Deep Science Publishing
https://doi.org/10.70593/978-93-49910-16-4_5

DeepScience
Open Access Books

Chapter 5: Identity in the digital age and the fight against fraud through predictive analytics

5.1. Introduction

The revolution in information and communications technology (ICT) has marked the current historical period, profoundly altering the speed, complexity, and extent of access to information, power, and control revealing opportunities and threats of unprecedented dimensions. It is evidently possible to spend one's life immersed in ICT, using electronic identity to do business, run banking transactions, interact socially, seek entertainment, or simply go shopping. The vast majority of these transactions are welcome, generating income, jobs, knowledge, information, and entertainment. Sadly, an ever-increasing portion of this identity use is unwelcome and equivalent to eating democracy and freedom. Issues of identity, power, and control reveal a battlefront without a victor. WWII has changed aspects of today's society but has not ended the battle nor brought unquestioned or unquestionable triumphs. Nonetheless, the Internet has fundamentally transformed the relationship between an individual's identity and his/her ability to personally control it. For many, the possession of a physical identity brings access to ICT and the content it delivers. This coalition of identities is like the trunk and branches of a great tree; each assists in bearing the weight of arrivals, providing pathways for information, and maintaining integrity.

The proliferation of vehicles and the gradual growth of e-business naturally expand the scope for e-business fraud and non-compliant behaviour. E-country, with rapid expansion and an ever-widening scope for e-business transactions, is by definition an emulated society of 'individuals otherwise known as elementary logic circuits (ELCs)'. Further given that no single jurisdiction regulates Cyberspace its rapid growth continues without a speed limit. Nonetheless an imitation of the proceedings between Onara and Yenda speeds up the solution on the basis of a number of policy overarching principles

that may apply on a global scale. E-democracies containing significant growth in and reliance on its establishment, venues, facilities or mobility should necessarily have regulators having enforcement powers over terrestrial transactions across the following three regimens to ensure an on-par distribution of benefits, costs and risks.

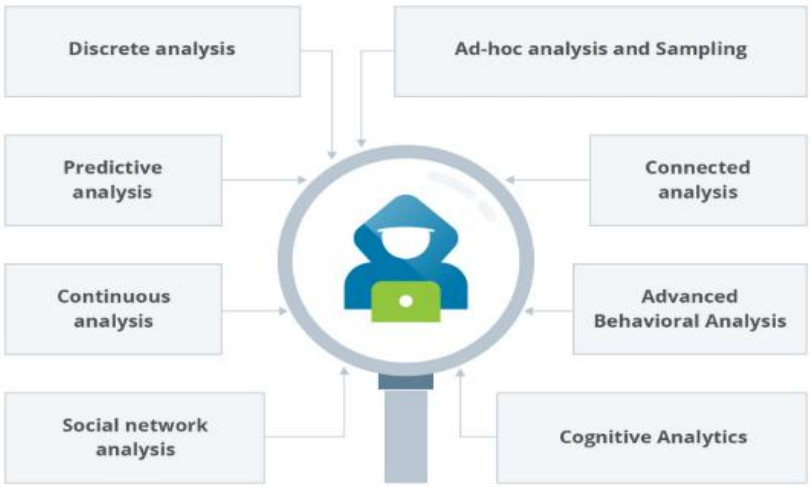

Fig 5.1: Predictive Analytics in Fraud Detection

5.1.1. Research design

Most identity fraud has low evaporating probabilities once an incident occurs. Individuals may be unaware for several months of identity fraud against them, and even fly under the radar of agencies responsible for fraud detection. Data breaches at organizations often predate individuals' awareness by months to a year or more, meaning that organizations may reside in stolen data pools before fraud occurs. Once wrongful transactions do start occurring, victims may not be aware of the fraud until a payment is rejected or collection attempts begin.

A recurring problem in combating identity fraud is the weighing of detection and preventative analysis undertaken by large organizations that are more likely to be targets of identity fraud in the first place. Massive datasets of transactions, changes of customer information, and breaches are cleaned at the expense of missed brands or slow decisions that allow fraud to continue for weeks until enough information is collected to make informed risk decisions. Newer customers are also generally assigned default risk scores at institutions, which can limit fraud detection and prevention accuracy.

A notable exception to this trend is the increased ability of individuals to more closely monitor their own digital identities and take more immediate manual action than the

whole organization can. Factors like increased awareness and ability to use digital identities have created a technical ecosystem that mitigates consumer personas on bigger identities and software providers on larger identities. Non-traditional data service providers, which monitor a wide set of transaction types more continuously than thorough analysis of single accounts is possible, have grown in these years. If these organizations are able to apply many, more subjective, features as scores to identity robustness, decisions may be reconstructed for staged fencing as well as possible.

5.2. Understanding Digital Identity

The concept of identity in the digital world is evolving; however, the same basic questions about identity remain fundamental. An individual possessing a recognizable set of identity attributes is recognized as a person. The same applies to nations, organizations, and businesses. Trust in any such entity arises because of recognition of such identity attributes. In the digital world, identity (digital identity) is defined as a set of attributes belonging to a person, organization or a device and being a part of the identity management system of a trustable partner of communication and exchange. In short, digital identity is a set of attributes about a person, organization or a device and able to determine that this entity is a trustable partner for a certain kind of communication and exchange.

Essential elements of this definition are the set of attributes, ownership of this set of digital identity attributes, ownership of the system and legal use of the personal data, which have been used to define these elements. Some basic attributes are – Name, Country of residence, E-mail address, Date of birth / age, Mobile phone number, Postal address, Bank account number, Driving license number, National ID card number, Tax number, Education, Work history, Sexually transmitted diseases, Criminal history, Employment status, etc. As digital activities spread, the set of personal attributes is growing. The basic social question of trust applies to the digital world too. In online and digital mode, identification is at the center of security and trust mechanics. Two entities need to prove their identity in order to establish a trustable relationship; without a recognized and trusted identity, it can be authenticated whether it is a trustable partner for communication and exchange.

5.2.1. Definition of Digital Identity

In the digital world, each entity is assigned a virtual representation referred to as a digital identity. This digital identity offers individuals the ability to gather resources, utilize services, and engage in social interaction, security, and commercial transactions. Following digital entities takes place through their linked digital identity, which is the

entry point. This gives access to the resources and means of diffusion. Digital identity can be described as a contract where attributes are the set of identifiers that create a reputation linkable to other traits. Online interactions create their own identity. Through these, digital identity creates and influences how it is perceived in the digital space.

Cybercriminals can impersonate any entity, receiving as reputation attributes maleficent raw data only. Information may be posted erroneously, but in any case, it can create confusion based on this perception. In a social environment, rules of acceptance and rejection exist. These facilitate recognition of each digital identity, power of action taken by the entity, and its evolution. Digital identity can be regarded as stable or evolving. A jurisdiction may consider a digital identity as an archived set of identifiers. Based on this representation, these identity attributes will exist or disappear. This means that evolutive attributes accepted by minors may create identities invalid as regulations raise.

A digital identity can be created through a process managed by an external provider. This introduces a moral aspect when entities are used to take advantage of transactions. These entities cannot be faded since they have an effect on a broader relation. They should contain a fixed structure controllable and auditable by the issuer. No one entity may have control on it or all security may be bypassed with the threat of deletion. A digital identity can be regarded as a construction enriched by online social interaction. An entity which uses communication means and a software able to structure those interactions creates an avatar equipped with attributes. This avatar progressively creates itself a unique representation.

5.2.2. Components of Digital Identity

Every day individuals generate diverse types of data linking them with a wide range of organizations, institutions, services, or individuals; up to a thousand of them in a reasonably short timeframe. These data are stored in millions of databases and used for a variety of purposes; some of them for legitimate operations but not all of them (e.g., fraud, cyber-crime, blackmailing, stalking, etc.). A digital identity is constructed which is able to recognize a unique entity among billions of others in the digital world by this number and types of primary data. This identity is built of attributes that include an entity's activities, personal information, credentials, certification, transactions, etc. The concept of digital identity is not new or unique; it has its own origin, and for centuries, its social counterparts have been discussed, and debated by Philosophers and Social Scientists alike.

The question of identification is one of the most important universal concerns for an individual and for the society at large. On the one hand, for individuals, well founded identification is necessary for a stable position in a social and digital society while on

the other hand profiling information can serve instabilities, discrimination, and oppression on societal level. The very first and foremost question of identification is who am I? To enable developers to answer this question correctly and make them invest trust in a digital service, a key component is recognition of identity elements or attributes. Recognized identity is linked to a large quantity of agreements and refuses these contracts on other parties' side, too.

Digital Identity is a set of attributes linkable to an entity created by itself and enriched by social interactions allowing recognition by others as a trustable partner for communication and exchange. Similarly to its social counterpart, the concept of Digital Identity is a social construction, however, social construction could be a too rough description, since the former is a shifting process so individual construction and group construction are not certain to overlap. Digital activities and interrelations are growing with an individual participating in digital life but the way and speeds of this growth differ widely.

5.3. The Rise of Fraud in the Digital Age

In the digital age, the struggle to create new identification and authentication systems has become critical, more than ever. As cryptographers, industry representatives, and governmental agencies discuss and implement such systems, as well as the wonderful innovations they make possible, criminals have already begun to exploit the weaknesses in the systems of identification and authentication being used today. The emergence of digital crimes that take advantage of weak identification and authentication systems or that simply could not have existed without them, is a pressing problem keeping the authorities of numerous countries awake at night. The infecting of a bank's computer or transmission lines by actors outside the organization can cost millions to rectify, while slowing down the entire economy to the benefit of those who would bring it to its knees. Computer viruses that destroy payroll systems or replace salaries with zeros could aggravate unemployment and cause a riot-like atmosphere were they to occur simultaneously at several banks. This rising cybercrime problem seems to have newly defined beneficiaries, victims, events, and situations. Victims of cybercrimes include young hapless users, washed-up hackers, neglected parents, and sleeping grandparents watching their bank accounts dwindle away overnight.

Individuals whose identifications have been hijacked are many, as are charities whose accounts have been pilfered and governments that have lost their visibility. Orphaned patches of digital land are accumulating, dragging along with them addresses and authentication codes still covered or despised. Bankruptcy and restructuring are resetting the economy, as thousands march in protest. A new economy, organizations, goods and services are all emerging through the clouds – the clouds that bring cyber-information

and conceal its actors. Who are they, these agents of fear? Are they lone hacktivists, small groups, big mafia organizations, or even foreign governments? Are they boys futzing at home? Ten-year-olds pirating a botnet? Drain-certain theory epidemics difficult to contain? Police, secret-service, agents provocateurs? Unreflective revenge-takers, cold-blooded profit-maximizers, or rough-humored practical jokers.

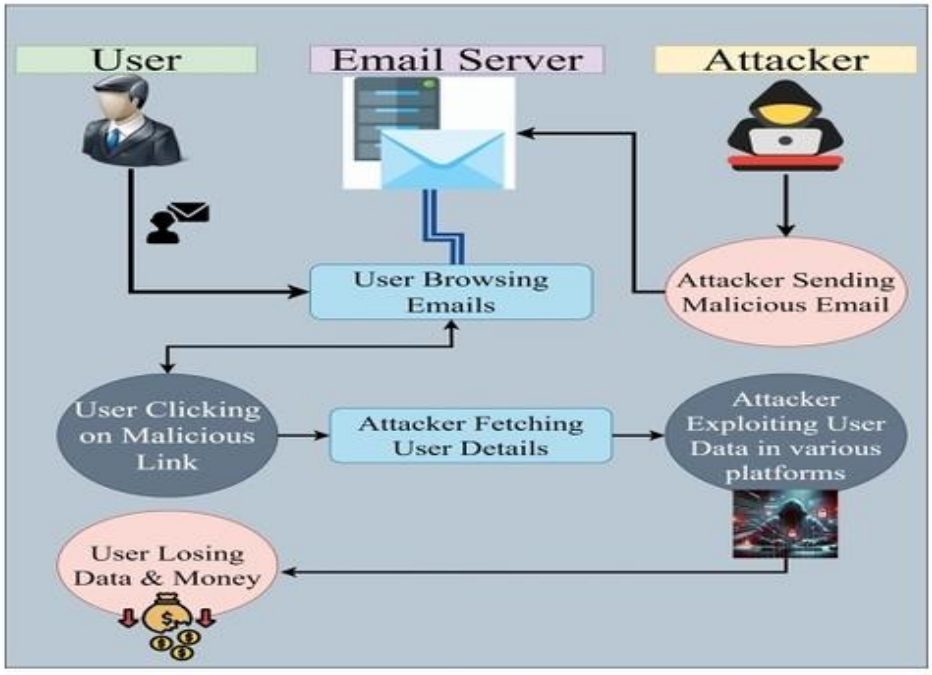

Fig 5.2: Fraud in the Digital Age

5.3.1. Types of Digital Fraud

Digital fraud flourishes in the context of weaknesses, and in virtually all concerns and systems, weaknesses exist. The distribution and access to information in the e-business world exceed even the broadest definition of the expression “free market.” Rapidly developing and robust information technologies assist the common consumer, but they also provide criminals with potent “tools of the trade.” Electronic office automation techniques have increased fraud schemes which, although not new, have changed form and complexity. Traditional scams have become more difficult to recognize and more costly to investigate. Complaints from the public are at an all-time high.

Fraud can be defined as any wrongdoing in which the perpetrator gains a benefit at the expense of the victim. It may occur in many forms, but most are broadly classified as either “Non-digital” or “Digital” fraud. Non-digital fraud consists of schemes, or scams,

which are carried out without the use of information technology. The formation and implementation of non-digital fraud schemes remain fundamentally unchanged over time. Although they may evolve to perform this function more effectively, their essentials usually remain the same.

Digital fraud comprises schemes and scams and are executed with the use of digital information technology. Digital fraud has become more complicated to commit and to detect than ever. The Internet has enabled digital fraud to flourish as it has vastly multiplied the number of possible victims. Scams that might previously have taken months or years to permeate the public information geography can now manifest themselves worldwide within hours. E-mail spam has been used to disseminate numerous online schemes, some combining the traditional energy-draining manipulation of prospect victims with the speed, reach, and deception made possible by digital technology.

5.3.2. Impact of Fraud on Individuals and Organizations

Fraud in its various models and settings financially impacts both individuals and organizations. Individuals fall prey to medical identity theft, stolen medical records, and fraudulent claims submitted to insurance companies. The fraudster usually submits billings under stolen identities to obtain payment for services that were not provided, and both hospital and patients suffer fiercer losses. Worse, misused identities have credit information stolen and someone else's credit history victimizes them when financial information is stolen. Also, information in credit bureaus related to a patient's credit history in the hospital system allows the fraudster to purchase drugs under the credit or to obtain auto loans and furniture loans through stolen identities. Stolen information from insurance companies is less likely to be used for an insurance market where claims are invented fraudulently using stolen IDs. Fraudsters have a wide array of advantages where they profit gross amounts from millions of patients whose identities are misrepresented, and insurance companies that are made to pay false claims.

Organizations are troubled with malpractice insurance fraud resulting from employers, doctors, or service providers who falsify case claims by creating fictitious injuries and fraudulent witnesses in hospital or home visits. Also, retired professionals that fraudulently executed home care cases enabled them better medical care with the deductible expenses covered by states on patients that imposed false receipts. A hospital is cheated with thousands of dollars by a worker that sells its expired drugs in a pharmacy. Medical frauds impose billions of losses annually. Healthcare fraud costs organizations financially as a minor payer that accrues the largest losses when vendors or employees deceive national scale operations. If fraudulent bills are still being paid, audit processes and fraud detection escalate expenses. Moreover, audit processes

introduce paperwork, calls, and time in insurance companies that negatively affect audits' effectiveness and efficiency. These are put in backlogs creating delays in payments. Fraud costs for an insurance company cannot be measured in monetary expenditure terms only, but they also consist of non-tangible indices like human assignment errors resulting in late payments.

5.4. Predictive Analytics: An Overview

Fighting fraud is challenging in the era of ai-assisted automation when humans can no longer be entirely in control of machines, machine-generated content (MCG) is ubiquitous, and online scams are rampant. It is also difficult to reach jurisdictions with no regulatory controls and safety nets, or to address emergent fraud areas of types or methods. In addition to having all sorts of capabilities and expertise in fighting fraud, predictive analytics, a technical commodity now ready to deploy, is harnessed for the purpose. Key techniques and methodologies of predictive analytics that are susceptible to fraud are examined to provide a theoretical foundation for its deployments.

Predictive analytics (PA), an asset to understanding the present and foreseeing the future, has been researched and transacted for decades. Production volume and applications of PA are booming. Many reputable software companies provide statistical software for classic PA, machine learning, and deep learning. Original PA implementations have been revised and upgraded significantly [2]. Machine learning renders the traditional PA technical commodity even cheaper and more accessible than before. Big data acquisition systems significantly lower the overall cost of PA by recovering the cost of data and infrastructure. This onrush of infrastructure, resources, and technical feasibility unleashes the potential of PA. Data has been collected at a convenient cost, and software implementation is available free of charge.

Fraud detection is a major application of predictive analytics. It not only saves losses but also prevents further fraudulent content and machine generated content from being generated and disseminated. Fighting fraud addresses humans in new dimensions. In contrast with slowly evolving off-line nature of humans, new types of online fraud have unprecedented measures of speed, in-genuity, and scoping:

Current tools for fighting fraud either target narrowly specified types of fraud or are not adequately tested in practice. Interdisciplinary expertise in fighting fraud is scarce, and deep partnerships with the knowledge available to schools of intelligent information technology that recently emerged are called for. While a wide range of application areas of counter fraud has been classified, the process of criminality from which fraud emerges has not been studied. Predictive agents have yet to be fully employed for criminality detection, as fraud emerges as unlabelled data which can be jurisdiction-specified.

Fraud detection in the current state of analysis is, in broad strokes, an error classifier trained to identify occurrences of this exception. Analyses are monitored, where patterns in algorithms are used to classify functions. Prediction analysis functions in a different environment, proposing data classes from fuzziness. As a result, a score function with a certainty level about how likely a class is present is produced. Recharge of predetermined knowledge, a score may be used inductively to set a new classifier or to augment the existing classifier with complete new knowledge, improving its performance to recognize it and, inevitably, its misbehavior.

5.4.1. Definition and Importance of Predictive Analytics

The tremendous growth of web technologies, facilitated by the expansion of the internet, communication speed and capacity, mobile access, and new social media platforms, has changed consumer habits and business strategies. Even the ancient integrity of brick-and-mortar stores as the main points of sale has been overcome, giving rise to e-commerce and virtual marketplaces. In addition to these benefits, this enormous leap into digital transformation has also generated challenges, including the rise of online fraud. Organizations lose an average of 5% of revenue due to fraudulent acts, much of which pertains to the online environment.

Fraudsters can be anyone from identity thieves and hackers to competitors and ex-co-workers or even from internal organs like angry employees. In any case, the professionals and businesses targeted are harmed by life-threatening monetary and reputational losses. Isolated, these losses are considerable, with average direct losses of US$1.7 billion attributed to digital payment fraud, US$338 billion in fraudulent transactions across online marketplaces, and US$908 billion in fraud losses for US banks.

5.4.2. Techniques Used in Predictive Analytics

Despite the vast array of odds-based and transaction-based models, few of them successfully capture the unobserved information that would better inform analysts. Rather, transaction-based models are designed to create “dark” behavior, which suggests the background within the analyzed data. In contrast to odds-based and transaction-based models, predictive models inform early detection fraud alarms. Traditional models typically use rules that only rely on the history of transaction data, and expert knowledge might be limited due to the extent and complexity of observed behavior. The additional hidden dimensions of user activity open up new avenues for investigation [7]. This allows for meanings to be assigned to trees that represent descriptive features of user devices, behaviours, venues, and times at which they

transact. These additional dimensions might indicate fraud. Unlike odds-based and transaction-based models where input parameters are estimated as static inputs or series, the output of predictive modelling is taken as stand-alone questions or targeted alarms to fraud analysts. Despite the importance placed upon analyst feedback globally, very few models necessitate an analyst's input or present informative reasoning behind the case. Importantly, tree-based models present relevant questions and indicators to analysts that often elicit further investigation.

5.5. Using Predictive Analytics to Combat Fraud

Modern organizations face the challenge of helping fight fraud. Companies are increasingly concerned about fraudulent behaviour and the critical impact it can create on corporations. Therefore, it is necessary to gain a comprehensive understanding of predictive analytics and how it can ultimately help to anticipate and detect fraud. There is evidence in the literature that fraudulent behaviour prediction in a betting environment can take place in real time and efficiently. An approach has been proposed for challenging this task that consists of a novel, general, and extensible data preprocessing pipeline and supervised and semi-supervised learning methods, based on LightGBM and Gated Recurrent Units models.

A real-world betting dataset containing more than 15 million bets has been employed, using which the proposed approach detects numerous previously unknown cheaters that generate suspicious betting behaviour. Following the previous works, an infrastructure is coined, that allows extending that work to large, real-world databases and to develop novel approaches both on data preprocessing and on the modelling. Due to its flexible architecture, it may partially use the approach already developed using other data bases or specially designed to study different phenomena, such as reinvestment and moderation strategies.

The introduction of the Internet of things (IoT) has brought new opportunities to the world, but also unprecedented challenges. These opportunities are related to a vast increase in ex novo information availability, which gave rise to the Big Data paradigm. Fraudsters are known to be very creative, and on average, they are more intelligent than the capabilities of existing tools. Therefore, organizations are aggressively trying to develop systems and algorithms that will constantly learn new how fraudsters behave. On the other hand, Game Theory has the potential for understanding and modelling fraud detection, but it has not yet taken into account how this understanding can be translated in the context of predictive analytics.

Fraud is a major concern for most organizations today. It is estimated that organizations worldwide lose 5% of revenue per year to fraud, representing a projected annual loss of more than $3.5 trillion. In this context of organizations that increasingly store vast

amounts of data, it is important to maintain an edge in investment on information technology and build systems that would allow detecting fraud before it occurs. Acknowledgment that a broad set of factors impact fraud behaviour is growing. Different systems of automated rules and monitoring that aim at anti-fraud purposes differ in efficiency, highlighting the complex environment of fraud and evidence that benign behaviour can be sophisticated and mitigated.

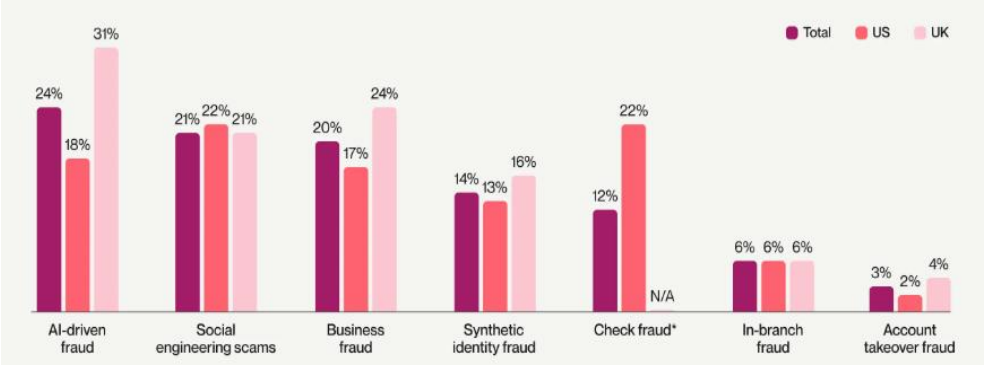

Fig : Financial fraud prevention

5.5.1. How Predictive Models Work

Fraud prediction is the prediction of the likelihood of a transaction being defined as fraud by the organization, for example, by setting a threshold discriminating fraudulent and non-fraudulent occurring events. The atypical transactions can represent extremely valuable information, so it is important that no information is lost during the operationalization of the solution. Initially, each transaction is described by a set of variables and a binary variable indicating whether the event was fraud or not [2]. These fraud events are rare, so a fundamental pre-processing phase is the construction of representative datasets, in which it is ensured that these populations are more balanced. This is possible through sampling strategies or using the full non-fraudulent population. Random samples are used because they allow for departures of the theoretical assumption of statistical methods, automatically taking the complexity of the process into account.

The next step is to model the fraud behavior after understanding how the information is structured. By using supervised classification models, the target variable is a piece of information known a priori and continuously asymptotically observable with relevant quality. Following other workflows, the focus is on three types of supervised classification models, specifically the gradient boosting algorithm, which is recently getting more attention because of its performance and flexibility. To solve the problem

posed by credit card fraud detection, such as how to define, pre-process, and analyze the transactions and how to build classification models to predict erroneous classifications, both in the classical and machine-learning sense, methods and results showing how credit card fraud detection problems can be addressed by data mining techniques. In detail, commercially adapted model evaluation and comparison techniques give the analyst a clear insight into the results of classification performance: the standard prediction accuracy, confusion matrix, error prediction cost matrix, and ease of interpretation of the classifier's decisions.

5.5.2. Data Sources for Fraud Detection

The data source and format for obtaining data can vary based on the need and the purpose for which it is required. Data can be provided in any structure technically. To effectively do fraud prediction in financial transactions, it requires Join Code, Product Group Code, Effective Date, Scan Date, Merchant Code and Amount spent. Apart from these, there are some other financial transaction metrics like Count of Transactions, Count of Days, Count of Stores for each account and Merchant Group Code. Some visualisations and statistical operations on all these features can produce similar inferences which can also be proved with the Relevance Metrics using Statistical Tests set. The continuous numerical features are more effective than categorical or nominal features in detecting or preventing the fraud in financial transactions. Dummy Variables were created to process the explicit values of categorical variables. For Neural Network training, after converting to continuous variables, the collected data must be Normalised.

Always while constructing pipelines, it is important to take care of behaviours of the transactions in the dataset. Outlier/Anomalies processing, field-wise statistics/analysis/operations must be performed before and in parallel to machine learning modelling. Data Collection & Preparation can contain more functionalities using the pre-existing libraries. Though less explored, compatible libraries can be built using other Libraries, or for specific models/libraries. Negative Class prediction can also be taken into account. An Independent component analysis based data cleaning method can be employed here for multidimensional datasets. Clustering based Missing Value Imputation solutions/Methods can also be built. Redundant sample identification methods (based on Basic Statistics, Correlation, Distance, Clustering etc.) can be built to compensate for storage. Non-parametric tests can also be employed on categorical/ordinal features of the transactions, so that hypotheses can be tested theoretically apart from domain knowledge.

The modelling space is very vast and whitespace with abundant scope for exploration. Highly scalable and efficient ensemble models can still be built. Steps for adaptively updating models can be built following the approach of optimally hibernating old models

for resource management using peak memory, execution time etc., and a model suitable for high and low distribution data can also be trained. Metrics can also be explored beyond Area Under the Curve (AUC) which obtains an optimum threshold but fails to fulfil the efficacy Tariff/Cost. Fringe cases can also be explored like Appropriateness of modelling consumptions based on analysis and Financial transactions based on Text analysis etc.

5.6. Challenges in Implementing Predictive Analytics for Fraud Detection

A growing number of individual businesses and big firms are swamped by fraud. Even a relatively small firm can suffer daily losses amounting to thousands of dollars if fraud is not detected and stopped soon enough. Meanwhile, predicting, detecting and blocking fraud is of paramount importance. The speed at which firm funds are transferred from transaction accounts to some other place on the internet is on the rise. Credit firms or banks often allow money to be transferred from firm accounts without specific certification. This is very convenient for fraudsters, who often transfer fraudulently obtained money out of firm accounts inside minutes and become hard to catch. Under these conditions, fraud must be detected and blocked in real time, a very different problem than the already late detection of fraud and clients getting to know about it a day or a week later .

Miners of values and fraud fighting hackers have very different sizes today, with the former being backed by huge corporations and apparently unlimited access to technology, while the latter usually consists of underpaid, underpowered teams of graduate students. If the underlying systems of money transfer is wired, a potentially better solution could be moving capturing fraud to the inside. On the one hand, individual banks or credit firms are very reluctant to share transfer transaction data because it is their most valuable asset. On the other hand, it is possible to use attempts of fraud as a form of private data or simply as a negative label for positive-unlabeled data. Thus, capturing fraud with locally trained models is possible. However, the state of the art of fraud detection modeling assumes the availability of past examples of fraud. If this assumption does not hold, as is the case with credit cards, there can be a delay of years between implementation of modeling and emergence of fraud. This delay threatens the modeling effort not only through rapid evolution of fraud technology, but also computation performance issues, as locally trained shared models grow very large. A framework utilizing isolation forest to seed a locally trained model on the underlying trained model of all visible payment transfer frauds is able to accurately capture fraud in near real time even when there haven't been seen payment transfer frauds prior to implementation, being localized and hence aligned with solvable by individual banks problem.

5.6.1. Data Privacy Concerns

The rise of data breaches and security vulnerabilities in organizations who hold sensitive data on individuals has sparked ethical debates on data ownership, privacy and the right to opt out of data collection and retention. This has led to increasing consumer concern and skepticism about what companies do with data they collect, and the ethics of data usage. Compounding these concerns is the rise of data selling, and/or sharing unwanted, excessive and sensitive information. Recent surveys have found that a significant percentage of financial services consumers are concerned about how their data is used, with comparison shopping and advertising targeting widely seen as intolerable uses. These surveys indicate that a large fraction of consumers not only own financial accounts but are nonetheless skeptical, if not cynical, about the data collection, sharing and retention practices of the companies who hold that data.

Privacy concerns are intensified by social media. Participating in social media usually requires disclosing if not exposing one's personal details for collation and sharing with a vast array of third-party data suppliers, marketers and researchers. Major social media companies have been called to account for the unethical use of individuals' data and the exposure of this data by security vulnerabilities. In addition to unwarranted data use, privacy advocates claim that participation in social media has the potential to cause privacy harms through exposure by breaches in the duty of care. The general public often feels vulnerable to privacy harm due to participation in social media, and for this reason, is understandably sensitive to the privacy policies of social media companies. Social media companies are starting to recognize this reality, and respond by updating the privacy notices.

5.6.2. Algorithmic Bias and Fairness

Algorithmic decision-making (ADM) systems often depend on input data that are collected based on a certain social context or are a product of some historical events. The goal of governance mechanisms of ADM systems is to ensure not only that the computation is trusted, but also that the decision-making process does not reinforce discrimination present in the input data. This is manifested in certain fairness criteria that depend on the input data, its representation, the model, or its prediction outcomes. Implementing fairness criteria as constraining mechanisms into the regime of governance of ADM systems is not trivial. Implementing fairness criteria as constraints on the algorithmic decision-making process can negatively affect the computational performance of the model. If this is the case, how should fairness best be traded off against accuracy? Past research in the context of social choice theorists has shown that, in general, societal considerations cannot be traded off against computational considerations; this is referred to as the impossibility results. A computational

independence of societal and computational considerations might be achieved through increasing computational power; however, this is not an option in algorithmic governance. Not recommendations saying 'just do better', but definite prohibition of acts that can cause unfair model predictions is possible, the scope of which is usually broader than recommendations. In other words, if a governance mechanism is not prescriptive or prohibitive, it might not be a governance mechanism at all.

Data bias means that if a protected group is subject to unfair treatment and the model being trained is sensitive to the bias, then the model is also likely to disproportionately disadvantage the protected group. Automated decision systems (ADS) are overseen by people who must be able to make sense of their predictions. In a nutshell, it is up to the machine learning practitioner to decide if an issue is serious enough to warrant further attention. Likewise, one may argue that this is also up to the decision maker; fairness is merely a sentiment, ultimately subjective. Since predictions might not lead to direct actions and since there is always the chance, how serious of an issue is it if a few wrong predictions slip through the cracks? A common way to address this is through the use of metrics. However, this is where some problems arise. Common fairness metrics, like most accuracy-understandable metrics, give constant values over the prediction space. This is hard to square with human comprehension.

5.7. Conclusion

The integrity of identity in the digital age is fragile. It is based on a tenuous balance of convenience and trust. Technology has inadvertently expanded the potential to exploit naive users. The role of the “gatekeeper” often sees financial institutions and technology firms, be they banks, credit card providers or software suppliers, placed in the position of determining who is “real” and what to trust. Fraud has followed the pace of technological change, and an emergent proliferation of methods and tricks has scheduled multiple cycles of decline for any individual countermeasure. In this rapidly changing age of convenience, there is a need for vigilance and investment. However, much more remains to be done in combating fraud in whatever forms it takes. The digital age has facilitated many changes in the way that people interact, in the way that services are delivered, and in the way that government departments and private enterprises operate. Such changes have not been without implications for those wishing to commit acts of fraud. Technology will transform, but it will not protect. The challenge for businesses and organizations remains as it has always been in protecting the integrity of identity. Identity will always be a social construct, finite and fragile, and a method of operation vulnerable to exploitation. A countervailing effort to foster a secure identity will always be necessary if you wish to minimize the risk of practical, potential, and adaptive fraud.

5.7.1. Emerging Trends

This paper will describe some emerging trends in the use of new and potential new technologies to develop and manage personal relationships. Much of the new technology in question will fall under the broad subheading of Information and Communication Technologies (ICTs). Information technology includes all kinds of ICTs, whereas communication technologies generally connotate a focus on the structural properties of information technology that shapes their social effects. In a similar spirit to Murray's treatment of communication technologies, the effects of different uses of the Internet on the nature and nuances of personal relationships will be emphasized. Also like Murray, the aim of this paper is not to provide a comprehensive overview critique of the issues spawned by new ICTs, nor a fully fleshed out interactive social mechanisms approach. Rather, by noting some of the more interesting emerging issues and discussing them in some detail, the goal is to better frame this new area for subsequent research. In particular, it is hoped that it might spur further research in terms of the development and application of quantitative indicators, an interactive mechanism approach and empirical evaluation of findings and hypotheses derivable from such an approach.

More narrowly, the focus will be on a voyeuristic view of identity, how a self-constructed pouch that takes on a faux persona — a network nickname (NN) — in open chat rooms changes the naïve perceptions of knowing others better in the cyber world than in the real one and reveals a more complex social world governed by the vagaries of wit, charm, charisma, witlessness, insipidity, profusion, and rarity to the point of instant loss and the mere past tense of one's own implied identity. As Thoreau said, men have a hard enough time concealing their thoughts; why should they presume to hide their deeds? Yet, in cyberspace where the anonymity afforded by computers matching modems and pseudonyms may allow for the construction of virtual lives generated by combining selected aspects of different online and offline selves.

References

Soldatos, J., & Kyriazis, D. (2024). Big Data and Artificial Intelligence in Digital Finance. OAPEN. https://library.oapen.org/handle/20.500.12657/54429OAPEN

G., S., & Pahuja, A. (2023). FinTech Frontiers: Cloud Computing and Artificial Intelligence Applications for Intelligent Finance Investment and Blockchain in the Financial Sector. International Journal of Intelligent Systems and Applications in Engineering, 12(4s), 654–659. https://doi.org/10.21307/ijisae-2023-011IJISAE

Bodemer, O. (2024). Transforming Financial Decision-Making: The Interplay of AI, Cloud Computing, and Advanced Data Management Technologies. ResearchGate. https://doi.org/10.13140/RG.2.2.36486.59209ResearchGate+1ResearchGate+1

Zhao, D., & Zhang, W. (2021). Fintech towards Intelligent Finance. In Financial Mathematics and Fintech (pp. 1–16). https://doi.org/10.1007/978-981-16-5592-0_1IJISAE

O'Leary, D. E. (1995). AI in Accounting, Finance and Management. Intelligent Systems in Accounting, Finance and Management, 4(3), 149–153. https://doi.org/10.1002/j.1099-1174.1995.tb00088.x