VILNIUS TECH
Vilnius Gediminas Technical University

12th International Scientific Conference

BUSINESS AND MANAGEMENT 2022

May 12–13, 2022, Vilnius, Lithuania

ISSN 2029-4441 / eISSN 2029-929X
ISBN 978-609-476-288-8 / eISBN 978-609-476-289-5
Article Number: bm.2022.787
https://doi.org/10.3846/bm.2022.787

*FINANCE AND INVESTMENT: NEW CHALLENGES AND OPPORTUNITIES* *http://vilniustech.lt/bm*

# INVESTIGATION OF FINANCIAL FRAUD DETECTION BY USING COMPUTATIONAL INTELLIGENCE

Ieva VOSYLIŪTĖ*, Nijolė MAKNICKIENĖ

*Department of Financial Engineering, Faculty of Business Management, Vilnius TECH, Saulėtekio av. 11, LT-10223, Vilnius, Lithuania*

Received 2 February 2022; accepted 7 April 2022

**Abstract.** Due to increasing technical capabilities, financial fraud becomes more sophisticated and more difficult to detect. As there are various categories and typologies of financial fraud, different detection techniques may be applied. However, based on the data generated daily by financial organizations, a technical solution must be implemented. This paper presents a comprehensive literature review of financial fraud, the categorizations of financial fraud, and financial fraud detection with the particular focus on computational intelligence-based techniques. As outlined in the reviewed literature, money laundering is a multilayered crime involving several fraud typologies; therefore, it was selected to be analysed in this research. The purpose of the research is to investigate the synthetic dataset of the money laundering scheme to see whether additional patterns could be outlined, which would help financial organizations to recognize suspicious activity easier. To achieve this goal, computational intelligence - decision tree, was selected as a classification method to identify additional patterns. As a result, data classification provides new data parameters which are essential in improving accurate and efficient financial fraud detection.

**Keywords:** financial fraud, fraud detection, money laundering, computational intelligence, machine learning, neural network, decision tree.

**JEL Classification:** G40, G28, G38, C45, C55, C63.

## Introduction

In a time where technologies evolve at such a rapid pace, it is essential to adapt them into the financial system. Fintech organizations are the leaders who implement new technologies and tools to improve financial services and their accessibility (Gomber et al., 2018). However, we should not forget that with every great technical achievement more risks arise. Technological growth allows not only legitimate financial organizations to improve their services, but also to provide various ways for bad actors to use these technical paths to defraud customers of financial services or use these services for illegitimate activities (Reurink, 2018). Although organizations adopt new ways of providing financial services, they must remain vigilant and use all the technical advantages to detect financial fraud. The ability to quickly and accurately review and classify a huge amount of data is the main asset when identifying financial fraud and its risks (Kordon, 2010). With the amount of data involved in a day-to-day financial activity, it is impossible to effectively evaluate and assess the threat of financial fraud using only human capital. Artificial intelligence is a great tool that provides financial companies with the ability to identify financial fraud faster and more accurately without using manual labor (Saia & Carta, 2019). Since there is a great variety of financial fraud types and ways of using a financial system for illegitimate purposes, the theoretical part of this paper reviews the most common types of financial fraud, ways to detect financial fraud, and explains how computational intelligence can be used to identify fraud patterns and red flags. Since the decision tree algorithm is described as one of the best ways to categorize a large amount of data (Esmaily et al., 2015), it was selected as the main research method and is reviewed in detail in the second part of the article. The third part is dedicated to analyzing the research results and obtain the conclusions. Such research not only gives us the opportunity to familiarize with a financial fraud and its detection using computational intelligence, but also allows us to identify new perspectives and approaches to do it.

* Corresponding author. E-mail: *ieva.vosyliute@stud.vilniustech.lt*

The research problem that this paper addresses is to investigate the use of computational intelligence in the detection of financial fraud by creating new data patterns that would help minimize the potential risk of fraud in financial organizations. The main purpose of this research is to identify whether certain transactional criteria could suggest possible fraudulent activity. To further investigate the problem of the research, key objectives were set:

- Analysis of the scientific literature to define key concepts of financial fraud, financial fraud typology, and techniques for financial fraud detection.
- Identification and investigation of computational intelligence methods that are the best fit to detect fraudulent activity patterns in the financial transaction dataset.

## 1. Concept of financial fraud

Nowadays we have a variety of financial products, and the market is still expanding (Krueger, 2006). This rapid development not only enables financial companies to reach wider consumer groups, but also increases the risk of financial fraud (Teichmann, 2019). Financial fraud is a sophisticated crime which evolved over the time and now affects more companies and individuals; since financial institutions are creating more impersonal ways of conducting their business, this opens a rich environment for committing fraud (Subramanian, 2014). The Oxford Dictionary defines fraud as: *wrongful or criminal deception intended to result in financial or personal gain*; however, a more detailed and thorough characterization of the fraud phenomenon is provided by Van Vlasselaer (2017): "*Fraud is an uncommon, well-considered, imperceptibly concealed, time-evolving, and often carefully organized crime which appears in many types and forms*". This description emphasizes the complexity of fraud that varies in its types and forms. The Table below provides a description and overview of the most important fraud types based on its frequency of occurrence and monetary value involved.

Table 1. List of fraud categories and types (source: Baesens et al., 2015; Singh & Best, 2019)

| | |
|---|---|
| Credit card fraud | Credit card fraud is an unauthorized use of another's credit. Common credit card fraud methods are counterfeiting credit cards, using lost or stolen cards, or fraudulently acquiring credit through mail. |
| Insurance fraud | Broad category-spanning fraud related to any type of insurance, both from the side of the buyer or seller of an insurance contract. |
| Corruption | Corruption is the misuse of entrusted power (by heritage, education, marriage, election, appointment, etc.) for private gain. |
| Counterfeit | An imitation intended to be passed off fraudulently or deceptively as genuine. |
| Product warranty fraud | Warranty fraud occurs when an individual or organization exploits warranty policies for their own benefit. |
| Healthcare fraud | Healthcare fraud is a type of white-collar crime that involves the filing of dishonest health care claims in order to turn a profit. |
| Telecommunications fraud | Telecommunications fraud is the theft of telecommunications services (telephones, cell phones, computers, etc.) or the use of telecommunication service to commit other forms of fraud. |
| Money laundering | Money laundering is the process by which criminals attempt to disguise illicit assets as legitimate assets that they have a right to possess and spend. |
| Identity theft | The crime of obtaining the personal or financial information of another person for the purpose of assuming that person's name or identity in order to make transactions or purchases. |
| Tax evasion | Tax evasion is illegal act or practice of non-payment or under-payment of taxes that are owed. |

Despite different categories of financial fraud, the representation of fraud varies widely depending on the market segment in which it is perpetrated, the financial instruments on which it is dependent, and the actors involved (Reurink, 2018). Based on these variables, a conceptual distinction is made between three typologies of financial fraud (see Table 2).

Table 2. Typology of financial fraud (source: Reurink, 2018)

| | Nature of the deception | Nature of the enterprise |
|---|---|---|
| False financial disclosures | Plain lies / misstatements of facts | Legitimate |
| Financial scams | Plain lies / misstatements of facts | Illegitimate |
| Fraudulent financial mis-selling | Misleading impressions | Legitimate / Illegitimate |

By this classification, fraud typologies seem defined and the environment in which they are perpetrated is straight forward; however, in real life the boundaries between the categories are blurry and not all cases fit neatly only into one typology (Reurink, 2018). It is essential to understand the fundamental principles of each of the typologies to be able to detect them effectively and efficiently.

*False financial disclosures*. This term groups a wide range of behaviors where financial market participants falsify statements about the financial health or performance of investment product and manipulate the data to make investment outlet more attractive (Black, 2006). Despite the deceptive information, financial fraud disclosures pertain to a legitimate enterprise. This type of fraud occurs when representatives of the legitimate entity manipulate to cover the misuse of the company's funds or mislead investors by falsifying financial reports (Reurink, 2018). The complexity and dynamic movement of information makes it difficult to detect financial statement

alterations; therefore, this fraud typology is thriving regardless of all the regulations (Chen et al., 2019).

*Financial scams*. This is one of the oldest types of fraud which is built on fabricated information and lies (Kadoya et al., 2020). It differs from other typologies in that the information provided is deceptive and the enterprise involved in fraud scenario is not legitimate; this is purely a social engineering in which targeted victims are tricked to provide their sensitive personal and financial details (Airehrour et al., 2018). Based on the financial tools used and the targeted victims, such as elderly people or other vulnerable groups, financial scams can be divided into two branches: investment scam and financial identity scams (Fenge & Lee, 2018).

*Fraudulent financial mis-selling*. This is a term that describes the use of manipulative marketing to sell a financial product to the end user knowing that the product or service does not meet the needs of the end users' needs (Singh & Dipika, 2018). As outlined by Reurink (2018) mis-selling fraud scenarios use legitimate financial products such as pension saving plans or life insurance plans while manipulating information to convince the user that this solution is suitable for them. In this fraud typology, fraudsters may use both legitimate and illegitimate enterprises to support their scenario, which makes it difficult to detect and prevent (Brannan, 2017).

### 1.1. Concept of money laundering

Money laundering is a complex criminal activity that is one of the most significant threats to financial systems (Nestorova, 2019). Money laundering is a process of disguising the illegal origin of criminal proceeds consisting of three stages of money laundering (Salehi et al., 2017):

1. Placement – the first stage of money laundering where illegally acquired funds are placed into legitimate financial systems, for example, using offshore accounts.
2. Layering – the second stage of money laundering a complex system of transactions is created to move money within the financial system, for example, transferring funds from the bank account to the holding company.
3. Integration – during this final money laundering stage, money is absorbed into the economy by purchasing goods and services, for example, buying real estate, art. After this stage, the source of funds appears to be legitimate.

Fraud is considered a basis for money laundering, as it requires deception to embed illegally obtained funds into the financial system concealing their criminal origin. As there are three stages of money laundering, several fraud typologies are applied: false financial disclosure and financial scam. On 2003 Financial Action Task Force (FATF) set anti-money laundering (AML) regulations for financial institutions, where based on customer, business relation and transaction data customer due diligence measures must be applied. The regulations evolved and were strengthened during the years, which requires constant data monitoring in order for financial institutions to comply (Ross & Hannan, 2007). With the amount of data generated daily by financial institutions, a technical solution is needed in order to follow AML requirements (Tundis et al., 2021).

### 1.2. Computational intelligence in financial fraud detection

The amount of information kept in modern databases is enormous; but to detect financial fraud and effectively make decisions, this information needs to be structured and summarized (Bodyanskiy, 2005). Financial fraud is a growing threat with considerable consequences to the financial sector; therefore, effective and timely fraud detection is crucial to control and minimize fraud risk (Kou et al., 2017). Internal audits and ongoing monitoring are the main tools to detect red flags that could lead to financial fraud. Previously to thoroughly evaluate fraud risk factors, auditors needed to review company policies, procedure, financial statements, and other documentation, taking into account management, industry, and operating characteristics (Kenyon & Tilton, 2011). Due to the amount of data financial institutions generate daily, it is impossible to manually review it and assess the fraud risks. A set of automated activities were generated to detect and block fraudulent attempts creating a fraud detection cycle (see Figure 1.).

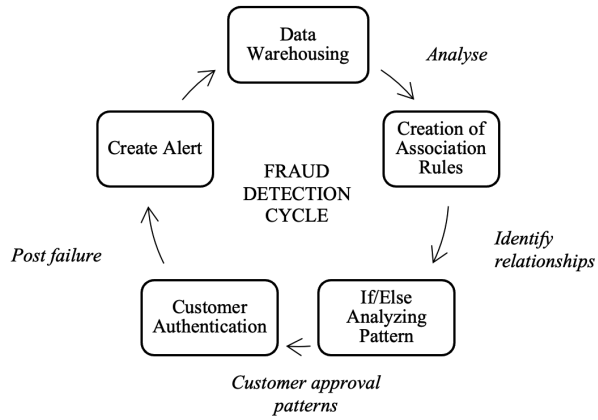


Figure 1. Fraud detection cycle
(source: Kanade, 2021)

As Kanade (2021) reviews the relationship between automated activities, the importance of each segment and correct sequence is emphasized. This is a combination of risk management systems and modern fraud detection and prevention tools that monitor fraudulent events in real time across various platforms. As financial fraud is a complex crime and has different types and forms, there are also different techniques used to detect it. Data analysis-based techniques are the most effective (Farouk et al., 2019) and can generally be categorized into statistical data analysis techniques or artificial intelligence techniques (see Figure 2).

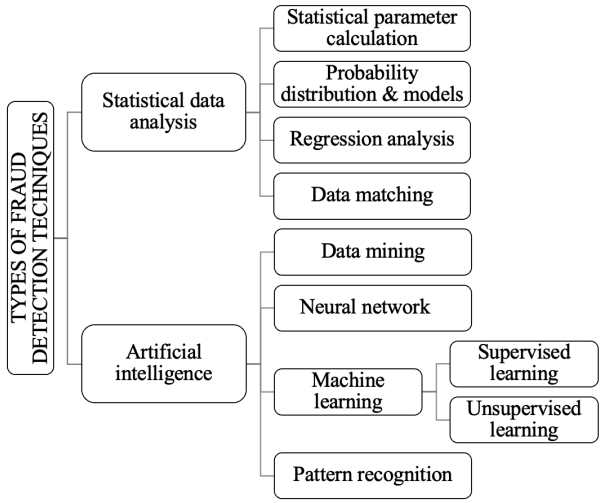


Figure 2. Types of fraud detection techniques (source: Kanade, 2021)

Computational intelligence encloses numbers of different methodologies, and one of the most popular is Artificial Neural Networks (ANN) (Bodyanskiy, 2005). Neural networks are not only based on intelligence and pattern recognition (Smith, 2003); they were designed to mimic how the brain learns and analyses information (Soumya & Deepika, 2016). This method is widely used in large organizations where complex predictive analysis is required. Computational intelligence is more accurate and effective in detecting tendencies that are too complex to be noticed by humans or other computer techniques. ANN have several different architectures where the most prominent are multilayer perceptron, radial basis function networks, and self-organizing maps (see Table 3).

Table 3. Architectures of neural networks (source: Bodyanskiy, 2005)

| | |
|---|---|
| Multilayer perceptron | Used for approximation, regression, and classification. Training of the multilayer networks is very slow. |
| Radial basis functions networks | Used for classification and regression. Training is faster than for multilayer perceptron. |
| Self-organizing maps | Used for clustering, visualization, and classification. Their learning is called competitive learning. |

By using artificial neural networks, organizations have better fraud detecting abilities under different contexts (Soumya & Deepika, 2016). The overview of financial fraud typologies and categories showed the wide scope of data that needs to be taken into consideration while looking for the red flags: this is not only the main personal transactional information such as name, country, or the amount involved; it also includes technical data such as passwords, fingerprints, and IP addresses (Zhang et al., 2018). ANN is a great tool that can learn and classify different variables related to financial fraud, allowing organizations to reduce risk and protect their customers. As a financial fraud detection tool, computational intelligence has its own advantages and disadvantages. The main benefits of neural networks are the level of accuracy and the ability to identify links that cannot be discovered by humans (Kordon, 2010). This not only helps to detect financial fraud in a timely manner but allows one to group and link various patterns and red flags which could not be manually identified. As any other technological solution, it has its downsides as well, and, as Kordon (2010) outlined, it takes a considerably long time for neural networks to learn new paths from the amount of data gathered. However, with the increasing amount of data gathered by organizations required to provide their services, computational intelligence is one of the most reliable techniques to detect financial fraud (Wang et al., 2021).

## 2. Methodology

### 2.1. Methodological steps

The main purpose of this research is to apply and investigate one of the computational intelligence techniques in financial fraud detection. Based on the literature review, the following criteria were selected for this research:

1. Fraud type analyzed – money laundering.
2. Fraud detection technique applied – neural network decision tree.

Based on the impact of money laundering and the amounts involved in this activity, this type of fraud was selected for the research investigation. The synthetic money laundering dataset used for this research was taken from the open-source database kaggle.com. Dataset simulation is based on three money laundering stages in financial transactions: placement, layering, integration. The dataset has a specification whether the transaction is fraudulent or not, and if fraudulent, it is additionally classified as to which stage of money laundering it belongs.

The multilayer perceptron neural network and decision trees are the most applicable and most popular machine learning algorithms for classification (Esmaily et al., 2015). Classification algorithms are able to retrieve relevant information from the dataset and detect patterns, allowing to improve analysis, forecasting and decision making (Tundis et al., 2021). Since the objective of the research is to investigate whether there are additional patterns in fraudulent activity, the data classification method, the decision tree, was selected. MATLAB (Matrix Laboratory) is utilized to perform the experiment due to its ease and beneficial programming environment for researchers. MATLAB is a multi-worldview arithmetical processing environment and exclusive programming language established by MathWorks. It permits framework controls, plotting of functions and information, execution of algorithms, production of User Interfaces, written in different languages.

### 2.2. Decision tree algorithms

Decision tree is a supervised learning technique that allows to identify features and patterns in large databases, which is important for predictive modelling (Myles et al., 2004). There are several statistical algorithms available to build decision trees: CART (Classification and Regression Trees), C4.5, CHAID (Chi-Squared Automatic Interaction Detection), and QUEST (Quick, Unbiased, Efficient, Statistical Tree) (Song & Lu, 2015). Comparison of the most widely used decision tree algorithms is provided in the Table 4.

In the decision tree, the decision and data classification are done based on the given dataset which is split into *decision node* – used to make decision and further segregate the data; and *leaf node* – final output of the node with no additional segregation (see Figure 3).

By applying this method, the information in the dataset will be classified according to the criteria of whether it is a fraud or not. Also, by additional criteria which would reveal if specific patterns can be outlined in the fraudulent activity, allowing to indicate them as potential red flags for future financial fraud investigation.

## 3. Research results

The objective of this research was to apply the decision tree algorithm to identify whether there are additional indications of fraudulent activity by classifying transactional data. In this algorithm, the transaction was selected as predictor variable [X] which was sorted by fraud indicator [Y] – fraud or no fraud (see Figure 4).

In this research, the dataset was spilt into two parts: 70% of the data was used to train the algorithm and 30% was used to test the accuracy of the algorithm. Transactions were selected randomly for both training and testing, to obtain more precise calculations of the accuracy of the decision tree algorithm. Based on the calculated accuracy level (Figure 5), the determination can be made that the amount of transaction may indicate money laundering activity.

### 3.1. Results and discussion

After applying data classification, decision tree, and evaluating the accuracy of the classification, the determination can be made that with an average accuracy around 96,46%, this type of data classification allows

Table 4. Comparison of different decision tree algorithms (source: Song & Lu, 2015)

| | CART | C4.5 | CHAID | QUEST |
|---|---|---|---|---|
| Measure for input variable | Gini index; Twoing criteria | Entropy info-gain | Chi-square | Chi-square for categorical variables; J-way ANOVA for continuous/ordinal variables |
| Pruning | Pre-pruning using a single-pass algorithm | Pre-pruning using a single-pass algorithm | Pre-pruning using Chi-square test for independence | Post-pruning |
| Dependent variable | Categorical/ Continuous | Categorical/ Continuous | Categorical | Categorical |
| Input variables | Categorical / Continuous | Categorical / Continuous | Categorical / Continuous | Categorical / Continuous |
| Split at each node | Binary; Split on linear combinations | Multiple | Multiple | Binary; Split on linear combinations |

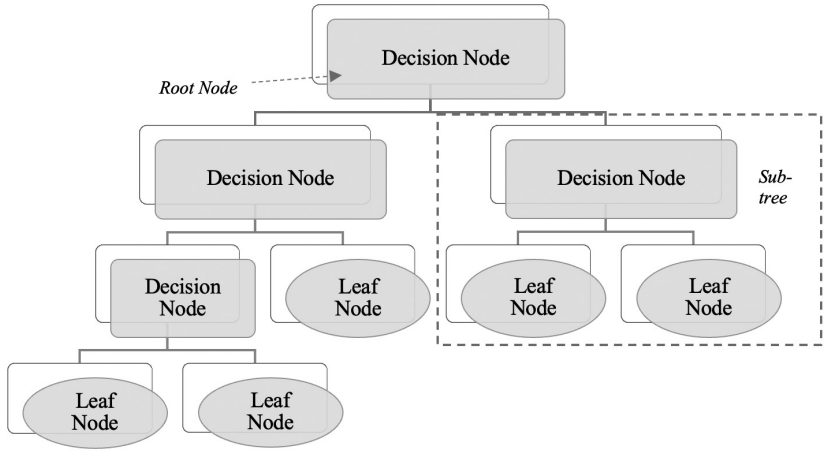


Figure 3. Decision tree scheme (source: Song & Lu, 2015)

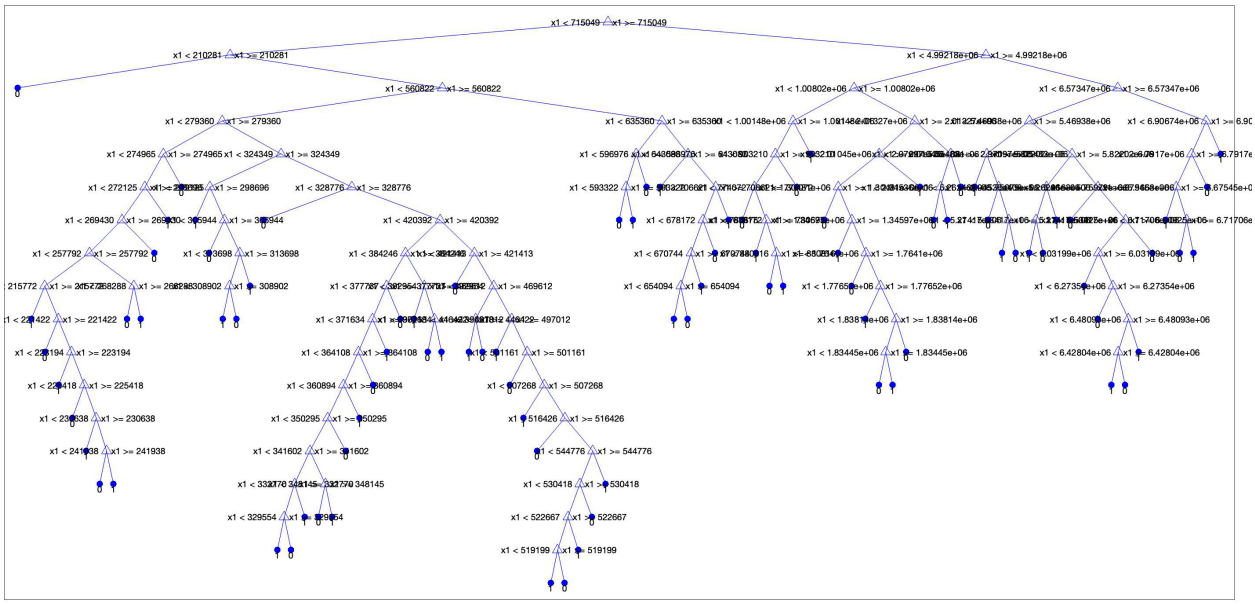

Figure 4. Fragment of decision tree classification (source: MATLAB outcome, prepared by the authors)

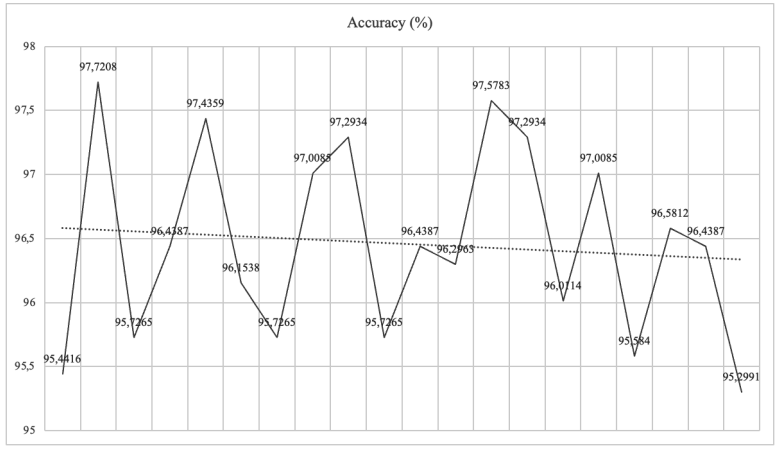


Figure 5. Accuracy level of decision tree classification (source: prepared by the authors)

one to indicate transaction amounts which were mostly used in money laundering activities and mark them as potential fraud for further review. Figure 4. Shows us how many data segregations are performed to accurately classify and distinguish which amounts were linked with money laundering related activity and which were not. Such data classification brings the ability to reduce the scope of potential fraudulent transactions, allowing financial institutions to review them in depth faster and with greater response.

## Conclusions

The reviewed theory suggests that financial fraud affects the entire financial sector due to the variety of products and services offered, as it is very complex and has a lot of variables depending on its methods and typologies. Therefore, it is crucial to implement technological solutions not only to broaden the organization's portfolio, but also to protect it from financial fraud risk.

Although there are different tools and techniques to detect and prevent financial fraud, extensive analysis is required for organizations to adopt the most suitable solution based on their products and services offered, as well as the target customer. Subject matter experts outline that computational intelligence is a great tool to implement in financial organizations, as it offers the ability to detect the most sophisticated fraud patterns and red flags. However, it has its disadvantages, the ability to learn and adapt to a rapidly changing financial environment, which overweigh potential negative implications of this tool.

To fulfil the set goal of the research, the decision tree method was selected as it is one of the best suited classification algorithms that could be used in large datasets. It allows the data to be segmented that could be investigated further to identify patterns of suspicious activity in the financial environment. The research results showed that transactional information, in particular the transactional amount, has indications of patterns of financial

fraud. Classifying data in this way allows financial organizations to accurately update their fraud detection tools and reduce the risk of fraud for the company.

This research covers just a small part of the computational intelligence ability to detect financial fraud and set a basis for further investigations. As discussed, there is a great variety of fraud methods along with a wide range of computational intelligence tools that could be applied in detecting financial fraud and should be further analyzed.

## References


Airehrour, D., Vasudevan Nair, N., & Madanian, S. (2018). Social engineering attacks and countermeasures in the New Zealand banking system: advancing a user-reflective mitigation model. *Information, 9*(5), 110. https://doi.org/10.3390/info9050110

Krueger, A. O. (2006). Financial Markets and Economic Growth. *CFA Digest (1999), 29*(3), 9–10. https://doi.org/10.2469/dig.v29.n3.504

Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud analytics using descriptive, predictive, and social network techniques: a guide to data science for fraud detection*. https://doi.org/10.1002/9781119146841

Black, W. K. (2006). Book review: Control fraud theory v. the protocols. *Crime, Law & Social Change, 45*, 241–258. https://doi.org/10.1007/s10611-006-9031-7

Bodyanskiy, Y. (2005). *Computational Intelligence Techniques for Data Analysis*. 15–36. https://www.researchgate.net/publication/221106211_Computational_Intelligence_Techniques_for_Data_Analysis

Brannan, M. J. (2017). Power, corruption and lies: Mis-selling and the production of culture in financial services. *Human Relations*, *70*(6), 641–667. https://doi.org/10.1177/0018726716673441

Chen, Y.-J., Liou, W.-C., Chen, Y.-M., & WuKirkos, J.-H. (2019). Fraud detection for financial statements of business groups. *International Journal of Accounting Information Systems*, *32*, 1–23. https://doi.org/10.1016/j.accinf.2018.11.004

Esmaily, J., Moradinezhad, R., & Ghasemi, J. (2015). Intrusion Detection System Based on Multi-Layer Perceptron Neural Networks and Decision Tree. *2015 7th Conference on Information and Knowledge Technology, IKT 2015*. https://doi.org/10.1109/IKT.2015.7288736

Farouk, A., Zhen, D., & Laurier, W. (2019). Big data analysis techniques for intelligent systems. *Journal of Intelligent & Fuzzy Systems*, *37*, 3067–3071. https://doi.org/10.3233/JIFS-179109

Fenge, L.-A., & Lee, S. (2018). Understanding the risks of financial scams as part of elder abuse prevention. *British Journal of Social Work*, *48*, 906–923. https://doi.org/10.1093/bjsw/bcy037

Gomber, P., Kauffman, R. J., Parker & Bruce, C., & Weber, W. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Kadoya, Y., Saidur, M., Khan, R., & Yamane, T. (2020). The rising phenomenon of financial scams: evidence from Japan. *Journal of Financial Crime, 27*(2), 387–396. https://doi.org/10.1108/JFC-05-2019-0057

Kanade, V. (2021). *What Is Fraud Detection? Definition, Types, Applications, and Best Practices | Toolbox It-security*. https://www.toolbox.com/it-security/vulnerability-management/articles/what-is-fraud-detection/

Kenyon, W., & Tilton, P. D. (2011). Potential red flags and fraud detection techniques. In T. W. Golden, S. L. Skalak, & M. M. Clayton (Eds). *A Guide to Forensic Accounting Investigation: Chapter 8*. http://160592857366.free.fr/joe/ebooks/Corporate%20Finance/Wiley%20A%20Guide%20to%20Forensic%20Accounting%20Investigation.pdf

Kordon, A. K. (2010). *Applying Computational Intelligence*. https://doi.org/10.1007/978-3-540-69913-2

Kou, Y., Lu, C.-T., Sinvongwattana, S., & Huang, Y.-P. (2017). Survey of fraud detection techniques. *International Conference on Networking, Sensing & Control*, *2*, 749–754. https://doi.org/10.1109/ICNSC.2004.1297040

Myles, A. J., Feudale, R. N., Liu, Y., Woody, N. A., & Brown, S. D. (2004). An introduction to decision tree modeling. *Journal of Chemometrics*, *18*(6), 275–285. https://doi.org/10.1002/cem.873

Nestorova, V. (2019). Anti-money laundering policies in the financial sector. *5th LIMEN Conference Proceedings (Part of LIMEN Conference Collection), 89–94*. https://doi.org/10.31410/LIMEN.2019.89

Reurink, A. (2018). Financial fraud: a literature review. *Journal of Economic Surveys*, *32*(5), 1292–1325. https://doi.org/10.1111/joes.12294

Ross, S., & Hannan, M. (2007). Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control*, *10*(1), 106–115. https://doi.org/10.1108/13685200710721890

Saia, R., & Carta, S. (2019). Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. *Future Generation Computer Systems*, *93*, 18–32. https://doi.org/10.1016/j.future.2018.10.016

Salehi, A., Ghazanfari, M., & Fathian, M. (2017). Data Mining Techniques for Anti Money Laundering. *International Journal of Applied Engineering Research*, *12*, 10084–10094. http://www.ripublication.com

Singh, D. S., & Dipika, M. (2018). MIS-Selling of financial products: a review. *NOLEGEIN-Journal of Financial Planning and Management*, *1*(2), 1–11. https://www.mbajournals.in/index.php/JoFPM/article/view/128

Singh, K., & Best, P. (2019). Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, *34*. https://doi.org/10.1016/j.accinf.2019.06.001

Smith, P. I. (2003). *Neural Networks*. https://doi.org/10.2172/815740

Song, Y. Y., & Lu, Y. (2015). Decision tree methods: applications for classification and prediction. *Shanghai Archives of Psychiatry*, *27*(2), 130–135. https://www.researchgate.net/publication/279457799_Decision_tree_methods_applications_for_classification_and_prediction

Soumya, S. B., & Deepika, N. (2016). Data mining with predictive analytics for financial applications. *International Journal of Scientific Engineering and Applied Science (IJSEAS)*, *2*(1), 310–319. https://ijseas.com/issue-archive-2/volume2/issue-2/

Subramanian, R. (2014). *Bank fraud : using technology to combat losses*, 3. https://doi.org/10.1002/9781118886168

Teichmann, F. (2019). Recent trends in money laundering. *Crime, Law and Social Change 73*, 237–247. https://doi.org/10.1007/s10611-019-09859-0

Tundis, A., Nemalikanti, S., & Mühlhäuser, M. (2021). Fighting organized crime by automatically detecting money laundering-related financial transactions. *The 16th International Conference on Availability, Reliability and Security (ARES 2021)*, *38*, 1–10. https://doi.org/10.1145/3465481.3469196

Van Vlasselaer, V., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2017). Network-based fraud detection for social security fraud. *Management Science*, *63*(9), 3090–3110. https://doi.org/10.1287/mnsc.2016.2489

Wang, Y., Stuart, T., & Li, J. (2021). Fraud and Innovation. *Administrative Science Quarterly*, *66*(2), 267–297. https://doi.org/10.1177/0001839220927350

Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2018). A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection. *Security and Communication Networks Volume 2018, Article ID 5680264, 9 Pages*. https://doi.org/10.1155/2018/5680264