Research Article

Citation date: 2018/11/08

Artificial Intelligence in Banking Industry: A Review on Fraud Detection, Credit Management, and Document Processing

Musaab Mohammad Alhaddad

Director, IT Solutions, Technoware for IT and Telecom

How to cite:

Musaab, M, A "Artificial Intelligence in Banking industry: A review on Fraud Detection, Credit Management, and Document Processing ," *Res. Rev. Sci. Technol.*, vol. 2, no. 3, pp. 25–46, 2018.

Article history:

Received: 2018/07/21
Available online: 2018/11/08

Abstract

AI is likely to alter the banking industry during the next several years. It is progressively being utilized by banks for analyzing and executing credit applications and examining vast volumes of data. This helps to avoid fraud and enables resource-heavy, repetitive procedures and client operations to be automated without any sacrifice in quality. This study reviews how the three most promising AI applications can make the banking sector robust and efficient. Specifically, we review AI fraud detection and prevention, AI credit management, and intelligent document processing. Since the majority of transactions have become digital, there is a great need for enhanced fraud detection algorithms and fraud prevention systems in banking. We argued that the conventional strategy for identifying bank fraud may be inadequate to combat complex fraudulent activity. Instead, artificial intelligence algorithms might be very useful. Credit management is time-consuming and expensive in terms of resources. Furthermore, because of the number of phases involved, these processes need a significant amount of work involving many laborious tasks. Banks can assess new clients for credit services, calculate loan amounts and pricing, and decrease the risk of fraud by using strong AA/ML models to assess these large and varied data sets in real-time. Documents perform critical functions in the financial system and have a substantial influence on day-to-day operations. Currently, a large percentage of this data is preserved in email messages, online forms, PDFs, scanned images, and other digital formats. Using such a massive dataset is a difficult undertaking for any bank. We discuss

how the artificial intelligence techniques that automatically pull critical data from all documents received by the bank, regardless of format, and feed it to the bank's existing portals/systems while maintaining consistency.

Keywords: AI, Banking, Document processing, Fraud detection, ML

Declarations

Competing interests:

The author declares no competing interests.

1. Introduction

AI is a collection of novel technologies, processes, and approaches that are critical to the present and future growth of our society and economy. AI is used in a wide variety of fields, including disease diagnosis, optical character recognition, autonomous driving in automobiles, and financial services. Currently big and small corporations are already using AI technology. For millions of people, AI has been ingrained in their everyday lives. The use of artificial intelligence is seen as a possible catalyst for disruptive technological growth and innovation.

The use of AI methods in finance may result in increased efficiency by lowering friction costs (e.g., commissions and fees associated with transaction execution) and increasing productivity, which results in increased profitability. Automation and tech-led cost reduction, in particular, offer capacity reallocation, greater expenditure effectiveness, and increased decision-making openness. AI applications in financial service providing may also improve the efficiency of products and services given to financial customers, boost product customization and personalization, and broaden the product offering. AI techniques may be used to extract insights from data to improve investment plans, while also possibly enhancing access to financial services by allowing for the study of creditworthiness of customers with minimal credit history.

The application of machine learning helps overcome some of these challenges. Advantages of machine learning for financial institutions include speed, effectiveness, salability, and accuracy.

a) Speed: Machine learning techniques can assess large volumes of data in a very short period of time. They have the capacity to continually gather and evaluate fresh data in real-time. Speed is more critical as the pace and complexity of eCommerce grows. b) Effectiveness: Machine learning techniques can conduct repeated jobs and identify minor variations across enormous volumes of data (Bolton and Hand, 2002). This is crucial to identifying fraud in a lot shorter period of time than with what humans can accomplish. Algorithms can evaluate large number of payments each second, which is much more work than multiple human analysts can complete in the same length of time (Adewumi and Akinyelu, 2017) (Chaudhary, Yadav and Mallick, 2012). This decreases expenses as well as time required to examine transactions, therefore making the operations more effective. c)

Scalability: As the volume of transactions rises for banks, the burden on human analysis rises. This causes a spike in expenses and time, and a drop in accuracy. Using a machine learning technique, it's quite the opposite. The larger the data volume, the richer the results. The algorithm improves when more data are obtained, allowing it to identify fraud quicker and with greater precision (Abdallah, Maarof and Zainal, 2016).

d) Accuracy: Machine learning models may be taught to evaluate and find patterns across apparently small dataset. They can find obscure and complex patterns which would be challenging, or perhaps impossible, for a human to notice (Jordan and Mitchell, 2015). This boosts the reliability of fraud detection, indicating that there would be less false positives and scams that go unnoticed (Jordan and Mitchell, 2015; Albashrawi, 2016).

AI has significant potential to improve the detection of financial fraud quicker, more efficient and – by removing rising amounts of false signals – far more efficient. However, deploying these systems efficiently is tough, particularly for smaller financial institutions that lack human resources of significant numbers of data professionals. Identifying frauds in sets of bank data while limiting false positives is an especially

tough challenge for AI-based systems: the small amount of frauds in relation to the real transactions in financial data sets offers relatively limited input with which to develop the models (Benson Edwin Raj and Annie Portia, 2011; Stolfo et al., 1997). Simultaneously time, the quantity of distinct fraud types is huge and bank clients display a broad variety of activities that the system needs learn to identify and accept. Only the biggest and best-resourced businesses will be able to enhance and deploy these systems internally.

Even with the greatest of the technology and procedures, regrettably, criminal-minded individuals are frequently one step ahead. Though AI cannot avoid all forms of frauds, particularly those that arise directly from inside corruption, it is undoubtedly playing a big role to decrease and prevent the total fraud.

Artificial Intelligence can also help with credit risk assessment. Credit scoring models in the majority of financial institutions are still dependent on the scorecard method, i.e., the dynamics prevalent at the time of their formation. To be regarded as scorable. A prospective borrower must possess adequate historical data on prior borrowing behavior (Li and Zhong, 2012). When such past information is unavailable (as is often the case for new banking accounts), even creditworthy consumers are refused credit.

Unlike conventional credit scoring methods (for example, the scorecard method), which are based on a borrower's past performance, AI credit rating is more responsive to real-time indicators of a client's creditworthiness, such as their current income level, employment opportunities, and potential ability to earn (Wang et al., 2011). Thus, loan programs are open to borrowers with high potential, whereas those who nominally pass the traditional credit score evaluation are excluded. AI-powered credit rating enables exact profit forecasting via the use of intelligent AI models.

Automatically interpreting client papers for intelligent insights provides banks with important data that may be passed into other parts of the company or into programs (Roychoudhury, Bellarykar and Kulkarni, 2016; Sumathi and Sheela, 2017). From that, financial firms may design solutions that address the requirements of retail, SME, and commercial clients and alleviate their problem areas; they can also enhance the

customer interaction and facilitate dialogues about financial health between customers and the sector (Vafin, 2017a, 2018b).

Every sector is evaluating choices and implementing strategies for value creation in a technology-driven environment. The banking industry is undergoing revolutionary changes, chief among which is an increase in customer-centricity. Customers who are exposed to modern technology on a daily basis want banks to provide seamless experiences. Banks have extended their industrial landscape to include retail, information technology, and telecommunications in order to offer services such as mobile banking, e-banking, as well as real-time transfer of funds. These developments have allowed users to access the majority of financial services from any location, at any time.

2. Detecting fraud transaction with Artificial intelligence

There is a strong necessity for improved fraud detection algorithms and fraud prevention systems in banking, since the majority of transactions have become digital; the rise of online banking and financial transactions in recent times has resulted in an exponential growth in transaction volume (John et al., 2016). And fraudsters have evolved as well, adopting creative fraudulent activities in order to avoid disclosing suspicious activity online.

These troubling banking fraud trends lead to a great concern, and they underscore the need of banks and other organizations implementing stronger fraud protection systems. The usual approach for detecting bank fraud may be insufficient to counteract sophisticated fraudulent activities (Bouchti et al., 2017).

Machine learning algorithms for fraud detection and other similar prediction algorithms can become valuable.

2.1 Form of fraud transaction

There are several forms of fraud transaction in the financial industry. The following are some of the most prevalent kinds of financial fraud:

• Transactions that are not authorized: Credit card transactions that are not initiated or approved by the account holder continue to be a source of contention for both banks and customers (Mason and Bohm, 2017; Sakharova, 2012).

• Phishing scams: Phishing is a technique used by criminals to dupe people into disclosing sensitive data such as credentials, account, identity, or credit card details (Aburrous et al., 2010). Email messages, text messages, phone calls, or internet material may all be used in phishing schemes (Alsayed and Bilgrami, 2017) (Alhaddad, 2018). Consumers and business personnel alike are susceptible to phishing schemes, which may result in illegal transfers, account takeovers (ATO), data breaches, and identity theft (Vasquez, 2018; Dzomira, 2015).

• Identity theft: Identity theft is the theft of private, or financial details with the goal of utilizing it to assume the identity of another person. The acquired identity is most often used to execute fraudulent transactions or to create credit card or bank profiles (Slosarik, 2002). Additionally, a forged identity might have a negative implication for health insurance, income, and even criminal background. Identity theft is the most often reported kind of consumer complaint. Identity fraud has a significant effect on both customers and financial firms (Anderson, Durbin and Salinger, 2008). Figure 1 shows the percentages of each fraud transaction category.

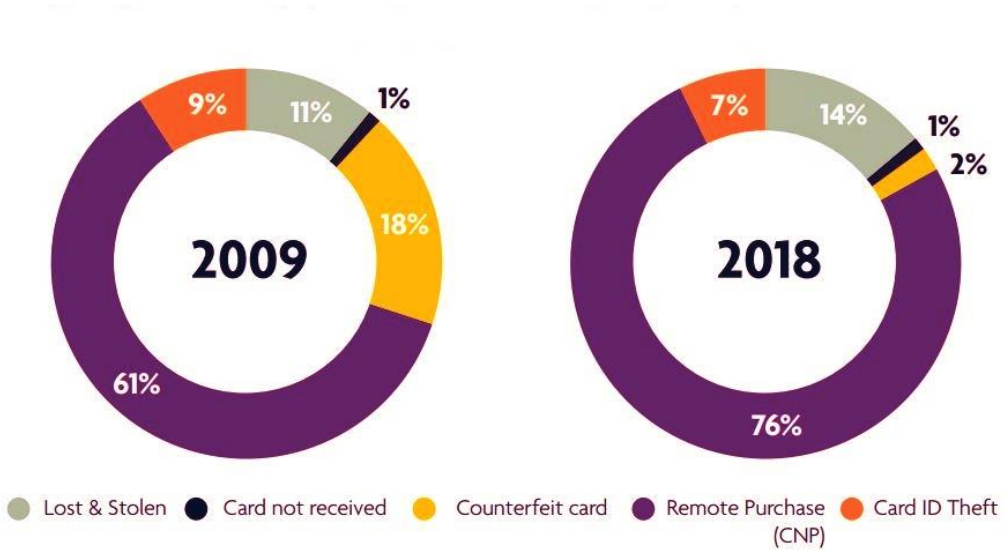

Figure 1 Card fraud loss by category (2009, 2018)

2.2 Artificial intelligence-based strategies for detecting and preventing fraud

1. Integrating Supervised and Unsupervised AI Algorithms

Due to the sophistication and adaptability of organized crime techniques, defense attempts relying on a single analytics approach will probably fail. Each use case should be backed by expertly built anomaly detection algorithms that are optimum for the circumstance at hand (Benson Edwin Raj and Annie Portia, 2011).

As a consequence, combined supervised and unsupervised algorithms are crucial in detecting fraud and should be incorporated into comprehensive upcoming fraud techniques.

A supervised modeling is one that has been trained on a large quantity of accurately "labeled" transactions, and is the most common kind of machine learning in all domains. Each transaction is classified as either fraudulent or not fraudulent. The model can be trained by ingesting massive amounts of labeled transaction data in order to uncover patterns that best depict legitimate activity (Ryman-Tubb, Krause and Garn, 2018). The quantity of quality, appropriate training data required to construct a supervised model is directly proportional to the model's accuracy.

Unsupervised models are meant to identify anomalous behavior in the absence of tagged transaction data. Self-learning must be utilized in these circumstances to identify patterns within the data that are masked by standard analytics (Paruchuri, 2017).

2. Applied behavioral analytics

In behavioral analytics, machine learning is utilized to evaluate and forecast behavior at the micro level across all parts of a transaction (Veeramachaneni et al., 2016). The data is analyzed to create profiles that explain the behaviors of each customer, retailer, account, and smartphone. These identities are continuously updated in response to each transaction, enabling the computation of analytic features that provide precise projections of future behavior. The profiles cover both financial and non-financial transactions. Non-monetary transactions include address changes, requests for duplicate cards, and recent password resets (Patil and Lilhore, 2018).

Financial transaction data enables the building of patterns that may reflect an individual's average spending frequency, the days and hours when they typically transact, and the time length between geographically distributed payment venues (Shabtai and Elovici, 2010). Profiles are particularly beneficial since they maintain an accurate representation of activity, which may assist reduce transaction failure due to unpleasant false positives. A robust corporate fraud solution consists of a collection of modelling techniques and profiles that give the data necessary to assess real-time transaction patterns (Gao and Ye, 2007).

3. Creating Models from Massive Datasets

According to studies (Herland, Khoshgoftaar and Bauder, 2018; Bologa et al., 2013), the volume and richness of data has a higher impact on the effectiveness of ML algorithms than the intelligence of the algorithms. It is the computational counterpart of human experience. This means that, wherever feasible, expanding the dataset used to generate the predictive characteristics employed in a ML algorithms may improve prediction accuracy (Bauder and Khoshgoftaar, 2018). A big volume amount of information, or education, allows data scientists to make accurate diagnoses within their area of specialty.

In the case of fraud detection, a model will benefit from the experience gained through collecting millions or billions of examples of both genuine and unauthorized transactions (Cárdenas, Manadhata and Rajan, 2013). Enhanced fraud detection is accomplished by analyzing a huge volume of transactional data in order to have a better understanding of and estimate risk for each person.

4. Self-Learning Artificial Intelligence and Adaptive Analytics

Fraudsters make securing customers' accounts very tough and dynamic. In this situation, machine learning thrives. For continual performance improvement, fraud detection professionals should investigate adaptive systems that aim to sharpen responses, especially on marginal judgements (Bynagari, 2015; Danenas, 2015).

Where accuracy is most critical is on the sharp line between a false positive activity — a lawful transaction that rated too highly — and a false negative activity — a fraudulent activity that rated too low. Adaptive analytics accentuates this distinction by offering a current awareness of a business's risk vectors (Rattadilok and Petrovski, 2014).

By dynamically responding to newly established case dispositions, adaptive analytics systems strengthen their sensitivity to emerging fraud patterns, leading to a more accurate differentiation of frauds from non-frauds (Peng and Chen, 2014; Colchester et al., 2017).

When an analyst conducts an investigation into a transaction, the outcome is reported back into the system, if the transaction is verified as valid or fraudulent.

This enables analysts to correctly represent the fraud environment in which they operate, including emerging methods and hidden fraud behaviors that have lain dormant for an extended period of time. This adaptive modeling technique automatically updates the model.

Applying this adaptive modeling technique, the weights of predictive parameters in the fraud algorithms are continuously updated (Zeager et al., 2017). It's an effective method for enhancing fraud detection and limiting the emergence of new types of fraud attacks (Abdallah, Maarof and Zainal, 2016).

3. Credit management with artificial intelligence

Credit management is time-consuming and resource-costly. Additionally, these procedures need a large amount of labor due to the number of stages involved - from the early phase of prospect screening through making the loan decision, handling underwriting and disbursements, managing the portfolio, and ultimately, collections (Khandani, Kim and Lo, 2010; Tsai and Chen, 2010).

Credit organizations deal with risks on a daily basis, and credit choices serve as a shield that separates the negative risks. Historically, credit agencies assigned an internal score using complicated statistical models that took into account many criteria specific to a credit applicant's profile (Kruppa et al., 2013). This assigns a risk level to a loan that represents the company's real-world business standards. When credit judgments

are made manually, they need several manual hours and come short of meeting the business requirements necessary to function in today's climate.

Predictive data mining techniques, automated credit scoring have changed the performance levels. The pioneers of the online lending sector leverage unstructured and structured dataset from customers' online activities to infer additional details for credit scoring using machine learning techniques such as random forests, SVM, ensemble learning, and hybrid genetic algorithms, among others (Vartak et al., 2016).. Process automation makes a significant improvement in the collecting, warehousing, processing, and decision-making processes associated with end-to-end loan offerings and credit limit expansions (Attigeri, Pai and Pai, 2017; Sayjadah et al., 2018) (Vafin, 2017b). Banks can assess new clients for credit services, calculate loan amounts and pricing, and decrease the risk of fraud by using strong AA/ML models to assess these large and varied data sets in real time.

1. Credit assessment.

For many years, lenders analyzing credit bureau information to assess if a consumer qualifies for a certain sort of loan have utilized rule-based or logistic regression models (Huang et al., 2004). This method, which is based on a restrictive set of criteria, excludes a huge proportion of individuals and small businesses without a formal credit record, prompting these prospective customers to seek loans from nonbank sources (Lee, 2007). However, prominent banks and fintech lenders have created sophisticated algorithms for evaluating structured and unstructured data in recent years, scrutinizing hundreds of data points gathered from social media, browser history, and telecommunications use data, among other sources. This decision-making process is entirely automated, allowing the bank to forecast the possibility of default for people in a sizable and potentially lucrative category of financially excluded consumers and SMEs. Banks can proceed gradually in developing and refining their qualification model, testing and improving it along the way—for instance, by using automated approvals for customers with significantly lower default risk up to a certain threshold and manual verification for those approximated to have a higher default risk, and then progressively moving more situations to automated decisioning (Bose and Mahapatra, 2001).

Additionally, leading banks are automating the process of establishing the highest level a consumer may borrow using AA/ML models. By using optical character recognition (OCR) to retrieve information from traditional data sources such as bank accounts, tax returns, and utility bills, these loan-approval systems may swiftly determine a customer's disposable income and ability to make regular loan payments (Mithe, Indalkar and Divekar, 2013; Singh, 2013; Asif et al., 2014). Additionally, the growth of digital interactions generates massive and varied data sets that may be used to power complicated machine-learning algorithms. By combining data from both traditional and new sources, banks may develop an extremely precise projection of a customer's ability to pay. Emails and e-commerce spendings are just a few data streams that may be analyzed (with the customer's agreement).

2. Pricing

Banks have historically provided largely standardized loan rates, with limited freedom granted to sales personnel and relationship managers to change rates within specific limits. However, severe competition in loan pricing, especially for clients with a high-risk score, puts banks that rely on conventional ways at a significant disadvantage compared to leaders in AI and analytics. With remarkably precise machine-learning algorithms for risk rating and loan pricing in place, AI-first banks are able to provide competitive rates while maintaining low risk costs. Additionally, some firms are using their decision-making skills to measure a customer's proclivity to purchase based on their usage of various sorts of financial goods. Several companies even use natural language processing (NLP) to evaluate unstructured transcripts of conversations with sales and service professionals, as well as collection employees in certain circumstances. By establishing the provided rate on both credibility and willingness to purchase, a bank may manage the relationship between total asset size, risk, and interest earnings within a loan portfolio (Fisher, Garnsey and Hughes, 2016; Ghosh, 2018).

3. Observation and collecting

Once a bank has automated loan screening and pricing via the use of ML ML models, it may also use AI and sophisticated analytics to alleviate the pressure of non -

performing loan (Kalaycı, Kamasak and Arslan, 2018; Kalayci and Arslan, 2017). Banks are increasingly interacting with customers proactively to assist them in staying current on payments and working more actively with clients who have issues. By combining multiple data sources to provide a holistic picture of a customer's financial situation, banks may identify early warning signs that a borrower's risk profile has altered and that the risk of defaulting should be evaluated.

4. Customer Segmentation.

Traditional credit scoring techniques have been consistently criticized for being out of date, mostly due to their homogeneity and lack of consideration to individual differences and subtleties. By incorporating AI into credit rating systems, banks may get new insights into their clients' financial behavior not just based on previous data, but also on projected income (Smeureanu, Ruxanda and Badea, 2013). These studies of massive customer data allow increased segmentation and grading of customers in terms of related credit risk, allowing financial institutions to price and offer credit products to the appropriate groups of customers (Vafin, 2018a) (Abad-Grau, Tajtakova and Arias-Aranda, 2009).

5. Increased operational speed for credit management.

AI applications, particularly in credit scoring, are gaining traction owing to their potential to accelerate the procedure of generating loan choices without sacrificing quality or accuracy (Das et al., 2015). Historically, banks generated a client's credit score using decision trees, regression analysis, and sophisticated mathematical calculations. Today, massive amounts of unnecessary, unstructured, and partly structured data (e.g., social media usage, cellphone activities, etc.) are included into analysis in order to make wiser credit-related judgments, while the pace of information processing remains high because of AI (Le and Viviani, 2018) (Mendling et al., 2018).

6. Increased Credit Access.

Credit scoring has grown more future-oriented as a result of data science, as opposed to old-school past-oriented methodologies. Thus, more borrowers (e.g., graduates, founders of potential firms, and foreign residents) now have access to finance, which encourages their businesses and helps them launch their ideas. Obtaining one's first credit has also been easier, since it is now conducted with the AI's financial forecasts of the client's possible income and career options (Surya, 2015).

The use of AI technologies for credit evaluation and lending selections enables banks to make data-driven judgments, concentrate on margin maximization rather than risk reduction, and assess risk vs. profit curves rather than depending on pre-calculated score card brackets (Donepudi, 2017). This is a strategy that would have been extremely unachievable prior to the broad use of AI and data collection tools. Banks and consumers both benefit from the implementation of AI in credit evaluation: banks gain more customers and revenues (Fethi and Pasiouras, 2010), while people in need of credit get access to more favorable loan solutions.

While Artificial Intelligence may assist model creators in mitigating model risk and increasing the overall predictive power of models, a sizable portion of the finance sector remains wary of the explainability barrier associated with machine learning approaches (Holzinger et al., 2017). Indeed, advances in model accuracy are often accomplished at the expense of their explainability. Additionally, this shortage of clarification presents a practical and ethical dilemma for credit specialists.

For banks, the application of AI offers new prospects for dramatically enhancing future efficiency, decreasing processing times and pleasing consumers via intelligent credit operations. They are quickly reaching practical usage of this promising innovation on their route to open banking. They must first construct their information technology infrastructures flexibly using modular solution components inside a banking platform. They may therefore choose consume AI apps from outside third

parties without needing to build them in-house as stakeholders in systems where nodes are connected through APIs.

4. Document processing

Documents play key roles financial system and have a significant impact on everyday operations. Currently, a significant portion of this data is saved in email messages, web forms, PDFs, scanned photos, and a variety of other digital formats. Utilizing this large dataset is a big task for any bank (Moro, Cortez and Rita, 2015). As enterprises expand in size, the need for improved document processing increases proportionately. The continual flood of printed or PDF documents has compelled organizations in the banking industry to consider updating existing document processing abilities. In such instances, enterprises and organizations are forced to install a robust document analysis pipeline capable of automating and scaling the processing of these documents (Alhaddad, 2017) (van der Aalst, Bichler and Heinzl, 2018).

There are two possible methods for banks to handle this data in order to maintain seamless operations.

1) To begin, workers may sift through all data, categorize it consistently, and then manually input it into the bank's individual portals.

2) The second alternative is a standard technology that extracts important data from all papers received by the bank, regardless of their format, then automatically extracts the data and feeds it to the bank's current portals/systems while keeping consistency.

Intelligent document processing (IDP) is a tool that extracts data from documents and processes it employing machine learning and artificial intelligence (Esposito et al., 2005). In contrast to typical standalone OCR systems, IDP leverages artificial intelligence (AI) by merging RPA with OCR. As the system accumulates more data, it trains and improves, requiring less human interaction (Tang, Lee and Suen, 1996).

The document processing begins with the scanning of paper documents to generate a digital picture, followed by the reading of those documents using OCR-based technology (Tang, Lee and Suen, 1996). This stage of document processing converts document pictures to text, which is then used to search for pertinent information such

as the amount paid, the payee's details, or other critical data. This is accomplished via the process of document imaging, which includes document search, document verification, and document retrieval.

Document processing can also be used for other purposes, such as comparing documents to certain criteria to distinguish checks from statements, connecting to platforms to perform check digit validation, which aids in document authentication, and indexing, which means the capacity to sort and store documents in a database by instantly obtaining characteristics such as the name of clients or file reference number (Singh, Bacchuwar and Bhasin, 2012; Chaudhuri, 2007).

For an extended period of time, corporations and small businesses depended on handwritten invoicing to manage their accounts and make payments. Organizations suffered from disgruntled and agitated personnel, missing or lost invoices, decreased productivity, inefficient processes, higher costs and operator mistakes, and unreliability as a result of late or missed payments.

Intelligent Document Processing (IDP) uses sophisticated techniques for extracting particular data from a number of sources of data, such as bank accounts, financial records, credit card purchases, and other sources (Tripathy and Rath, 2014). Banks may determine how much value they would like to collect and how much they would like to utilize from each part of the extraction technique. Indeed, manual papers offer a significant risk to banks due to the possibility of omission and inclusion mistakes. However, IDP enables banks to concentrate systematic attention on remaining risk exposures by increasing the accuracy and speed of document processing while drastically decreasing human error. Based on important risk indicators, banks may further minimize any weak regions (KRIs).

If they choose to evaluate individual components, innovative software digitizes them and produces an accurate and consistent record that can be checked at any time and from any location. It allows to redirect critical data to a system, assist customer service in order to enhance the client experience, and much more (Mich and Garigliano, 2002) (Becker and Kao, 2009).

AI can assist in streamlining and automating some of the most critical components of KYC compliance by automating document identification (Goode, 2018). Banks can minimize staff burden and maintain compliance with KYC regulations by delivering a more precise risk assessment (Goode, 2018; Lipton, Shrier and Pentland, 2016). The technology enables the simple archiving and storage of documents on the cloud for later access.

5. Conclusion

The use of artificial intelligence (AI) in finance has increased significantly, owing to the amount of accessible data and the decrease in the cost of computing resources. This trend is projected to continue, with some estimates predicting that worldwide investment on AI would nearly double in the near future. Artificial intelligence is a significant investment that needs not just a sizable budget, but also specialized infrastructure, staff skill sets, and maturity. That is why not all banks are prepared to deploy artificial intelligence solutions. The majority of organizations in the financial services sector have used AI somewhat around one-third of respondents claimed that their company has completely implemented artificial intelligence technology. As the use and relevance of AI grows, the financial sector's working methods will undergo significant transformation. AI will be able to replace many laborious jobs now done by humans. This opens up new possibilities: corporations can lower workloads and allow staff more time off without jeopardizing productivity.

With the integration of artificial intelligence into banking applications and services, the industry has become more client-centric and technologically competent. Large banks, in particular, are industry leaders in using AI to remain ahead of the competition, deliver superior customer service, more personalized services and products, and assist in the transformation of several back-end activities. AI-based solutions may assist banks in reducing costs by enhancing productivity and making judgments based on data that a human agent cannot comprehend. Additionally, clever algorithms are capable of detecting irregularities and fake information within seconds.

References

van der Aalst, W. M. P., Bichler, M. and Heinzl, A. (2018). Robotic Process Automation. *Business & Information Systems Engineering*, 60 (4), pp.269–272.

Abad-Grau, M. M., Tajtakova, M. and Arias-Aranda, D. (2009). Machine learning methods for the market segmentation of the performing arts audiences. *International Journal of Business Environment*, 2 (3), pp.356–375.

Abdallah, A., Maarof, M. A. and Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, pp.90–113.

Aburrous, M. et al. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. *Cognitive computation*, 2 (3), pp.242–253.

Adewumi, A. O. and Akinyelu, A. A. (2017). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *International Journal of System Assurance*. [Online]. Available at: https://link.springer.com/article/10.1007/s13198-016-0551-y.

Albashrawi, M. (2016). Detecting financial fraud using data mining techniques: a decade review from 2004 to 2015. *Journal of data science: JDS*. [Online]. Available at: https://www.airitilibrary.com/Publication/alDetailedMesh?docid=16838602-201607-201609120008-201609120008-553-569.

Alhaddad, M. M. (2017). The Impacts of EdTech Collaboration, IoT-Connected Classroom and Intelligent Grading System on Educational Performance. *Advances in Contemporary Science and Technology*, 2 (1), pp.44–67.

Alhaddad, M. M. (2018). Implementing Blockchain in Public Sectors in MENA Countries: Opportunities and Challenges. *Empirical Quests for Management Essences*, 2 (4), pp.30–45.

Alsayed, A. and Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *Int. J. Of Emerg. Techn. and Adv. Activ.* [Online]. Available at: https://www.researchgate.net/profile/Anwar-Bilgrami/publication/315399380_E-Banking_Security_Internet_Hacking_Phishing_Attacks_Analysis_and_Prevention_of_Fraudulent_Activities/links/59f19d7c0f7e9beabfca5f17/E-Banking-Security-Internet-Hacking-Phishing-Attacks-Analysis-and-Prevention-of-Fraudulent-Activities.pdf.

Anderson, K. B., Durbin, E. and Salinger, M. A. (2008). Identity Theft. *The journal of economic perspectives: a journal of the American Economic Association*, 22 (2), pp.171–192.

Asif, A. et al. (2014). An overview and applications of optical character recognition. *Int. J. Adv. Res. Sci. Eng*, 3 (7), pp.261–274.

Attigeri, G. V., Pai, M. M. M. and Pai, R. M. (2017). Credit Risk Assessment Using Machine Learning Algorithms. *Advanced science letters*, 23 (4), pp.3649–3653.

Bauder, R. A. and Khoshgoftaar, T. M. (2018). The effects of varying class distribution on learner behavior for medicare fraud detection with imbalanced big data. *Health information science and systems*. [Online]. Available at: https://link.springer.com/article/10.1007/s13755-018-0051-3.

Becker, K. and Kao, S. (2009). Finding stolen items and improving item banks. In: *annual meeting of the American Educational Research Council, San Diego, CA*. 2009. researchgate.net. [Online]. Available at: https://www.researchgate.net/profile/Kirk-Becker/publication/293853625_Finding_stolen_items_and_improving_item_banks/links/56bdf6e608aee5caccf2e782/Finding-stolen-items-and-improving-item-banks.

Benson Edwin Raj, S. and Annie Portia, A. (2011). Analysis on credit card fraud detection methods. In: *2011 International Conference on Computer, Communication and Electrical Technology (ICCCET)*. March 2011. ieeexplore.ieee.org. pp.152–156.

Bologa, A.-R. et al. (2013). Big data and specific analysis methods for insurance fraud detection. *Database Systems Journal*, 4 (4), pp.30–39.

Bolton, R. J. and Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical science: a review journal of the Institute of Mathematical Statistics*. [Online]. Available at: https://projecteuclid.org/journals/statistical-science/volume-17/issue-3/Statistical-Fraud-Detection-A-Review/10.1214/ss/1042727940.short.

Bose, I. and Mahapatra, R. K. (2001). Business data mining — a machine learning perspective. *Information management* , 39 (3), pp.211–225.

Bouchti, A. E. et al. (2017). Fraud detection in banking using deep reinforcement learning. In: *2017 Seventh International Conference on Innovative Computing Technology (INTECH)*. August 2017. ieeexplore.ieee.org. pp.58–63.

Bynagari, N. B. (2015). Machine Learning and Artificial Intelligence in Online Fake Transaction Alerting. *Engineering International*, 3 (2), pp.115–126.

Cárdenas, A. A., Manadhata, P. K. and Rajan, S. P. (2013). Big Data Analytics for Security. *IEEE Security Privacy*, 11 (6), pp.74–76.

Chaudhary, K., Yadav, J. and Mallick, B. (2012). A review of fraud detection techniques: Credit card. *International Journal of Computer*. [Online]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.677.970&rep=rep1&type=pdf.

Chaudhuri, B. B. (2007). *Digital document processing: major directions and recent advances*. Springer Science & Business Media.

Colchester, K. et al. (2017). A Survey of Artificial Intelligence Techniques Employed for Adaptive Educational Systems within E-Learning Platforms. *Journal of Artificial Intelligence and Soft Computing Research*, 7 (1), pp.47–64.

Danenas, P. (2015). Intelligent financial fraud detection and analysis: a survey of recent patents. *Recent Patents on Computer Science*. [Online]. Available at: https://www.ingentaconnect.com/content/ben/cseng/2015/00000008/00000001/art00004.

Das, S. et al. (2015). Applications of artificial intelligence in machine learning: review and prospect. *International Journal of Computer*. [Online]. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.5829&rep=rep1&type=pdf.

Donepudi, P. K. (2017). Machine Learning and Artificial Intelligence in Banking. *Engineering International*, 5 (2), pp.83–86.

Dzomira, S. (2015). Cyber-banking fraud risk mitigation conceptual model. *Banks & bank systems*, (10, Iss. 2), pp.7–14.

Esposito, F. et al. (2005). Intelligent document processing. In: *Eighth International Conference on Document Analysis and Recognition (ICDAR'05)*. August 2005. ieeexplore.ieee.org. pp.1100-1104 Vol. 2.

Fethi, M. D. and Pasiouras, F. (2010). Assessing bank efficiency and performance with operational research and artificial intelligence techniques: A survey. *European journal of operational research*, 204 (2), pp.189–198.

Fisher, I. E., Garnsey, M. R. and Hughes, M. E. (2016). Natural language processing in accounting, auditing and finance: A synthesis of the literature with a roadmap for future research. *Intelligent Systems in Accounting Finance & Management*, 23 (3), pp.157–214.

Gao, Z. and Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control*, 10 (2), pp.170–179.

Ghosh, A. (2018). *Stress testing: A precautionary measure of financial crisis in credit risk management*. [Online]. Available at: https://ruj.uj.edu.pl/xmlui/handle/item/231049

Goode, A. (2018). Biometrics for banking: best practices and barriers to adoption. *Biometric Technology Today*, 2018 (10), pp.5–7.

Herland, M., Khoshgoftaar, T. M. and Bauder, R. A. (2018). Big data fraud detection using multiple medicare data sources. *Journal of Big Data*. [Online]. Available at: https://link.springer.com/article/10.1186/s40537-018-0138-3.

Holzinger, A. et al. (2017). What do we need to build explainable AI systems for the medical domain? *arXiv [cs.AI]*. *arXiv* [Online]. Available at: http://arxiv.org/abs/1712.09923.

Huang, Z. et al. (2004). Credit rating analysis with support vector machines and neural networks: a market comparative study. *Decision support systems*, 37 (4), pp.543–558.

John, S. N. et al. (2016). Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm. In: *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*. December 2016. ieeexplore.ieee.org. pp.1186–1191.

Jordan, M. I. and Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*. [Online]. Available at: https://www.science.org/doi/abs/10.1126/science.aaa8415.

Kalayci, S. and Arslan, S. (2017). Early NPL Warning for SME Credit Risk: An Experimental Study. In: *KDIR*. 2017. scitepress.org. pp.190–197.

Kalaycı, S., Kamasak, M. and Arslan, S. (2018). Credit risk analysis using machine learning algorithms. In: *2018 26th Signal Processing and Communications Applications Conference (SIU)*. May 2018. ieeexplore.ieee.org. pp.1–4.

Khandani, A. E., Kim, A. J. and Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms. *Journal of Banking & Finance*, 34 (11), pp.2767–2787.

Kruppa, J. et al. (2013). Consumer credit risk: Individual probability estimates using machine learning. *Expert systems with applications*, 40 (13), pp.5125–5131.

Le, H. H. and Viviani, J.-L. (2018). Predicting bank failure: An improvement by implementing a machine-learning approach to classical financial ratios. *Research in International Business and Finance*, 44, pp.16–25.

Lee, Y.-C. (2007). Application of support vector machines to corporate credit rating prediction. *Expert systems with applications*, 33 (1), pp.67–74.

Li, X.-L. and Zhong, Y. (2012). An overview of personal credit scoring: Techniques and future work. *International journal of intelligence science*, 02 (04), pp.181–189.

Lipton, A., Shrier, D. and Pentland, A. (2016). *Digital banking manifesto: the end of banks?* Massachusetts Institute of Technology USA.

Mason, S. and Bohm, N. (2017). Banking and fraud. *Computer Law & Security Review*, 33 (2), pp.237–241.

Mendling, J. et al. (2018). How do machine learning, robotic process automation, and blockchains affect the human factor in business process management? *Communications of the ACM*. [Online]. Available at: https://aisel.aisnet.org/cais/vol43/iss1/19/.

Mich, L. and Garigliano, R. (2002). NL-OOPS: A requirements analysis tool based on natural language processing. *WIT Transactions on Information and*. [Online]. Available at: https://www.witpress.com/elibrary/wit-transactions-on-information-and-communication-technologies/28/1239.

Mithe, R., Indalkar, S. and Divekar, N. (2013). Optical character recognition. *International journal of recent technology*. [Online]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.673.8061&rep=rep1&type=pdf .

Moro, S., Cortez, P. and Rita, P. (2015). Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation. *Expert systems with applications*, 42 (3), pp.1314–1324.

Paruchuri, H. (2017). Credit Card Fraud Detection using Machine Learning: A Systematic Literature Review. *ABC Journal of Advanced Research*, 6 (2), pp.113–120.

Patil, V. and Lilhore, U. K. (2018). A survey on different data mining & machine learning methods for credit card fraud detection. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3 (5), pp.320–325.

Peng, L.-X. and Chen, Y.-F. (2014). Positive Selection-Inspired Anomaly Detection Model with Artificial Immune. In: *2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. October 2014. ieeexplore.ieee.org. pp.56–59.

Rattadilok, P. and Petrovski, A. (2014). Self-learning data processing framework based on computational intelligence enhancing autonomous control by machine intelligence. In: *2014 IEEE Symposium on Evolving and Autonomous Learning Systems (EALS)*. December 2014. ieeexplore.ieee.org. pp.87–94.

Roychoudhury, S., Bellarykar, N. and Kulkarni, V. (2016). A NLP Based Framework to Support Document Verification-as-a-Service. In: *2016 IEEE 20th International Enterprise Distributed Object Computing Conference (EDOC)*. September 2016. ieeexplore.ieee.org. pp.1–10.

Ryman-Tubb, N. F., Krause, P. and Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering applications of artificial intelligence*, 76, pp.130–157.

Sakharova, I. (2012). Payment card fraud: Challenges and solutions. In: *2012 IEEE International Conference on Intelligence and Security Informatics*. June 2012. ieeexplore.ieee.org. pp.227–234.

Sayjadah, Y. et al. (2018). Credit Card Default Prediction using Machine Learning Techniques. In: *2018 Fourth International Conference on Advances in Computing, Communication Automation (ICACCA)*. October 2018. ieeexplore.ieee.org. pp.1–4.

Shabtai, A. and Elovici, Y. (2010). Applying Behavioral Detection on Android-Based Devices. In: *Mobile Wireless Middleware, Operating Systems, and Applications*. 2010. Springer Berlin Heidelberg. pp.235–249.

Singh, A., Bacchuwar, K. and Bhasin, A. (2012). A survey of OCR applications. *International Journal of Machine Learning and Computing*, 2 (3), p.314.

Singh, S. (2013). Optical character recognition techniques: a survey. *Journal of emerging Trends in Computing and*. [Online]. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.671.7331&rep=rep1&type=pdf .

Slosarik, K. (2002). Identity theft: An overview of the problem. *The Justice Professional*, 15 (4), pp.329–343.

Smeureanu, I., Ruxanda, G. and Badea, L. M. (2013). Customer segmentation in private banking sector using machine learning techniques. *Journal of business* . [Online]. Available at: https://www.tandfonline.com/doi/abs/10.3846/16111699.2012.749807.

Stolfo, S. et al. (1997). Credit card fraud detection using meta-learning: Issues and initial results. *on Fraud Detection and* …. [Online]. Available at: https://www.aaai.org/Papers/Workshops/1997/WS-97-07/WS97-07-015.pdf.

Sumathi, N. and Sheela, T. (2017). An empirical study on analyzing the distortion detection on OSN using NLP amp; SA in banking institution. In: *2017 2nd International Conference on Computing and Communications Technologies (ICCCT)*. February 2017. ieeexplore.ieee.org. pp.6–14.

Surya, L. (2015). An Exploratory Study of AI and Big Data, and It's Future in the United States. *International Journal of Creative Research Thoughts*. [Online]. Available at: https://papers.ssrn.com/abstract=3785652

Tang, Y. Y., Lee, S.-W. and Suen, C. Y. (1996). Automatic document processing: A survey. *Pattern recognition*, 29 (12), pp.1931–1952.

Tripathy, A. and Rath, S. K. (2014). Application of Natural Language Processing in Object Oriented Software Development. In: *2014 International Conference on Recent Trends in Information Technology*. April 2014. ieeexplore.ieee.org. pp.1–7.

Tsai, C.-F. and Chen, M.-L. (2010). Credit rating by hybrid machine learning techniques. *Applied soft computing*, 10 (2), pp.374–380.

Vafin, A. (2017a). Negotiation with Dominant Supplier: Power Determination, Partnership, and Joint Buying. *International Journal of Contemporary Financial Issues*. [Online]. Available at: https://hcommons.org/deposits/item/hc:44887/.

Vafin, A. (2017b). The Impacts of Performance Records, Influence Potential and Passion on Leadership Training Productivity. *Journal of Modern Issues in Business Research*. [Online]. Available at: https://hcommons.org/deposits/item/hc:44885/.

Vafin, A. (2018a). Should Firms Lower Product Price in Recession? A Review on Pricing Challenges for Firms in Economic Downturn. *ResearchBerg Review of Science and Technology* , 2 (3), pp.1–24.

Vafin, A. (2018b). Volume Discount Sensitivity Analysis for Optimal Pricing Strategies in B2B Firms. *Empirical Quests for Management Essences*, 2 (4), pp.15–29.

Vartak, M. et al. (2016). ModelDB: a system for machine learning model management. In: *Proceedings of the Workshop on Human-In-the-Loop Data Analytics*. HILDA '16 14. 26 June 2016. New York, NY, USA: Association for Computing Machinery. pp.1–3.

Vasquez, M. H. (2018). *The financial crimes management of account takeover fraud*. [Online]. Available at: https://repositories.lib.utexas.edu/handle/2152/63762.

Veeramachaneni, K. et al. (2016). AI\^ 2: training a big data machine to defend. In: *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. 2016. IEEE. pp.49–54.

Wang, G. et al. (2011). A comparative assessment of ensemble learning for credit scoring. *Expert systems with applications*, 38 (1), pp.223–230.

Zeager, M. F. et al. (2017). Adversarial learning in credit card fraud detection. In: *2017 Systems and Information Engineering Design Symposium (SIEDS)*. April 2017. ieeexplore.ieee.org. pp.112–116.