Literature Survey of Data Mining Methods in Fraud Analysis

Samuel Meads and Leon Lee

***Abstract*—Fraud poses significant financial and reputational risks across multiple industries, including banking, insurance, and e-commerce. This survey reviews the current state of data mining methods used in fraud analysis, focusing on the effectiveness of various algorithms and the scientific results from their application. The comparison highlights that advanced machine learning techniques, such as artificial neural networks (ANN), support vector machines (SVM), and random forests, generally outperform traditional statistical methods. Despite advancements, challenges such as data imbalance, evolving fraud tactics, and ethical concerns persist. This survey identifies new ideas, proposed approaches, and future research directions to enhance fraud detection systems, emphasizing the integration of hybrid models, real-time detection, and explainable AI.**

***Keywords*—Data mining, fraud detection, machine learning, artificial neural networks, support vector machines, hybrid models, real-time detection, explainable AI.**

I. Introduction

Fraud poses significant financial and reputational risks across multiple industries, including banking, insurance, and e-commerce. The complexity and sophistication of fraudulent schemes have evolved, making traditional detection methods less effective. Consequently, data mining has emerged as a powerful tool for detecting fraudulent patterns and preventing financial losses [5]. By leveraging large datasets and advanced algorithms, data mining techniques can uncover hidden patterns and anomalies indicative of fraudulent behaviour.

This survey's objective is to review the current state of data mining methods used in fraud analysis. The focus is on understanding the various algorithms employed, their effectiveness, and the scientific results obtained from their application. By comparing different approaches and identifying key themes, this survey aims to provide a comprehensive overview that can guide future research and practical applications in fraud detection.

II. Background/Motivation

The increasing prevalence of fraud in various sectors necessitates the adoption of advanced detection methods. Traditional techniques, such as manual audits and rule-based systems, often fall short in identifying sophisticated and evolving fraudulent schemes. Data mining, with its ability to process vast amounts of data and uncover intricate patterns, offers a promising solution to this challenge.

Data mining techniques encompass a range of methodologies, including supervised learning, unsupervised learning, and hybrid approaches. Supervised learning methods, such as decision trees, support vector machines (SVM), and neural networks, rely on labeled datasets to train models that can predict fraudulent activities [1]. However, the availability of labeled data is often limited, especially in the context of fraud detection, where fraudulent instances are relatively rare.

Unsupervised learning techniques, such as clustering and anomaly detection, do not require labeled data and are particularly useful for identifying novel or previously unknown fraudulent patterns. These methods group similar data points together or detect outliers that deviate from normal behavior, providing valuable insights into potential fraud.

Hybrid approaches combine the strengths of both supervised and unsupervised learning, leveraging labeled data when available and utilizing unsupervised techniques to enhance detection capabilities. For instance, a hybrid model might use clustering to identify suspicious groups of transactions and then apply supervised learning to classify these groups as fraudulent or legitimate [2].

The application of data mining in fraud detection is not without challenges. One significant issue is the imbalance in datasets, where the number of legitimate transactions far exceeds the number of fraudulent ones. This imbalance can lead to biased models that favor the majority class, reducing the effectiveness of fraud detection [8]. Additionally, the dynamic nature of fraud necessitates continuous updating and retraining of models to adapt to new tactics employed by fraudsters.

The motivation for this survey is to address these challenges by reviewing the latest advancements in data mining methods for fraud analysis. By understanding the strengths and limitations of various approaches, this survey aims to identify best practices and assist in establishing a suitable framework (application area, tools, algorithms) on which our mining project will be based.

III. Comparison of related work

The survey conducted by Bauder, Khoshgoftaar, and Seliya [1] provides a comprehensive review of healthcare upcoding fraud analysis and detection, highlighting the significance of this type of fraud within the healthcare industry. Upcoding, a method where providers claim higher reimbursement by billing for more expensive services than those performed, poses a substantial financial burden on healthcare systems. The paper emphasizes the need for robust data mining techniques to detect such fraudulent activities due to the inherent challenges in obtaining labeled audit data. To address this, the authors explore various data mining approaches, particularly focusing on unsupervised learning methods. These methods are essential for dealing with

predominantly unlabeled records to identify patterns indicative of upcoding fraud.

The paper highlights the effectiveness of supervised learning techniques such as linear regression, decision trees, and support vector machines, which require labeled data for accurate prediction and classification. However, due to the scarcity of labeled data in healthcare fraud detection, the authors advocate for the exploration of unsupervised learning techniques. Methods like k-means clustering and the Apriori algorithm are discussed for their potential in identifying fraudulent patterns without the need for labeled data. Also, hybrid learning methods, which combine supervised and unsupervised approaches, are recommended to leverage the strengths of both techniques in fraud detection.

One of the significant findings from Bauder, Khoshgoftaar, and Seliya [1] is the potential of these data mining techniques to reduce healthcare costs by enhancing the detection of upcoding fraud. The authors underscore the importance of integrating heterogeneous data sources and addressing data formatting challenges to improve the robustness of these detection methods. The survey concludes with a call for innovative research focused on upcoding fraud to develop more effective and validated detection solutions, given the limited studies currently available in this specific area of healthcare fraud.

The scientific results from the reviewed studies indicate that while supervised learning models show promise, their dependence on labeled data is a significant limitation. Unsupervised and hybrid methods, although less frequently applied, offer substantial potential for improving fraud detection without labeled data. The paper's comprehensive review of existing techniques and their applicability to healthcare fraud detection provides a valuable resource for further research and development in this field.

The work by Sánchez-Aguayo, Urquiza-Aguiar, and Estrada-Jiménez [2] explores predictive fraud analysis by applying the Fraud Triangle Theory (FTT) through data mining techniques. This study addresses the gap in incorporating human behavior analysis into fraud detection, proposing a mechanism that combines a predefined topic model and a supervised classifier to detect potential fraud-related text. The research leverages synthetic data due to the scarcity of public datasets embedding fraudulent activities. The generated dataset includes 14,000 records balanced between fraud and non-fraud classes.

The authors benchmarked various topic modeling techniques—Latent Dirichlet Allocation (LDA), Non-Negative Matrix Factorization (NMF), and Latent Semantic Analysis (LSA)—and found that LDA provided the most consistent results. For classification, they employed several machine learning algorithms, including logistic regression, random forest, gradient boosting, Gaussian naive Bayes, decision trees, k-nearest neighbor, and support vector machines, alongside deep learning techniques such as convolutional neural networks (CNN), dense neural networks (DNN), and long short-term memory (LSTM).

TABLE I. AUC PERFORMANCE OF MACHINE LEARNING MODELS ON FRAUD CLASSIFICATION [2]

Classification Method's	Predictive Accuracy				Mean
	T1	T2	T3	T4	
Logistic Regression: AUC	0.83	0.64	0.68	0.65	0.70
Random Forest: AUC	0.88	0.77	0.80	0.79	**0.81**
GNB: AUC	0.86	0.70	0.74	0.73	0.76
Gradient Boosting: AUC	0.89	0.77	0.79	0.79	**0.81**
k-NN: AUC	0.86	0.72	0.76	0.74	0.77
Decision Tree: AUC	0.80	0.71	0.73	0.75	0.74
SVM: AUC	0.86	0.70	0.75	0.74	0.76

The results indicated that random forest and gradient boosting achieved the best performance, with an average Area Under the Curve (AUC) higher than 0.8, demonstrating the feasibility of integrating FTT with topic modeling and machine learning for predictive fraud analysis. As shown in Table 1, random forest and gradient boosting both achieved a mean AUC of 0.81, outperforming other models such as logistic regression and decision trees. This study contributes significantly by highlighting the importance of human behavior in fraud detection and proposing an effective, multidisciplinary approach to enhancing fraud detection systems.

The study by Mohammadi, Yazdani, Khanmohammadi, and Maham [3] focuses on the detection of financial reporting fraud using various data mining algorithms. The research evaluates the performance of five popular classification algorithms: artificial neural networks (ANN), Bayesian networks, discriminant analysis, logistic regression, and support vector machines (SVM). The study utilizes a dataset of companies with both fraudulent and non-fraudulent financial statements between 2011 and 2016.

TABLE II. DETECTION ACCURACY OF CLASSIFICATION MODELS [3]

Model	FFS (%)	Non-FFS (%)	Overall accuracy (%)
Bayesian Network	69.7	63	65.8
Discriminant Analysis	67	58	62
Logistic Regression	69.1	66.1	67.9
Artificial neural network	69.8	80.2	75
Support Vector Machine	67.5	66.7	67

The results as shown in Table 2, highlight the superior performance of ANN, which achieved the highest detection accuracy with 69.8% for fraudulent financial statements and an overall accuracy of 75%. Logistic regression and SVM also performed well, with overall accuracies of 67.9% and 67%, respectively. Bayesian networks and discriminant analysis showed lower performance with overall accuracies of 65.8% and 62%, respectively. The study identifies nine consistent

predictors used by different classification algorithms: employee productivity, accounts receivable to sales, debt-to-equity ratio, inventory to sales ratio, sales to total assets, return on equity, return on sales, liabilities to interest expenses, and assets to liabilities.

The scientific results from this study indicate that ANN is particularly effective for financial fraud detection, outperforming other algorithms in both accuracy and error rates. The findings suggest that integrating these data mining techniques into fraud detection systems can significantly enhance the identification of fraudulent activities, thereby improving the robustness and reliability of financial reporting [3].

The comprehensive survey by Phua, Lee, Smith, and Gayler [4], compares, and summarizes a wide array of published articles on automated fraud detection over the past decade. This survey is distinctive in its breadth, covering more technical articles than any other review in the field and suggesting alternative data sources and solutions from related domains. The paper defines various types of fraud and presents the nature of data evidence collected within affected industries. It emphasizes that fraud detection is essential in many sectors, including credit card, insurance, telecommunications, and e-commerce.

The study categorizes data mining techniques into supervised, unsupervised, and hybrid approaches. Supervised techniques such as neural networks, decision trees, and support vector machines (SVMs) are widely used due to their ability to leverage labelled data for training. However, the scarcity of labelled data often limits their effectiveness. Unsupervised techniques, including clustering and anomaly detection, are crucial for identifying fraud patterns in unlabelled data. Hybrid approaches combine supervised and unsupervised methods to enhance detection accuracy and robustness.

A significant contribution of this survey is its discussion of performance measures, emphasizing that traditional accuracy metrics are insufficient for fraud detection. Instead, metrics such as Area Under the Curve (AUC), cross-entropy, and Brier score are more appropriate. The paper also highlights the importance of domain-specific criteria and the integration of domain expertise in evaluating fraud detection systems.

The survey concludes by identifying the limitations of current methods and suggesting that future research could benefit from techniques used in related fields such as intrusion detection, spam detection, and anti-terrorism. The authors argue that incorporating these interdisciplinary approaches can enhance the effectiveness of fraud detection systems and provide a more comprehensive understanding of adversarial behaviour [4].

The study by Albashrawi [5] presents a decade review from 2004 to 2015 on the use of data mining techniques in detecting financial fraud. The review categorizes various data mining methods employed in different financial fraud applications, such as health insurance and credit card fraud.

TABLE III. USAGE FREQUENCY OF DATA MINING TECHNIQUES 2004-2015 [5]

Method [a]	Frequency
Logistic Regression	17
Neural Network	15
Decision Trees	15
Support Vector Machine	12
Naïve Bayes	8
Bayesian Networks	7
Discriminant Analysis	6
Nearest Neighbour	4
K-means clustering	4
Self-organising map	4
Random Forests	3
Genetic Algorithm	3
Probit model	3
Association Rules	2
Process mining	2
Fuzzy Logic	2

[a] Table only showing methods with frequency of ≥2

Out of the 65 articles reviewed, 41 data mining techniques were observed with logistic regression emerging as the most frequently used technique, accounting for 13% of the applications. Neural networks and decision trees followed, each representing 11% of the usage. The study emphasizes that supervised learning techniques have been predominantly used over unsupervised ones, highlighting their effectiveness in fraud detection.

Albashrawi's review reveals that financial statement fraud and bank fraud are the most studied areas, with 63% of the articles focusing on these types. The review provides a detailed analysis of the data mining techniques' performance, indicating that logistic regression, neural networks, and decision trees are among the top-performing methods. Furthermore, the study suggests that integrating these techniques into fraud detection systems can significantly improve accuracy and efficiency.

One of the key contributions of this paper is the high-level and detailed classification frameworks it offers, which can guide researchers and practitioners in selecting appropriate data mining techniques based on specific fraud contexts. The review also highlights the geographical distribution of the studies, with the United States, Taiwan, China's mainland, and Spain being the most represented regions in the research.

Overall, Albashrawi's comprehensive review underscores the critical role of data mining in financial fraud detection and provides valuable insights into the most effective techniques and their applications across different fraud types [5].

The study by Al-Hashedi and Magalingam [6] provides a comprehensive review of financial fraud detection using data mining techniques from 2009 to 2019. This review categorizes 75 relevant articles into four main groups: bank fraud, insurance fraud, financial statement fraud, and cryptocurrency fraud.

TABLE IV. USAGE FREQUENCY OF DATA MINING TECHNIQUES 2009-2019 [6]

Method [a]	Frequency
SVM	17
Neural Network	10
Naïve Bayes	11
Random Forest	11
Logistic Regression	9
K-Nearest Neighbour	8
Outliers Detection	7
Decision Tree	6
Bayesian Network	6
Hidden Markov Model	6
Genetic algorithm	5
Gradient Boosting Tree	4
Multilayer Perception	4
Autoencoder	3
Local Outlier Factor	3

[a] Table only showing methods with frequency of ≥3

The study reveals that 34 different data mining techniques have been applied across these financial fraud types, with Support Vector Machine (SVM) being the most frequently used, accounting for 23% of the studies, followed by Naïve Bayes and Random Forest, each contributing 15%.

The review highlights that most research has focused on bank and insurance fraud, comprising 81.33% of the total studies. The authors analyse the strengths and weaknesses of various data mining techniques, emphasizing that SVM and Random Forest are particularly effective due to their high accuracy in detecting fraudulent activities. The review also discusses the geographical distribution of studies, noting that the United States, Taiwan, mainland China, and Spain are the most represented regions in financial fraud research.

Al-Hashedi and Magalingam's study underscores the importance of integrating multiple data mining techniques to enhance fraud detection systems. The review suggests that future research should explore hybrid models that combine the strengths of various algorithms to address the limitations of individual techniques. The paper concludes by providing a roadmap for researchers and practitioners to select appropriate data mining methods for specific types of financial fraud, thereby improving the robustness and reliability of fraud detection systems [6].

The comprehensive review by Gupta and Mehta [7] explores data mining-based financial statement fraud detection methods through a systematic literature review (SLR) and meta-analysis. The study focuses on evaluating the effectiveness of various data mining classification techniques in detecting symptoms of financial statement frauds by comparing fraudulent and non-fraudulent companies. The authors reviewed articles published between 1995 and 2020, analysing different data mining techniques, including statistical methods and machine learning approaches, for their classification accuracy.

The study reveals that machine learning techniques, particularly artificial neural networks (ANN), support vector machines (SVM), and decision trees, generally outperform statistical methods such as logistic regression and discriminant analysis in terms of classification accuracy. The meta-analysis indicates that machine learning approaches can achieve high accuracy even with a 1:1 mapping ratio of fraudulent to non-fraudulent companies. For instance, a classification accuracy of 98.09% was achieved using probabilistic neural networks (PNN) with a 1:1 mapping ratio, whereas traditional statistical methods required larger datasets to attain similar results.

Gupta and Mehta's review also highlights the challenges in collecting and mapping fraudulent company data against non-fraudulent data, emphasizing the importance of sample size and data mapping ratio on the overall accuracy of classification methods. The study suggests that smaller sample sizes with a 1:1 mapping ratio can increase the efficacy of fraud detection models and reduce implementation costs. This comprehensive review provides valuable insights into the relative performance of various data mining techniques and offers a detailed classification framework to guide future research and practical applications in financial fraud detection [7].

The reviewed studies on data mining methods in fraud analysis highlight the effectiveness of various techniques in different fraud contexts, emphasizing the importance of integrating multiple approaches to enhance detection accuracy. Key findings suggest that machine learning techniques, particularly artificial neural networks (ANN), support vector machines (SVM), and random forests, generally outperform traditional statistical methods like logistic regression and discriminant analysis. Studies stress the significance of addressing data challenges, such as obtaining labelled data and optimizing data sample mapping ratios, to improve model robustness and reduce implementation costs. Additionally, interdisciplinary approaches and the incorporation of human behaviour analysis are recommended to further refine fraud detection systems. Overall, these reviews underscore the critical role of advanced data mining techniques in detecting diverse types of fraud across various industries, providing a comprehensive framework for future research and practical applications in fraud detection.

IV. OUR OPINION

In reviewing the extensive research on data mining methods for fraud detection, several key areas for further development and improvement have emerged. Our opinion centers on enhancing the robustness and effectiveness of fraud detection systems by leveraging innovative ideas and integrating advanced data mining and machine learning techniques.

A. New Ideas

Firstly, combining unsupervised and supervised learning methods in a hybrid approach appears promising, particularly in contexts with limited labeled data. This can be achieved through the integration of advanced anomaly detection techniques with supervised classifiers, allowing for the identification of potential fraud cases that can then be validated and used to train more accurate models.

Another idea is exploring the use of transfer learning, where models trained on one type of fraud detection can be adapted

to another, leveraging the common patterns across different fraud types. This approach can significantly reduce the time and data required to develop effective models for new fraud detection tasks. By reusing and fine-tuning pre-trained models, we can achieve higher efficiency and accuracy in identifying fraudulent activities in various domains, such as financial transactions, insurance claims, and e-commerce activities.

Moreover, integrating advanced data mining techniques such as feature engineering and selection can improve the performance of fraud detection models. By identifying and using the most relevant features, models can better capture the underlying patterns of fraudulent behavior, leading to higher detection accuracy.

B. Proposed Approaches / Models

One proposed model involves the use of ensemble learning methods that combine the strengths of various algorithms such as random forests, gradient boosting, and neural networks. This approach can mitigate the limitations of individual models and provide a more robust solution for fraud detection. Ensemble methods can aggregate predictions from multiple models, reducing the likelihood of false positives and improving overall detection accuracy.

Additionally, incorporating deep learning techniques, such as convolutional neural networks (CNN) and recurrent neural networks (RNN), can enhance the ability to detect complex patterns in large datasets, particularly in financial and healthcare fraud scenarios. CNNs can be utilized to identify spatial patterns and relationships in transaction data, while RNNs can capture temporal dependencies and sequence patterns, making them ideal for analyzing time-series data, such as transaction histories.

Furthermore, the development of graph-based models can provide a powerful tool for fraud detection, especially in scenarios involving networks of interactions, such as social networks and communication networks. Graph neural networks (GNNs) can effectively capture the relationships and dependencies between entities, identifying suspicious clusters of activity and anomalous connections that may indicate fraud.

Another innovative approach involves the integration of reinforcement learning techniques in fraud detection systems. Reinforcement learning models can be trained to make sequential decisions based on the feedback from previous actions, enabling them to adapt to changing fraud patterns and optimize detection strategies over time.

C. How to Extend Existing Work

Extending the existing work could involve integrating domain expertise into the model development process to improve the interpretability and accuracy of fraud detection systems. This can be achieved using explainable AI techniques that provide insights into how models make decisions, allowing domain experts to validate and refine the models' outputs. Explainable AI can help uncover the underlying reasons behind a model's predictions, facilitating trust and transparency in automated fraud detection systems.

Another area for extension is the application of real-time data mining techniques to detect fraud as it occurs. This involves developing models capable of processing streaming data and making immediate predictions, which is particularly useful in detecting transactional fraud in financial systems and e-commerce. Implementing real-time fraud detection systems can significantly reduce the time between the occurrence of fraudulent activities and their detection, minimizing potential losses and enhancing the overall security of financial transactions.

Additionally, research can be extended by incorporating advanced natural language processing (NLP) techniques to analyze unstructured text data, such as emails, chat logs, and social media posts, for signs of fraudulent intent. NLP can help detect deceptive language patterns, social engineering tactics, and other fraudulent communication methods, providing a more comprehensive approach to fraud detection.

Furthermore, developing collaborative fraud detection frameworks that allow organizations to share anonymized fraud data and detection models can enhance the collective ability to identify and mitigate fraud. Such frameworks can leverage federated learning techniques, enabling models to be trained on distributed data without compromising data privacy and security.

Future research should also focus on the ethical implications and privacy concerns associated with fraud detection using machine learning. Developing frameworks that ensure data privacy and adhere to ethical standards will be crucial in gaining public trust and ensuring the widespread adoption of these advanced techniques. Addressing issues such as bias in model predictions, data security, and the potential for misuse of fraud detection technologies will be essential for creating responsible and sustainable fraud detection solutions.

By addressing these areas, the field of fraud detection can be significantly advanced, leading to more accurate, efficient, and ethical solutions for identifying and mitigating fraudulent activities across various industries. The integration of cutting-edge technologies, innovative methodologies, and interdisciplinary approaches will pave the way for the next generation of fraud detection systems, ensuring a safer and more secure digital environment.

V. CONCLUSION

This survey reviewed the current state of data mining methods used in fraud analysis, highlighting the effectiveness of various algorithms and their application results. Our comparison of related work demonstrates that advanced machine learning techniques, particularly artificial neural networks (ANN), support vector machines (SVM), and random forests, generally outperform traditional methods like logistic regression and discriminant analysis. Hybrid models

combining supervised and unsupervised learning also show promise, especially in handling limited labeled data.

A. Future Issues

Despite these advancements, challenges such as data imbalance, evolving fraud tactics, and ethical considerations persist. Future research should address these issues by developing adaptive learning algorithms and reinforcement learning techniques to respond to changing fraud patterns. Advanced resampling methods and synthetic data generation can help mitigate data imbalance, while real-time detection systems need optimization for immediate fraud identification.

Integrating domain expertise through explainable AI can enhance model accuracy and transparency, ensuring decisions are more interpretable and trusted. Additionally, ethical and privacy standards must be prioritized to gain public trust and ensure responsible use of detection technologies. Interdisciplinary approaches from related fields can also offer valuable insights and methodologies for improving fraud detection systems.

By focusing on these areas, the field of fraud detection can advance significantly, leading to more accurate, efficient, and ethical solutions for identifying and mitigating fraudulent activities across various industries.

REFERENCES

[1] Bauder, R., Khoshgoftaar, T.M. & Seliya, N. “A survey on the state of healthcare upcoding fraud analysis and detection.” Health Serv Outcomes Res Method 17, 31–55 2017.

[2] M. Sánchez-Aguayo, L. Urquiza-Aguiar, and J. Estrada-Jiménez, “Predictive fraud analysis applying the fraud triangle theory through data mining techniques,” Applied Sciences, vol. 12, pp. 3382, March 2022.

[3] M. Mohammadi, S. Yazdani, M. Khanmohammadi, and K. Maham, “Financial Reporting Fraud Detection: An Analysis of Data Mining Algorithms,” International Journal of Finance and Managerial Accounting, vol. 4, no. 16, pp. 1–12, Winter 2020.

[4] C. Phua, V. Lee, K. Smith, and R. Gayler, “A Comprehensive Survey of Data Mining-based Fraud Detection Research,” Monash University, Baycorp Advantage, 2009.

[5] M. Albashrawi, “Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015,” *Journal of Data Science*, vol. 14, no. 3, pp. 553-570, July 2016.

[6] K. G. Al-Hashedi and P. Magalingam, “Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019,” *Computer Science Review*, vol. 40, pp. 100402, April 2021.

[7] S. Gupta and S. K. Mehta, “Data Mining-based Financial Statement Fraud Detection: Systematic Literature Review and Meta-analysis to Estimate Data Sample Mapping of Fraudulent Companies Against Non-fraudulent Companies,” *Global Business Review*, vol. 22, no. 3, pp. 1-24, Jan. 2021.

[8] H. Du, L. Lv, H. Wang, and A. Guo, "A novel method for detecting credit card fraud problems," PLoS ONE, vol. 19, no. 3, pp. 1-26, Mar. 2024.