their model results and refine the detection of anomalous behavior. The drivers of modification requests determine the type of samples that are selected for model retraining. By sharing labeled request data, algorithms can minimize bias choices due to cultural, ethnic or gender factors.

8.8.1. Data Privacy Concerns

The concern about data privacy in the use of AI-based models has several dimensions, from some data protection regulations and the potential breach of users' private information, to the legal and ethical responsibilities of the companies developing these models. Credit card transactions are pervasive and continuous, relatively easy to track, and linked with a multitude of other personal data sources publicly or privately available, which creates a unique environment that can drive customers to avoid transactional activity because of the fear of having sensitive data misappropriated or misused.

Data protection regulations aim to give back control of personal data to citizens and residents and consider the business and regulatory environment fundamentally changed. The fines that can be imposed for data protection breaches are enormous, amounting to significant financial penalties. Such enormous financial penalties may lead several companies to engage in reviewing procedures for collecting, storing, sharing, and processing users' information to guarantee compliance with the regulations, which may end up detracting from their efforts.

The provisions set forth by data protection regulations may impose limits on the amount of data credit card companies are allowed to collect and use when assessing risk with AI-driven technologies. For instance, collecting personal transaction-related information can be prohibited depending on the objectives that the company seeks to achieve. Local regulation can require companies to obtain prior consent from customers for data acquisition and processing, and grant customers the power to ask for the erasure or rectification of their data.

8.8.2. Algorithm Bias

A major challenge in implementing AI machine learning solutions is bias in the selections that the algorithms produce. Data sets used in the development of AI must be representative of the groups being studied. Both under-representation and over-representation can create problems for AI solutions. Imperfect data sets can also influence the initial bias of algorithm results. In the AI model training, particularly the supervised learning type, a “teacher” sets the desired answer on the training data set. While the training data set ideally should be free of bias if the data is imperfect the training output can amplify this existing bias.

As applied to credit cards fraud detection, risk assessment and credit decisions, algorithm bias can have serious consequences. If a data set is biased or discrimination exists in the training stage, or if the AI bias is not corrected, the algorithm’s final selections run a high risk of being biased against either entire groups or entire types. Groups of consumers may be unfairly treated because of a higher incidence of delinquency rates based upon a particular ethnicity, belonging to a minority group, or socio-economic background. Consumers may also be unfairly treated from being excluded from receiving certain benefits associated with low-risk determinations when development of algorithm results is determined to be lower than true risks of delinquency. Without sufficient input from diverse community stakeholders in proper data selection, future AI-related decisions will likely produce biased outcomes.

8.9. Risk Assessment in Credit Card Transactions

A significant and ever-present source of loss for credit card networks is card fraud. Card fraud originates from an individual not authorized to use the card attempting to complete a transaction using the card. Using the cardholder identity in a secure manner is critical here, although card networks are generally very forgiving of the cardholder if fraud occurs, as they know goods are still delivered, and the merchant may still have a significant loss when delivering the goods. Instead, fraud is primarily a loss for the network, and additional issues arise if the transaction is conducted in another currency without using domestic currency cards, as currency fluctuations mean that the dollar cost of the transaction may change between the time of booking and the time of delivery. Other non-recovery events occur in the transaction, such as not delivering goods and services, and, in some walk-in retail stores, over-the-counter theft, as here, the merchant has significant costs and losses, which can also run to hundreds of billions of dollars no matter the location of the incident.

Losses from card fraud have increased significantly in the last few decades, although transaction amounts also continue to increase rapidly, so that the loss rates have slightly decreased. The risks from fraud loss are exacerbated as more and more security risks are taken on not only by the credit card networks but by the credit card companies and intermediaries, including merchants, payment processors, e-commerce sites, wallet providers, banks, and account providers. These parties are all responsible for transactions, with the network being the risk party of last resort. It is estimated that combined losses to credit card fraud were caused by risk parties other than the network itself, while the total loss was significant.

8.9.1. Risk Scoring Models

The problem of fraud detection in electronic payments like credit card transactions and credit card network management have been largely reduced to risk scoring. Transaction fraud occurs when there is true fraud. That is, the credit card number, which could otherwise have been sold legitimate transactions, has been either stolen from the owner through phishing, skimming, or social engineering. When done by a hacker or by organized crime, the credit card is used on a site, usually foreign, selling fraudulent, hacked goods or services, e.g., stolen telephone service from frauded telephone services accounts; hacked gaming services, or goods from hacked businesses. In such cases, the business selling the services without receiving payment has not been done any bodily injury, and will not be able to prove penalties that apply to joint owners. To deter such losses, businesses use chargebacks, where a transaction is reversed and funds returned to the victim. Any affiliate of the party allegedly suffering loss from the transaction has standing to sue for losses that arise from the falsely credit transaction, and as well for recovery of losses sustained by other affiliates. But these chargebacks are not fraud detection, as there the fraud has already occurred.

In the credit card payment processes, independent of the country, the network creates a risk scoring model. Each model is responsible for ranking the transactions and altering merchant and issuer behaviors in order to detect or reduce the losses from a fraudulent transaction. There exist proprietary models but generally there is a model from each company implementing the network and a network model. There are a number of proprietary models and it's important to know how to find them or what they may contain.

8.9.2. Dynamic Risk Assessment

One of the shortcomings of the risk scoring systems is that they create a static model that is valid until re-calibrated. This means that the scores assigned to the various types of credit card transactions are estimated based on historical data and that these scores do not adapt to changing conditions such as changing consumer behavior, financial markets conditions, world events, credit card network policies, and so on. While this is suitable for certain tasks, it is a serious problem when you want to dynamically manage the risk associated with a credit card transaction as you would like to react to changing conditions, for example, by increasing the score of a certain risk factor when you see an increase in the probability of fraud for those transactions for which that particular risk factor is relevant.

In this section, I will describe a framework for credit card transaction risk assessment that creates a risk score that dynamically reacts to changes in the incoming transaction stream. This framework is inspired by dynamic risk factor models that give the risk factor used for the risk scoring a dynamic structure. Dynamic risk factor models allow you to create statistical estimators that receive at each time tick the risk factor that you want to estimate and provide an estimation of the risk factor that you want to estimate at time tick t. By using these estimators, it is possible to construct a risk assessment model that assigns for each transaction the value of at the next time tick. This value will depend on the behavior of the risk factor that is used for the risk scoring, which is common to all transactions, just as the value of a credit risk model assigns to a corporate client depends on the value of the risk factor that drives its credit risk. The advantage is that, by construction, the value of the model will react (quickly or not so quickly depending on the model specifications) to the values taken by this common risk factor.

8.10. The Role of Data Analytics in Risk Management

A critical part of many fraud detection and risk management initiatives is the analysis of a large amount of data or information. Data analytics focuses on enabling organizations to derive insights and meaning from their data. Meanwhile, predictive analytics involves the use of statistical models and algorithms to discover relationships among the data and make predictions based on the data. Many organizations have developed extensive data analysis and predictive modeling capabilities to assist them in validating transactions, managing merchant accounts, managing chargeback portfolios, reducing losses from fraud and managing various aspects of risk.

There are several areas where data analysis plays a key role. In many instances, the ability to rapidly analyze a specific transaction to identify potential issues is considered significantly. This can either be a real-time transaction or a pre-authorization transaction. For example, the applicant for a credit card account requests to make a purchase at a retail establishment and the merchant utilizes a card to request payment for the goods or services. Data analytics plays a role by examining factors such as the amount of the transaction, the location of the point of sale terminal, the name of the retail establishment, the type of goods or services being purchased, the type of card being presented, the characteristics of the cardholder, whether the cardholder is utilizing the card for the first time or has a track record of usage, and other factors, and checking this against exceptions that have been predefined in the predictive algorithm.

8.10.1. Data Sources for Analysis

Before deciding which risk analytics tools to use, organizations must first identify the potential data elements that contribute to risk and require data capture, cleansing, and warehousing. The following sources of data are worth considering. External data sources are good for assessing a corporation or municipality's financial health or liquidity but are not sufficient alone. Internal transaction-level information from the enterprise resource planning system shows annual spend, payment terms, and vendor details. Legal contracts with the vendor may include direct payment terms and grace period allowance. Accounts payable data gives risk managers visibility into executed contracts and payment terms at a minimum as well as transactional information relating to the underlying goods or services. Contracts for financial instruments held by the treasury department represent another type of exposure with terms specifics such as counterparties, hedged bonds or share classes, notional amounts, currencies, durations, and option features. A/P and contract data provide the basis for identification of at-risk relationships between the organization and its external parties.

Data mining software working in conjunction with data capture can be applied to purchase order, contract, and exception detection identification. Monitoring of cross-organizational and exception aggregation will identify unusual spikes in flight activity for audit review. In addition to the risk-useful data already identified, software tools exist that monitor parental relationships and where individuals are involved in multiple related transactions. Project and department allocation in the A/P system can at least surface areas of interest related to company business objectives. With bridge events an annual consideration, review of P&L allocation for the activity should identify spikes worthy of further evaluation. The entity-level controls within the organization should be accessed for sufficiency. Identification of a parent-subsidiary relationship will shape the risk analysis such that no major surprises are presented, either favorably or unfavorably.

8.10.2. Predictive Analytics

There are several different types of data analysis, each offering unique advantages. One category, descriptive analytics, focuses on summarizing what occurred and why. In credit risk decisioning, this can take the form of cohort analysis, which identifies customer segments that historically performed well or poorly. This approach can be useful for assessing risk within existing portfolios, but it has limitations; it offers no predictions about the future, and it cannot be relied upon to identify new collections of high-risk individuals. Other forms of descriptive analytics can summarize how underlying risk factors for credit risk change over time, helping to reveal specific economic or demographic factors that lead to a rise or fall in credit risk.

More useful for predicting missing behavior are inferential statistics, which use historical data to create simple parametric models of key relationships among data. Such models can then be used to predict specific components of missing behavior, explain data that remains unexplained by cohort analysis, and help throughout the decisioning process. There are caveats to this inferential approach as well, the most important being the simplicity of the relationship structure that can successfully be considered. The real world is complex, and it is possible to build models whose simplicity is their downfall, as they cannot adequately predict patterns in data that they have not learned. In this context, the applicability of such models, particularly to collections decisioning, is limited, as their performance is conditional on data for recent periods.

Finally, using such predictive analytics makes it possible to build significantly better forecasts of risk components that inform the risk management decision than can be built using either cohort analysis or explanatory analytics. Such forecasts become very important in deciding what degree of conservatism should be factored into risk management decision.

8.11. Case Studies of Successful AI Implementation

In the previous sections, we demonstrated how neural networks and other AI techniques could provide significant improvement in performance metrics compared to existing solutions for very large application domains. These statistics, however, do not guarantee success, as the cost involved in developing an AI-based solution is quite large. In this section, we provide some interesting real-world examples of the successful application of AI solutions to domain problems.

Bank A realized that only about 10% of credit card transactions by their customers were genuine payments, with all other transactions being fraudulent. Ninety percent of the transactions were therefore false positives, leading to existing systems incorrectly flagging these transactions as suspicious on 90% of the transactions. This led to a large number of false alarms that used up a lot of time by both card holders who were contacted and self-service bank personnel who had to handle the calls from card holders. As a consequence, Bank A lost millions of dollars in falsely rejected transactions and had to deal with huge call volumes from both merchants who lost business and card holders whose credit was not valid.

Bank A deployed a neural network-based AI fraud detection system that reduced the false positives (90% in the existing model) to about 25%. The system ran on closed-loop transactions, allowing Bank A to acquire existing real-time data from the fraud detection device. During the first year that it was rolled out, Bank A saved millions of dollars. It did not have to throw more resources at staffing up its fraud centers and self-service facilities to handle more false alarms. It saved additionally by being able to detect the real frauds earlier and impose transaction limits on these customers. Thus, Bank A was able to significantly reduce its losses that it would otherwise have suffered by being late in controlling the fraudulent transactions.

8.11.1. Bank A's Fraud Detection System

The AI system is used in Bank A to score the risk of transactions. Each transaction is assigned a risk score, which is then compared against a threshold to determine if the transaction should be accepted, flagged for manual review, or rejected. Predictive models are triggered at different steps in the decision-making process to predict the likelihood of that a transaction being erroneous, and if so, if it is chargebackable, if the fraud consortium is to be consulted, and whether the merchant is to be reviewed. Other models predict the probability of loss and the expected cost of false positive and negative decisions. Fraudulent transactions can cause chargebacks, which are refunds that a merchant is obliged to make for an online payment, which are initiated by customers who claim fraudulent use of their payment cards. These transactions should be detected beforehand by fraud prevention systems to avoid merchants issuing refunds afterward. The system lacks in providing useful information in real time about merchants involved in transactions. For the system to detect withholding reasons on specific merchants to better help the customer decision makers should count resources needed to evaluate chargebacks from specific merchants.

In addition, the AI system uses as input a variety of card, transaction, merchant, and trade information and feeds its output to an automated decision-making system. The AI system outperforms simpler models and is selective in that a small number of transactions generates most of the system losses when compared to a human expert-based review process. The AI model has been successfully used to reduce the nuisance of prior fraud defenses. The credit card business is a high sign-on cost business and, therefore, easy prey to fraud by cyber criminals during its first negotiations and business years. For a credit card company, a high fraud rate is an expensive strategic bottleneck. Lowering it helps the company to gain and retain customers while increasing individual returns.

8.11.2. Retailer's AI Risk Assessment

A large international retailer selling online some of the largest volume categories – consumer electronics and toys – receives digital marketing investment from hundreds of important brands to help drive brand and product awareness, traffic, and sales while offering the most comprehensive selection of products. The retailer has a proprietary marketing and analytics technology stack primarily focused on helping brands achieve their marketing goals. Fully aware of the damage caused by fraudulent schemes, the retailer has implemented an AI-driven risk assessment module to protect its seller ecosystem from scam and illegal activities.

The AI risk assessment module scores the financial risk associated with each seller on-boarded to the seller ecosystem via two different CRMs: self-service multi-scope and dedicated full-fledged scope. Risk management is necessary for both scopes but is more stringent for the dedicated scope given its strategic relevance. The risk model acts as the first line of defense before blockers are legit-checked by the customer success organization. The expected revenue is computed for a seller onboarding request leveraging the proprietary algorithm. The retailer is forced to legit-check thousands of sellers monthly, which can only be done in an automated way beyond a certain risk score. Some sellers can pose a potential large-scale financial risk threat to the retailer, thus bias remarks or requests showing a relevant black flag must be verified in any case. For cost savings optimization purposes, only a selected group of sellers must be legit-checked regardless of the risk model score assigned to the seller.

8.12. Future Trends in Credit Card Fraud Detection

The predictions from experts hint at a number of exciting new fraud detection strategies hitting the market. With its integrity, transferability and rapid settlement capabilities, Blockchain technology promises to be a revolutionary technology in fraud detection. It can minimize the increasing risks and costs of credit card fraud. The suggestion is for credit card issuers to use Blockchain and Cryptographic Hashing to automate key steps in the transaction process, where users transact with their wallets without relying on highly secured centralized locations. The solution relies on allowing free and interactive transactions and allows customers to authenticate multiple transactions through the transaction's identity and hash value, while creating a unique block for each transaction, which will be added to the block-chain network. This provides a "third and trusted party," the network, which validates the payment, thereby reducing the fraud risks artificially implied by merchants at a cost which is identified as being shifted back to the credit card's issuers and their customers.

While credit cards usually stipulate the use of Strong Customer Authentication, that alone cannot altogether eliminate the possibility of fraud. Recent trends may point towards enhanced biometric alternatives. Banks typically employ voiceprint, palm and finger scanning, heartbeat, and facial verification for biometric protection. The potential of Card-Not-Present transactions, with the authentication stored in the device, oversight, or device capability is massive as of now. The benefit from having an integrated biometric revenue stream could lead financial institutions to invest massively in biometric credit cards, enhancing both user experience and security. These institutions could thus also implement third-party biometric card feature providers or partnerships at early stages, decreasing costs and spreading risk in many transactions overridden by risk signals.

8.12.1. Blockchain Technology

Blockchain technology was originally designed for the Bitcoin cryptocurrency. The blockchain for each Bitcoin transaction is stored on a peer-to-peer network of thousands of computers. Each transaction, along with confirmations of its validity from the network, is stored in a publicly available ledger containing a growing list of records known as blocks. Each record has a timestamp and a cryptographic link to the previous transaction. Whenever a new block in the chain is confirmed, the blockchain is updated in all computers on the network. As a result, creation of false entries in the ledger becomes nearly impossible. Original authorship of all transactions is securely retained, thus preventing the users from repudiating any past transaction. Digital signatures using public key cryptography ascertain signer identity and authenticity.

Blockchain technology promises new mechanisms for detection and prevention of consumer fraud. Different versions of blockchain may be used to secure credit card and related details. Blockchain technology ensures that identity manipulation during a transaction cannot occur. The private data is encrypted and, together with a digital signature, is stored within the blockchain. The unique transaction stored in the blockchain is immutable and will always point to the unique encrypted identities of both the transactor and the transaction holder. Blockchain technology functions as a decentralized and unbiased digital third party for transactions occurring within an information ecosystem. Blockchain technologies can be integrated with existing credit card and payment architectures for near real-time credit card fraud detection. Functions like monitoring transactional metadata can be enabled by adding new fields in the existing data architecture for data files. Enhanced, near real-time forensic analysis can be implemented. All parties concerned benefit from saving the cost associated with fraud detection.

8.12.2. Enhanced Biometrics

Personal identification numbers (PIN) are an established form of identity verification but have become impractical for verifying retention identity during face-to-face payment transactions. Verifying identity has become particularly problematic for card-not-present transactions such as online purchases. The traditional method of cardholder verification is the credit card number and expiration date. These numbers can be easily harvested and reused. Other measures include:

– Requiring the user to pay an additional fee to have a credit card sent to their street address. The credit issuer will normally send the card through regular mail, while the PIN will go through special delivery. It is easy to obtain old cards before a cardholder identity can be verified and steal a valid user's identity.

Sending the person a one-time password (OTP) or contactless verification over a cellphone that must be entered before making the online transaction. These fail if the customer does not have a cell phone. It also leads to social media spoofs and falls short for identity verification since possession of a cellphone is not sufficient proof that the cellphone belongs to that person.

We propose the use of definitely expanded biometrics. A typical biometric is a measurement of unique physical characteristics used for identification purposes. A brief survey of enhanced biometrics may include using or combining several currently available systems for more reliable verification procedures. Fingerprints are the classic ethical biometric system. However, some people may not have fingerprints, plus physical systems can deteriorate with time. Alternative or additional methods for biometric processing could involve systems based on: Voiceprints; keystroke cadence; retinal vein pattern recognition; heart or heartbeat rhythm; pulse or ECG; and/or ear shape.

8.13. Regulatory Considerations and Compliance

As part of the ecosystem of actors involved in financial as well as credit card payment transactions, credit card networks have to take into account regulatory considerations for consumer protection and risks. They also need to comply with data protection regulations of some regions. Some key regulations that impact the way credit networks manage and sustain credit risk throughout the lifecycle of cardholders, in particular using machine learning techniques are described next.

Data Protection Laws require credit networks to protect the privacy of each consumer's data. Global Commerce must comply with data protection regulations. The applicability of these regulations is triggered when consumers give explicit consent to the processing of their data. These regulations aim to protect the confidentiality of personal data including social security numbers, credit cards, bank accounts, passwords and digital identity as well as behavioral data such as cookie tracking online so that identity cannot be inferred. They describe the set of citizens' rights about data protection: Rights of Access – the consumer has a right to obtain confirmation from the Data Controller whether or not personal data concerning him are being processed; Right to Erasure – consumers have the right to obtain from the Data Controller the erasure of personal data concerning them; Right to Data Portability – consumers can receive their personal data in a structured, commonly used, and machine-readable format; Right to Object – consumers have the right to object to the processing of their personal data.

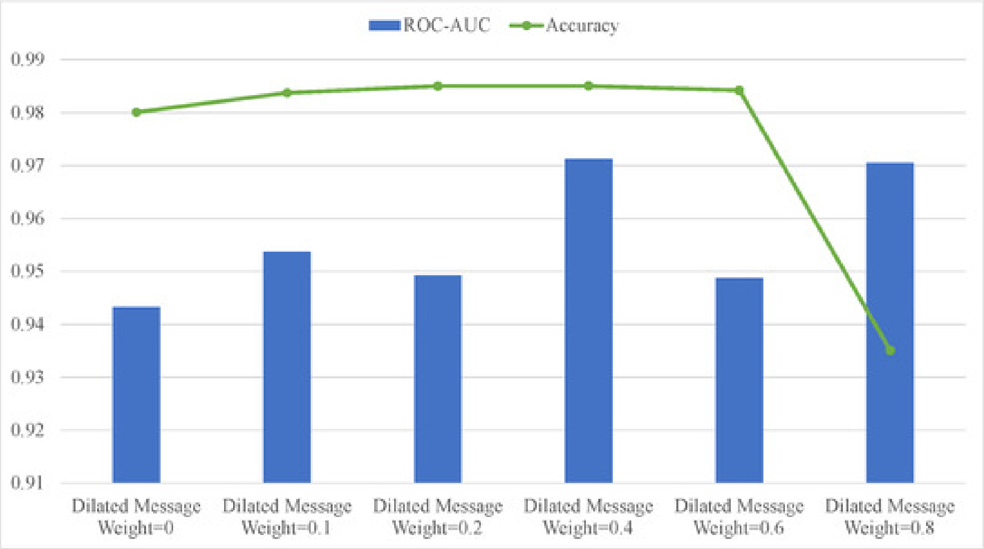

Fig : Advanced Credit Card Fraud Detection Using Federated Learning

On the other hand, the requirements for data protection also apply to credit networks in terms of protection of cardholder data, activities related to card modules such as authentication and balancing and cardholder data management through secure systems.

The requirements provide a framework for compliance. The core of these requirements lies in encryption of cardholder data with restricted access as well as data logging, access control management and monitoring security measures to protect customers against unauthorized use of credit cards in case of fraud.

8.13.1. GDPR and Data Protection

The General Data Protection Regulation establishes a robust regulatory requirement regarding the processing and protection of personally identifiable information. Personally identifiable information is defined broadly and payment transaction data could fall into this definition. Many aspects of credit card processing require compliance, including secure disclosure to the consumer, management, and protection of personally identifiable information.

The credit card processing ecosystem involves multiple stakeholders, and personally identifiable information is typically maintained in the processors risk analytics engine, on merchant POS systems, and in cardholder proprietary confidential information, which can be compromised in the case of an irreputable merchant. All of these areas must be in compliance with the terms of the regulation. In fact, a frequent advisory opinion from regulators cautions any company who processes the personally identifiable information of residents to assume they are subject to the regulation, regardless of the nature of the company or where their operations are headquartered. As a result, from a legal standpoint, the regulation always applies if the data subject market is targeted or present.

The challenge for companies operating in the financial services and payment transaction space is determining which party to the transaction is responsible for what aspects of compliance, and that each party has sufficient protections built into the merchant and operational agreement to assure compliance with industry best practices. For example, the processors risk analytics engine captures large amounts of data including the consumers and merchants bank accounts, devices, transaction amounts, and payment flow structure. These controls are implemented across multiple teams, including architecture, development, cloud services, data, operations, product, and security. Each team has a designated risk associated with the role they play in the information lifecycle and has the relevant controls in place to satisfy those risks. The teams work together to implement controls and procedures that satisfy the requirements.

8.13.2. PCI DSS Requirements

The PCI DSS is a set of security standards designed to ensure that companies that process, store or transmit credit card information maintain a secure environment. These security standards are intended to prevent credit card fraud through their exposure to compromised data. The PCI DSS represents a unified effort among credit card issuing banks and various major credit card brands to ensure the integrity and safety of the global payment system and, in turn, protect the growing amount of sensitive personal information being stored by organizations today. As such, any organization that accepts, transmits or stores cardholder data must comply with the PCI DSS. The PCI Data Security Standard (PCI DSS) is just that: Data Security Development Standards. They do not by themselves ensure safety or security, they merely state how a company should go about accomplishing that goal. The PCI DSS contains six goals and twelve main requirements.

In the following section, we discuss these key requirements and the implications for credit card networks risk assessment. When validating compliance, an organization determines the level or levels of credit card acceptance relevant to them as well as whether or not they are part of a 'sensitive' parent level organization. If so, they must validate compliance at the highest level. Otherwise, the levels or levels of credit card acceptance apply. The requirements are commonly grouped and read as follows: build and maintain a secure network and systems—install and maintain a firewall configuration to protect cardholder data; do not use vendor-supplied defaults for system passwords and other security parameters; protect stored cardholder data; encrypt transmission of cardholder data across open, public networks; maintain a vulnerability management program—protect all systems against malware and regularly update anti-virus software or programs; develop and maintain secure systems and applications; implement strong access control measures—restrict access to cardholder data by business need to know; identify and authenticate access to system components; restrict physical access to cardholder data.

8.14. Conclusion

The world is rapidly adopting credit cards or, more generally, information networks that support electronic money. With these changes come a flood of new banking regulations and new banking products. Many of these new products will race through the marketplace only to collide with fraud. What often begins as the imitation of an honest service, progresses to cheating and a general breakdown of the system, is then met with artificial intelligence driven risk assessment, which creates the possibility of a new cycle of innovation, fraud, and control.

Many new products which aid credit card issuing companies are being created everywhere. One set will provide consumers with increased services that will support a faster implementation of electronic money transactions. At the same time, they will fortify these transactions against the criminal element's latest research results. Other programs will begin the search for the auspicious location around the world. After folding in the bottom additional credit markets, fraud's invariant path through time may be discovered. In this manner, the most successful retail transportation banks will be constructed. Other systems will utilize new approaches to the design of self optimizing internal fraud monitoring programs. These will be the leaders in the internal fight against fraud. They will use AI to help with the problem. The years will be the richest years in terms of the diversity of products from which banks may choose.

In the end, large scale banks, which create a new set of consumer support services, will develop. These businesses will recognize the potential for fraud to ruin these lucrative businesses and will take the necessary steps to prevent fraud. These are but a few of our thoughts on the issue. In the end, the net benefits of attempting to control fraud will rise in the interim, and the business will experience sudden outburst of fraud and supportive interventions.

References:

Gupta, A., & Singh, R. (2022). Predictive modeling in portfolio optimization: A machine learning approach. Journal of Financial Data Science, 4(3), 45–62. https://doi.org/10.3905/jfds.2022.1.034

Chen, Y., & Zhang, L. (2021). Data-driven investment strategies using deep reinforcement learning. Quantitative Finance, 21(10), 1653–1672. https://doi.org/10.1080/14697688.2021.1893847

Li, J., & Wang, X. (2020). Integrating big data and predictive analytics for dynamic portfolio management. International Review of Financial Analysis, 72, 101575. https://doi.org/10.1016/j.irfa.2020.101575

Kim, D., & Lee, S. (2023). The impact of AI algorithms on asset allocation and risk management. Journal of Investment Strategies, 12(1), 28–46. https://doi.org/10.2139/ssrn.3891259

Narayan, P. K., & Bannigidadmath, D. (2020). Machine learning trading strategies: Empirical evidence from global stock markets. Applied Economics, 52(48), 5253–5266. https://doi.org/10.1080/00036846.2020.1733485