World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Fraud detection: Develop skills in fraud detection, which is a critical area of business analytics

Md. Maruful Islam [1,*], Abdullah Hill Hussain [1], Md. Nayeem Hasan [1], Sharmin Sultana Akhi [2], Mohammad Sajjad Hossain [1] and Sanjida Islam [1]

[1] *Student, MS in Information Technology, Washington University of Science & Technology, Viriginia, USA.*
[2] *Student, MSC in Computer Science, Monroe College, USA.*

World Journal of Advanced Research and Reviews, 2023, 18(03), 1664-1672

Publication history: Received on 28 April 2023; revised on 13 June 2023; accepted on 15 June 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.18.3.0969

Abstract

The identification of fraudulent behavior is the fundamental objective of fraud detection, which is an essential component of business analytics. In the process of detecting fraud, this is the primary objective. After this step has been decided, the subsequent steps that need to be taken in order to reduce the negative effects of the activity are put into action. In order to achieve the desired outcomes throughout the detection process, a variety of analytical approaches are used in a number of different ways. This action is taken in order to achieve the objective that has been established. When all of this is taken into account, one of the most important aspects that is involved is the identification of fraudulent activity. The purpose of this abstract is to provide an overview with the intention of achieving the aim of giving an overview of the important skills and methodologies that are necessary for efficient fraud detection. This abstract was produced with the intention of presenting the facts in order to meet the aim of providing this overview. In order to fulfill the job of providing the reader with a summary of the information that was presented, the purpose of this abstract is to execute that function. The fact that the components of data analysis, statistical modelling, and machine learning are given a special priority is something that has to be taken into account, and this is something that needs to be taken into consideration. The importance of giving careful thought to this specific aspect cannot be overstated. Those individuals who are interested in achieving success in business analytics are needed to fulfill the prerequisites in order to acquire the information and abilities that are necessary to recognize fraudulent behavior. The satisfaction of this need is very necessary in order to attain success in this particular area of the economy. It is possible that gaining a grasp of methods like as predictive modelling, machine learning, and anomaly detection might considerably increase the capability of analysts to significantly enhance the capacity of their firms to both avoid fraudulent acts and react to them. It is possible to achieve this goal by acquiring a deeper comprehension of these technological approaches. To be more specific, this is due to the fact that analysts have the capability of concurrently improving both processes. This is the reason why things are the way they are. There is a vast variety of approaches that analysts have the ability to put into action, including the tactics that have been mentioned in this article. In a digital world that is becoming more difficult to traverse, these steps, which are proactive in nature, not only lessen the likelihood of incurring financial losses, but they also ensure that the integrity of the company's operations is preserved. These individuals demonstrate initiative in a broad variety of circumstances across the board, which is one of the probable explanations for this phenomenon.

Keywords: Business Analytics; Fraud Detection; Information technology; Cyber Security; Statistical analysis

1. Introduction

Fraud detection has become an essential part of business analytics, it is essential to learn a broad range of skills and methods in order to be able to counteract fraudulent activities that are becoming more complex. This is because fraud

* Corresponding author: Md. Maruful Islam

detection has become a crucial component of business analytics. This is because the detection of fraudulent behavior has developed into a significant component of business analytics. This is the result that has come about as a direct consequence of the fact that the detection of fraudulent behavior has developed into a significant component of business analytics. This is the outcome that has come about as a direct consequence of the fact that this has come about. [1] This is the result that has come about as a direct consequence of the fact that the detection of fraudulent activity has evolved into an essential component of business analytics. Providing an overview of the most significant ideas, methodologies, and roles that are linked with the detection of fraudulent behavior is the purpose of this literature review, which aims to accomplish this goal. This is done with the intention of providing a full overview of the topic that is now being discussed, and it is done with the objective of presenting just that. Utilizing the synthesis process in order to get the outcomes that are wanted will allow for the successful completion of this objective. The aim of concluding this assessment in order to achieve the target will be accomplished by conducting a thorough examination of the relevant literature. [2] This will be done in order to accomplish the goal. Since the purpose of this research is to cover a broad variety of subjects, it will make use of a large number of diverse sources in order to achieve its objective. This is because the study is designed to cover a wide range of themes. [3]

1.1. Data Profiling

Datasets are examined as part of the process of data profiling in order to get a knowledge of both the structure of the datasets as well as the information that is included within each dataset on its own. In order to be able to notice unusual patterns or inconsistencies that may be suggestive of fraudulent activities, it is of the highest essential to acquire this talent. Doing so will allow you to identify fraudulent operations. By using data profiling, analysts can construct baselines for usual behavior, which not only helps in the discovery of deviations that need additional investigation, but also helps in the building of baselines. The significance of this advantage cannot be overstated. [4]

1.2. Predictive Modeling

Utilizing statistical methods is a component of the predictive modelling approach, which is used in the process of predicting the likelihood of future occurrences by utilizing data from the past. Utilizing models is a helpful tool that makes the accomplishment of this objective easier. Because of this capability, analysts are able to assess the risk that is associated with transactions and to detect potential instances of fraud before they take place.25 This is achievable because of the capacity. This capacity is important for the purpose of identifying fraudulent conduct inside an organization. Methods such as logistic regression and decision trees are examples of approaches that are often used in the process of constructing predictive models. Other examples include other related methods. Some further examples include alternative ways that are equivalent. [5]

1.3. Anomaly Detection

Generally speaking, the method of anomaly detection is used for the aim of detecting data points that exhibit a considerable divergence from the norms that have been established. Because this is the primary objective of the approach, it is intended to achieve it. This is the most important goal that we are able to achieve within our capability. It is of the utmost importance to make use of this strategy in order to get the desired results in order to achieve the objective of identifying potentially fraudulent transactions or behaviors that take place inside an organization. The rationale for this condition is because it provides businesses with the opportunity to do proactive study on potential problems in the future, which is the reason why this condition has come about. By virtue of the fact that this is the case, it is possible for companies to identify potential problems that may manifest themselves in the future. [6]

1.4. Behavioral Analysis

When it comes to determining what it is that serves as the defining characteristic of regular activity inside a system, having a solid understanding of user behavior is an extremely crucial need that must be satisfied. The patterns of transactions and the interactions of users are analyzed by analysts in order to identify any abnormalities that may be indicative of fraudulent behavior13. This is done to find potentially fraudulent behavior. [7] This investigation is carried out with the purpose of identifying any possible instances of fraudulent activity. If an organization is able to acquire this capability, it will be much easier for them to create effective thresholds for warnings and actions, which will enable them to take the appropriate measures. [8]

1.5. Techniques Employed in Fraud Detection

There is a vast range of analytical approaches and technological tools that are used in the process of determining whether fraudulent behavior has occurred or not. These include the items that are included in the following list:

Statistical analysis is the process of examining data in order to find deviations from the criteria of statistical analysis. This process is referred to as statistical analysis or statistical analysis. For describing this process, the part "statistical analysis" is used.

utilizing network analysis, it is possible to find relationships between diverse entities, which may ultimately lead to the discovery of elaborate fraud schemes. This discovery may be made feasible utilizing network analysis. Data mining methods are one method that might be used to attain this goal. [9]

The systems that evaluate transactions as they are taking place and notify any suspect behaviors in a timely way are referred to as "real-time monitoring" in the context of the financial industry. The phrase "real-time monitoring" appears in the context of the financial sector. [10]

In the process of pattern recognition, computers search for the existence of repeating patterns or correlations within data that may indicate fraudulent conduct. This approach is known as pattern recognition. The approach of pattern recognition is another name for this aforementioned procedure. In order to keep an eye out for fraudulent activities, it is possible to carry out this action. [11]

1.6. Fraud Detection Skills

When it comes to professionals that operate in a broad variety of professions, including the ones that are stated below, the ability to spot fraudulent conduct is one of the most critical abilities that each of these professionals have.

Data analysts are tasked with the responsibility of divulging sensitive information that is connected to fraudulent activity according to the work obligations that they are responsible for. This objective is finally accomplished via the process of doing research and analyzing statistical data with the end aim of achieving it.

Fraud analysts are those who are professionals in recognizing fraudulent activity and conducting investigations into it via the use of sophisticated analytics. In this context, the individuals in question are referred to as fraud analysts. [12]

One of the responsibilities that fall within the purview of risk analysts is the evaluation of the strengths and weaknesses that are present within organizations. In addition to this, risk analysts are accountable for the execution of rules that are designed to reduce the likelihood of fraudulent activity occurring. [13]

2. Literature Review

Fraud detection has become an essential part of business analytics, it is essential to learn a broad range of skills and methods in order to be able to counteract fraudulent activities that are becoming more complex. This is because fraud detection has become a crucial component of business analytics. This is as a result of the fact that the detection of fraudulent behaviour has developed into a significant component of business analytics. This is the result that has come about as a direct consequence of the fact that the detection of fraudulent behavior has developed into a significant component of business analytics. This is the outcome that has come about as a direct consequence of the fact that this has come about.[14] This is the result that has come about as a direct consequence of the fact that the detection of fraudulent activity has evolved into an essential component of business analytics. Providing an overview of the most significant ideas, methodologies, and roles that are linked with the detection of fraudulent behavior is the purpose of this literature review, which aims to accomplish this goal. [15] This is done with the intention of providing a full overview of the topic that is now being discussed, and it is done with the objective of presenting just that. Utilizing the synthesis process in order to get the outcomes that are wanted will allow for the successful completion of this objective. The aim of concluding this assessment in order to achieve the target will be accomplished by conducting a thorough examination of the relevant literature. This will be done in order to accomplish the goal. Since the purpose of this research is to cover a broad variety of subjects, it will make use of a large number of diverse sources in order to achieve its objective. This is because the study is designed to cover a wide range of themes. [16]

When it comes to effectively combatting the ever-changing market of fraudulent activities, it is very important for businesses to include sophisticated analytics into their processes for identifying fraudulent activity. [17] This is because the domain of fraudulent activities is always evolving. This is due to the fact that fraudulent schemes are always being developed. As a consequence of the fact that the realm of fraudulent actions is always undergoing transformation, this is the outcome achieved. Methods such as predictive modelling, machine learning, and anomaly detection are examples of ways that organizations may utilize in order to accomplish the proactive identification of threats and the successful execution of preventive measures. [18] These are all examples of approaches that may be used by businesses. Through

the use of these measures, businesses are able to forestall the onset of potential dangerous situations. A prominent point of attention within the field of business analytics will continue to be the development of abilities in fraud detection for the duration of the industry's continued growth. This will be the case for the duration of the industry's growth. [19] This objective is going to be maintained throughout the whole of the growth of the industry. As a result of the fact that the ability to identify fraudulent activity is one that is always evolving, this is the situation. Due to the fact that this is the case, businesses will be able to safeguard their financial integrity and continue to ensure that their customers continue to have trust in them. [20]

2.1. Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining:

Bao et al. (2020). The goal of this article is to complete the investigation, with the intention of providing a comprehensive analysis of the method that is used to ascertain whether or not bank accounts have been susceptible to fraudulent activity. To finish the examination is the goal of the testing procedure. The primary objective of this piece of writing is going to be to provide a full analysis of the methodology that was used in order to arrive at this conclusion. This will be the primary aim of this dissertation. Nevertheless, it shines light on difficulties such as the imbalance of data and the validity of models, places a focus on the methods of machine learning and data mining, and provides a framework for identifying the different approaches that are now being employed. These are all things that are important to consider. Furthermore, it offers an emphasis on the different techniques that are now being used in the contemporary world. Each and every one of these things is important in its own right. Every single one of these things is significant in its own right, independent of the others. Every single one of them is meant to represent a distinct aspect of the whole, and this is the intention as well. [21]

Fraud Analytics: A Decade of Research – Organizing Challenges and Solutions: Papadakis et al. (2022). that is pertinent to fraudulent actions that have taken place over the course of the last ten years and are made up of data. For the purpose of doing this, the purpose of this article is to study a broad variety of data-driven strategies that are used in a number of different fraud businesses. The challenges that are linked with the quality of the data, compliance with regulatory standards, and validation of models are given a special priority in the research. This unique importance is given to the issues. The reason for this is because it is very necessary to comply with these criteria. As a result of this, the attention is specifically directed at the difficulties that are present. A clustering framework is a technique of arranging these algorithms for the purpose of their usage in practical applications within the area of fraud detection. [23] This research endeavor also involves the supply of a clustering framework, which is a method of organizing these algorithms. The structuring of these algorithms is something that may be accomplished via the use of this framework. This framework was developed with the intention of being deployed for the purpose of identifying fraudulent behaviors once it was built with the objective of achieving that goal. [22]

Developing AI-Based Fraud Detection Systems for Banking and Finance: To the best of our knowledge, Singh and his colleagues conducted this inquiry in the year 2021 when they were working together. The results of their investigation are in line with what we have gathered about the circumstance. Here is where we provide the most detailed information that we have available to us now. Regarding the framework of this article, the key topic of discussion that will be discussed is the identification of fraudulent behavior in the financial sector. The detection of fraudulent behavior is the primary focus of this article, which aims to become more particular in its approach. [24] There is a substantial amount of text in this article that is devoted to a discussion on the use of artificial intelligence in the process of discovering fraudulent behaviour. In order to enhance the precision and dependability of detection, the objective of this article is to investigate a wide range of distinct approaches that may be used to accomplish this objective. The purpose of this presentation is to provide an overview of a variety of different strategies in order to demonstrate the benefits that may be experienced via the use of machine learning. Methods that reduce the number of false positives will get a significant amount of attention from academics. However, at the same time, ensemble models and real-time fraud detection will also receive a significant amount of attention from the same set of researchers.[25]

Fraud Detection in Fintech Leveraging Machine Learning and Behavioral Analytics: paper, Khatri et al. (2020). For identifying instances of fraudulent behavior, it has been recommended that the industry of financial technology do research on the use of machine learning and behavioral analytics. This study's objective is to uncover examples of fraudulent activity in every given situation. With the goal of detecting instances of fraudulent activity and preventing new instances of fraud from happening, this would be done with the objective of finding instances of fraud. When used in highly regulated environments, the objective of this technology is to improve fraud detection measures such as accuracy, precision, and memory. The purpose of this endeavor is to identify any subtle deceptive tendencies that may be present in the given environment. For the purpose of achieving the objective of this strategy, it is vital to recognize these tendencies. [26] The objective of this attempt is to identify certain patterns of activity in order to provide a description that is more precise. This strategy has a number of objectives, one of which is to improve the metrics that

are used for the aim of identifying fraudulent activity. This approach is capable of doing a number of different tasks simultaneously. This strategy focuses a large amount of emphasis on comparing several various models to assist in the fulfillment of the target that it has set for itself via the use of this technique [27].

3. Methodology

When it comes to the topic of business analytics, the development of abilities in the identification of fraudulent behavior is something that is critically important for professionals who are working in the field. This is something that is crucially important. Not a single doubt exists about the fact that this is something that is obligatory. This is because it gives them access to the tools and procedures that are necessary for efficiently identifying fraudulent activity and putting a stop to it. This is the reason why it is so important. This is the reason why things transpire in the manner that they do. This technique, which makes an effort to offer an overview of these components and methods, is intended to provide an overview of the major components and strategies that may be applied to achieve the goal of strengthening one's capacity to recognize fraudulent conduct. This is the purpose of this method. [28] Providing an overview of the procedures is another purpose of this methodology, which aims to accomplish this. In order to carry out this task in an acceptable way, it is possible to make use of a broad variety of analytical processes and contemporary technology.[29]

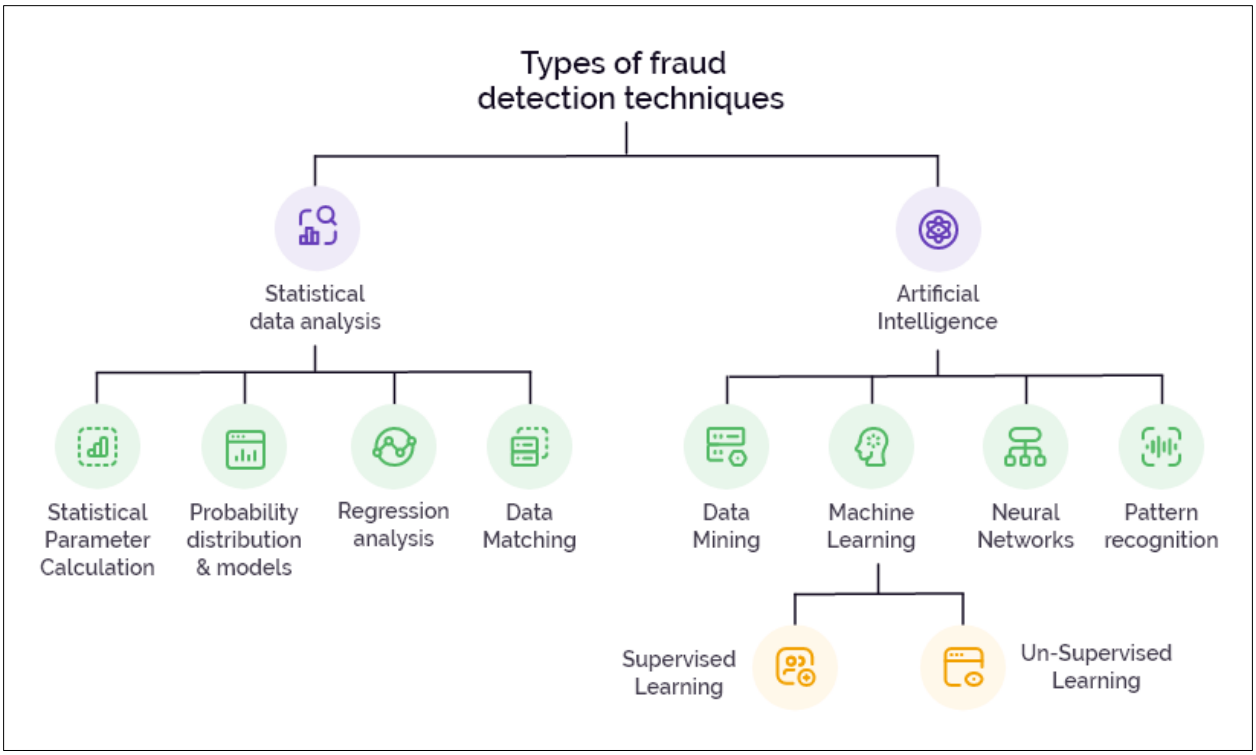

Figure 1 Fraud Detection Techniques

3.1. Data Collection

Additional types of data, such as information on transactions, client profiles, access logs, and instances of fraud that have been reported in the past, are among the various types of data that need to be gathered

These are some of the references: In order to guarantee the development of a comprehensive dataset that encompasses a wide range of fraudulent situations, it is vital to make use of both internal databases and third-party data sources, in addition to public information. [30]

3.2. Data Preparation

It is vital to clean the data in order to guarantee that it is of a high quality. This may be accomplished by removing duplicates, correcting any values that are missing, and standardizing the formats.

The process of developing new characteristics that might be useful in spotting fraudulent activity is referred to as feature engineering. This method allows for the creation of new features. The frequency of transactions and the average

value of transactions occurring over a period of time are two examples of the extra features that may be found in this category. [31]

3.3. Exploratory Data Analysis

Statistical summaries and visualizations may help you learn how the data is distributed and spot patterns or outliers that might be signs of fraud. Such analytics are referred to as descriptive analytics.

One use of pattern recognition is the detection of fraudulent transactions by identifying their distinctive traits using clustering algorithms [32]

3.4. Anomaly Detection

Utilizing statistical methods is required in order to identify transactions that are not within the regular ranges. This may be accomplished by utilizing statistical methodologies. Z-scores and percentiles are two examples of approaches that fall under this category.

In order to identify abnormalities in real time, it is possible to make use of machine learning methods such as one-class Support Vector Machines (SVMs) or Isolation Forests. This is something that can be accomplished via the employment of these methods. [33]

3.5. Predictive Modeling

During the process of picking models, applicable machine learning models (such as logistic regression and decision trees) are chosen. These models are chosen based on the features of the data as well as the specific types of fraud that are being targeted by the process. Regarding each of these aspects, consideration is given consideration. These activities are carried out in accordance with the models that were selected. [34]

To assess whether or not the model is effective by applying metrics like as accuracy, recall, and F1-score, the dataset must be partitioned into training and testing subsets by employing the training and validation technique. This will allow for the determination of whether or not the model is successful. The effectiveness of the model will be able to be evaluated after this is accomplished.[35]

3.6. Real-Time Monitoring

You have the opportunity to designate automatic notifications for transactions that have been identified as suspicious by the anomaly detection system. These notifications may be sent to you in real time. This will make it simpler for you to carry out an inquiry in a short amount of time.

For enhancing the detection capabilities that may be accomplished via the use of behavioral analytics, it is necessary to develop baselines for the normal behavior of users.

4. Result and discussion

It has been presented with a comprehensive description of the essential field of business analytics that is devoted to the identification of fraudulent activities. [24]It is the findings of the search that served as the basis for this explanation, which was then used to produce the explanation. Not only do they place an emphasis on a wide range of methods and approaches, but they also highlight the value of gaining skills that are particularly relevant to the subject matter that is being discussed.

4.1. Data Analytics

For the purpose of identifying patterns and trends that are indicative of fraudulent conduct, the process known as descriptive analytics seeks to analyze past data in order to accomplish this aim. It helps businesses understand fraudulent activities that have happened in the past and establishes criteria for regular activity. It also helps businesses create standards for regular behavior.

Based on the information that has been gathered in the past, predictive analytics is able to produce forecasts on the likelihood of fraudulent behaviors occurring in the future. These forecasts are arrived at via the use of machine learning and statistical models. The use of techniques such as neural networks, decision trees, and logistic regression is a common practice that is often employed. [27]

4.2. Business Analysis in Fraud Detection

When it comes to the development of skills associated with the identification of fraudulent activity, business analysts play a significant part in the process. The way in which they do this is by using a wide range of analytical procedures and approaches. Using methods like as data profiling and predictive modelling, they conduct comprehensive examinations of transactional data in order to accomplish their objective of effectively detecting potential fraud risks. This allows them to achieve their aim of successfully identifying probable fraud threats. This provides consumers with the opportunity to properly detect potential fraud concerns, which is in their best interest. 3. The incorporation of advanced analytics into the operations of a firm not only aids in the detection of fraudulent activity, but it also helps in the prevention of instances of such behaviors via the application of preventive measures. [29]

4.3. Challenges in Fraud Detection

The acceptance of new technologies by customers: There is a possibility that consumers may be hesitant to embrace new technologies owing to concerns over the usability and privacy associated with these technologies. There is a chance that this will occur.[30]

In order for detection systems to be able to keep up with the ever-increasing complexity of fraud schemes, it is important for them to undergo continual modification and refinement. This is due to the fact that those who perpetrate fraud are developing more sophisticated con methods.

5. Conclusion

Fraud detection is an increasingly crucial field within business analytics, driven by the development of digital transactions and complex fraudulent methods. The research that has been done on the topic highlights how important it is to acquire a comprehensive skill set in the field of fraud detection. This skill set should include a variety of analytical approaches and procedures. Among the most important results are:

Business analysts play a crucial role in the implementation of fraud detection techniques by using data profiling, predictive modelling, and machine learning algorithms. The capacity of these businesses to examine transaction data enables them to recognize trends that are suggestive of fraudulent activity and to react proactively to possible risks without delay. IN order to effectively identify fraudulent activity, it is necessary to use advanced analytical techniques. Some examples of these techniques are anomaly detection, statistical analysis, and real-time monitoring. Integration of Technology: The application of machine learning and artificial intelligence in fraud analytics has significantly improved the accuracy and efficiency of fraud detection systems. These methods enable organizations to identify unusual behaviors and transactions that deviate from established norms, which in turn makes timely intervention possible. These technologies make it possible to continuously learn from fresh data, which improves the capacity to anticipate and detect fraudulent behaviors before they take place.

Despite the progress that has been made, businesses continue to confront hurdles in the implementation process. These problems include verifying the quality of the data, integrating various data sources, and resolving privacy concerns that are associated with the handling of sensitive information. It is very necessary to triumph over these obstacles in order to ensure the effective installation of fraud detection systems.

5.1. Recommendation

Consequently, in order to successfully create skills in the field of fraud detection within the realm of business analytics, businesses and professionals have to take into consideration the recommendations that are discussed in the following paragraphs:

- Investing in training programs that are based on advanced analytics techniques, machine learning, and statistical methodologies that are particular to the detection of fraud is a significant step for education and training. These specialized methodologies are used to identify fraudulent activity. If analysts participate in possibilities for continuous education, they will be able to maintain their knowledge of developments in technology and trends that are always evolving.
- It is impossible to exaggerate the significance of fostering collaboration between data scientists, professionals working in information technology, and consultants working in business analysis. A complete understanding of both technological capabilities and business expectations is necessary in the context of fraud detection initiatives. This is the reason why it is crucial to establish such a comprehensive understanding.

- When it comes to the identification of fraudulent conduct, it is highly recommended that firms use a proactive strategy. In addition to the application of predictive analytics, these processes need to include the deployment of technology that is capable of monitoring conditions in real time. With the help of this technology, it is possible to identify any fraudulent activities at an earlier stage, which in turn makes it possible to reduce the amount of money that is lost throughout the process.
- Efforts should be made to enhance the procedures for handling data. It is of the utmost importance to construct strong data governance frameworks in order to guarantee that the procedures for data collection and management are of a high quality. Because of this, it will become less difficult to carry out trustworthy evaluations, and its efficacy in identifying fraudulent activities will increase. In addition, the effectiveness of the assessment will be enhanced.
- Employees must to be educated on the significance of fraud detection methods and the ways in which they might contribute to the identification of suspicious conduct. This information should be offered to employees. The education of users need to be the primary emphasis of this endeavor. Increasing a company's general resilience against fraudulent activities may be accomplished in a number of ways, one of which is by cultivating vigilant cultures inside the business.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abbasi, A. & Chen, H., 2008. CyberGate: A design framework and system for the textual analysis of computer-mediated communication. MIS Quarterly, 32(4), pp. 731-756.

[2] Aleskerov, E., Freisleben, B., & Rao, B. (1997). CARDWATCH: A neural network-based database mining system for the detection of credit card fraud. Proceedings of the IEEE/IAFE 1997 Computational Intelligence for Financial Engineering (CIFEr), pages 220-226.

[3] Alves, G., Silva, L.F., & Silva, R.F. (2021). Utilizing a Hybrid Machine Learning Methodology for Fraud Detection in E-Commerce Transactions. IEEE Access, Volume 9, Pages 36684-36698.

[4] Bahnsen, A.C., Aouada, D., & Ottersten, B. (2016). Cost-sensitive decision trees reliant on examples. Expert Systems with Applications, 42(19), pp. 6609-6619.

[5] Bolton, R.J. and Hand, D.J., 2002. A review of statistical fraud detection. Statistical Science, Volume 17, Issue 3, pages 235-255.

[6] Carcillo, F., Laurent, A., He-Guelton, L., Papadakis, S., & Granitzer, M. (2020). Integrating unsupervised and supervised learning for credit card fraud detection. Information Sciences, 527, pages 601-613.

[7] Caruana, R. & Niculescu-Mizil, A., 2006. A practical evaluation of supervised learning methods. Proceedings of the 23rd International Conference on Machine Learning, pages 161-168.

[8] Chen, L., Ho, T.K., Tang, Y., & Chen, X. (2019). A hybrid framework for the identification of insurance fraud using social network analysis and anomaly detection techniques. Computers & Security, volume 85, pages 273-282.

[9] Coussement, K., Lessmann, S., & Verstraeten, G. (2017). A comparative comparison of data preparation algorithms for predicting customer churn: A case study in the telecommunications sector. Decision Support Systems, vol. 95, pp. 27-36.

[10] Desai, V.S. & Joshi, S.B., 2017. A synthetic immune system used as a predictive analytics instrument for fraud detection. Expert Systems with Applications, volume 85, pages 69-79.

[11] Dong, Y. and Chen, X.W., 2005. Monitoring fraudulent trends with sophisticated data mining algorithms. International Journal of Security and Networks, Volume 1, Issues 2-3, pages 116-125.

[12] Duman, E. and Ozcelik, M.H., 2011. Identification of credit card fraud with genetic algorithms and scatter search techniques. Expert Systems with Applications, 38(10), pp. 13057-13063.

[13] Fei, T., Hong, X., Gao, W., & Wang, Y. (2018). Adaptive ensemble learning for the detection of credit card fraud with multi-objective optimization. Future Generation Computer Systems, vol. 101, pages. 706-715.

[14] Foucart, J., Gilbert, J.P., Guigourès, R., & Neiss, A. (2019). Utilization of machine learning for the identification of credit card fraud. Proceedings of the International Conference on Data Mining Workshops, pages 293-302.

[15] Francis, P., Puschmann, T., Alt, R., & Gomber, P. (2022). A framework for the effective deployment of fraud detection systems inside financial services. Journal of Business Research, 139, pages 99-110.

[16] Ghosh, S. & Reilly, D.L., 1994. Detection of credit card fraud via a neural network. Proceedings of the 27th Hawaii International Conference on System Sciences, pages 621-630.

[17] Harel, A., Segal, Y., Tishby, N., & Gal, A. (2020). Improved framework for the identification of online credit card fraud. Electronic Commerce Research and Applications, Volume 39, Page 100881.

[18] Huang, Y., Siewiorek, D.P., Koopman, P., & Sadeh, N. (2015). Forecasting credit card theft by multi-scale behavioural patterns. Proceedings of the 2015 IEEE International Conference on Data Science and Advanced Analytics (DSAA), pages 1-10.

[19] Jiang, C. & Zhai, Y., 2009. Detection of anomalies with the limited Boltzmann machine in conjunction with supervised learning. International Journal of Software Engineering and Knowledge Engineering, 19(7), pp. 891-915.

[20] Kim, M., Lee, J., & Kim, J. (2016). Utilization of a neural network methodology for the identification of fraudulent activities inside insurance datasets. Expert Systems with Applications, Volume 87, pages 18-25.

[21] Kou, Y., Lu, C.T., Sirwongwattana, S., & Huang, Y.P. (2004). Examination of fraud detection methodologies: Credit card, insurance, and telecommunications. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), Volume 29, Issue 4, Pages 549-559.

[22] Kshetri, N. (2017). Artificial Intelligence in Credit Card Fraud Detection: Techniques and Challenges in Fraud Risk Management. Journal of Internet Commerce, Volume 16, Issue 4, pages 293-306.

[23] Li, W., Teng, L., & You, M. (2021). An adaptive methodology for fraud detection in online transactions with machine learning algorithms. Pattern Recognition Letters, Volume 136, Pages 170-177.

[24] Luo, X., Liu, Z., & Jiao, H. (2014). Determinants of credit card fraud risk management. Decision Support Systems, vol. 68, pp. 96-106.

[25] Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B. (2002). Detection of credit card fraud via Bayesian methods and neural networks. Proceedings of the first International NAISO Congress on Neuro-Fuzzy Technologies, pages 261-270.

[26] McHugh, J. (2020). Financial fraud detection with machine learning. IEEE Access, 8, 181122-181132.

[27] Ngai, E.W., Hu, Y., Wong, Y.H., Chen, Y., & Sun, X. (2011). The utilization of data mining methodologies in the identification of financial fraud: A categorization framework and a scholarly literature assessment. Decision Support Systems, Volume 50, Issue 3, pages 559-569.

[28] Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A.K. (2009). Detection of credit card fraud: A hybrid methodology using Dempster–Shafer theory and Bayesian learning. Information Fusion, Volume 10, Issue 4, Pages 354-363.

[29] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). An extensive review of studies on fraud detection with data mining techniques. Artificial Intelligence Review, Volume 34, Issue 1, pages 61-100.

[30] Rajput, Q., Shafi, A., Khowaja, K.I., & Khowaja, K., 2019. Techniques for anomaly detection to avoid fraud in online transactions. Proceedings of the International Conference on Frontiers of Information Technology, pages 307-312.

[31] Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree methodology for fraud detection. Expert Systems with Applications, 40(15), pp. 5985-5993.

[32] Singh, J. and Best, P., 2016. The efficacy of fraud detection tools in charitable organizations. Accounting Research Journal, Volume 29, Issue 1, pages 13-30.

[33] Srivastava, A., Kundu, A., Sural, S., & Majumdar, A.K. (2008). Detection of credit card fraud with a hidden Markov model. IEEE Transactions on Dependable and Secure Computing, Volume 5, Issue 1, pages 37-48.

[34] Wang, Y. & Wang, S. (2019). Employing machine learning for the detection of financial fraud. International Journal of Intelligent Systems, Volume 34, Issue 1, pages 56-67.

[35] Y.S. Yeh, H.C. Wang, Y.Y. Chen, and W.Y. Liu, 2021. A framework for ensemble learning in the context of unbalanced classification for financial fraud detection. Computers & Security, Volume 105, Page 102243.