Published online on the journal's website:
http:// https://journal.isas.or.id/index.php/JAA

JOURNAL OF APPLIED ACCOUNTING (JAA)

Vol. 4 No. 2 (2025) 07 - 12 **ISSN Online: 2830-0149** Page: 152-157

Data Driven Approach for Detecting Financial Statement Fraud; A Systematic Literature Review

Fitriyeni Oktavia[1], **Rossy Endah Permatasari**[2]
[1,2]Department of Vocational, Economic and Business Faculty, Universitas Andalas
[1]fitriyeni@eb.unand.acid*, [2]rossyendah@eb.unand.ac.id

Abstract

Financial statement fraud represents a persistent and complex threat to organizational integrity, requiring more advanced analytical tools to detect subtle accounting manipulations. To provide an evidence-based understanding of how data-driven techniques have been utilized in this domain, this study conducts a Systematic Literature Review (SLR) guided by the PRISMA framework. The review addresses two research questions: (a) what data-driven approaches have been used to detect financial statement fraud, and (b) what are the characteristics of the data, modelling methods, and evaluation metrics employed in prior studies. A structured search and screening process was executed using predefined inclusion and exclusion criteria, enabling the selection of relevant peer-reviewed studies from multiple academic databases. The included articles were further examined using meta-analysis techniques to synthesize quantitative evidence where applicable. The findings reveal that financial statement fraud detection has increasingly shifted toward machine learning, deep learning, graph-based analytics, and other advanced data-driven models capable of identifying hidden or non-linear patterns in financial reporting data. The reviewed studies employ diverse data characteristics, including financial ratios, earnings indicators, transactional records, and graph-structured relationships. Overall, this review highlights both the advancements and the methodological challenges within the field, underscoring the need for improved data quality, consistent evaluation practices, and models that balance predictive performance with interpretability for auditing applications.

Keyword: *Fraud, data-driven, machine learning, anomaly detection, deep learning.*

Received by the Editorial Team: 07-12-2025 | Revised Completed: 28-12-2025 | Published Online: 28-12-2025

INTRODUCTION

Financial statement plays a crucial role in financial and business world. The needs of transparency become instrumental in realizing good governance, thereby fostering public trust and ensuring accountability in the use of public resources (1). On the contrary, if the financial statement is not transparently published, inaccuracy and the covert fraud that occurs within it will cause severe consequence not only for customer but also for the broader economy and public trust.

Nowadays, the evolvement of Internet of Thing play a significant role in economic complexity across countries. It finds a positive long-term relationship between digital business activities and economic complexity, suggesting that digitalization contribution to more intricate economic structures (2). In line with the aforementioned statement, multifaceted nature of digital initiatives and their impact on business complexity. It underscores the need for organization to understand various dimensions of digital transformation to manage complexity effectively (3). Thus, digital transformation creates the increasing of availability and complex data.

The increasing of availability of data and technologies like machine learning in providing a financial statement presents opportunities and challenges for auditors to detect a fraud. Machine learning and Artificial Intelligence enhances the improvement of data processing and error reduction but also pose challenges such as cybersecurity threats and the need for continuous employee training (4).

The threat of financial fraud gives significant impact to public and economics. Research by (5) shows that financial fraud has lost investors over $500 billion in years. Worldwide profile cases like Enron cause a $70 Billion loss in market capitalization, illustrating the great financial damage and erosion of public trust(5).

In Indonesia, financial statement fraud has continued to occur persistently over the years. Then it raises people's question about the effectiveness of auditors in detecting such fraud. This covert nature is exacerbated by systemic weakness in oversight and internal controls. The secretive characteristic of financial statement fraud contributes to its consistent occurrence in Indonesia.

https://doi.org/10.52158/jaa.v4i2.1472

Fraudulent activities are often conducted covertly, making detection challenging, perpetrators may use complex schemes and manipulate accounting records to hide their actions from auditors and regulators (5). These characteristic underscores the complexity of financial statement fraud and the importance of robust internal controls, ethical corporate culture, and vigilant oversight to mitigate the risk of such fraudulent activities and need a proper method to detect.

As a consequence of these constraints, the use of data-driven approaches for detecting financial statement fraud has gained significant attention. Unlike conventional audit methods, these method enables the examination of entire datasets rather than samples, making it possible to detect anomalies that might be unpredicted(6). Detecting financial statement fraud with data-driven approaches provides advances analytics and machine learning techniques.

Key categories of data-driven approaches used in financial statement fraud (FSF) detection include statistical models, supervised machine learning methods, unsupervised anomaly-detection techniques, and ensemble learning. Supervised learning models such as logistic regression, support vector machines (SVM), and neural networks are trained on labeled instances of fraud and non-fraud to learn discriminative patterns (7). Ensemble methods—particularly Random Forests, gradient-boosted trees, and deep-learning ensembles—combine multiple base learners to enhance predictive stability and generalizability.

Evidence in the literature, however, is not always consistent. Perols (2011), for example, finds that relatively simple models like logistic regression and SVM can outperform more complex data-mining algorithms when appropriate predictors are selected and evaluation conditions are carefully controlled (8). Other reviews highlight extensive use of decision trees, neural networks, SVM, and Bayesian models in financial fraud research across various settings.

As firms increasingly adopt digital and automated accounting systems, the volume, velocity, and variety of financial data have outpaced the capability of traditional audit procedures and fraud-detection mechanisms. Consequently, data-driven approaches such as machine learning, deep learning, and anomaly-detection algorithms have gained prominence as tools to support auditors and regulators (9).

Despite substantial progress, several critical gaps remain. Much existing research focuses on general fraud detection or specific industry settings, limiting its applicability to FSF contexts. Furthermore, there is a lack of cross-disciplinary synthesis that integrates accounting and auditing perspectives with advances in computer science and data analytics. The literature is also fragmented across diverse modelling techniques, heterogeneous datasets, and inconsistent evaluation metrics, making the empirical evidence difficult to compare and limiting practical adoption.

To address these issues, this study systematically maps the data-driven approaches used in FSF detection and characterizes the data types, modelling methods, and evaluation metrics employed in prior research. Through a systematic literature review and meta-analysis, this study consolidates dispersed findings, enables meaningful cross-method comparison, and proposes standardized evaluation practices for future academic research and audit applications.
This study addresses two research questions:
a. What data-driven approaches have been used to detect financial statement fraud?
b. What are the characteristics of the data, modelling methods, and evaluation metrics employed in prior studies?

RESEARCH METHODOLOGY

This study adopts the systematic literature review to explore and synthesize existing research on data driven approaches, particularly Machine Learning (ML) and Deep Learning (DL) for detecting financial statement fraud. The Protocol follows PRISMA 2020 guidelines to ensure transparency and replicability and is further supported by the Kitcheman (10) methodology which is designed for systemic reviews. The review also uses a meta-sythesis approach to extract conceptual insight and integrative finding from selected studies.

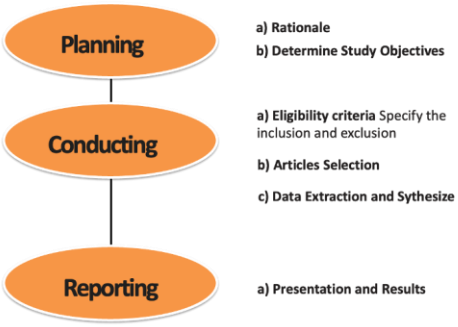
Planning
a) Rationale
b) Determine Study Objectives
Conducting
a) Eligibility criteria Specify the inclusion and exclusion
b) Articles Selection
c) Data Extraction and Sythesize
Reporting
a) Presentation and Results

Image 1. The Research Design

Inclusion Criteria

To Ensure the quality and relevance of the studies included in this review a set of inclusion criteria was developed: a) Topic Relevance: Studies must explicitly address: financial statement fraud detecting using machine learning and/or deep learning techniques; b) Type of publication: Only articles published in peer-reviews journals or presented at reputable conferences will be considered; c) Publication year: the review will include studies published between period 2010-2025. This 15-year period is justified by the following reasons: significant advancement in machine learning and deep learning technologies began to accelerate around 2010, leading to their growing application in financial fraud detection. It also offers a comprehensive longitudinal perspective, ensures inclusion of the most up-to-date methodologies and findings, especially relevant in the ear of digital transformation and big data; e) Only articles written in English will be reviewe to maintain consistency and comprehensibility; f) Methodological focus: Only review or employe data driven techniques within the context of financial statement fraud detection.

Exclusion Criteria

To refine the focus of the study, reviews will be excluded if they are: a) Do not involve in financial statement fraud; b) Use non data driven or purely theoretical approaches; c) Are not accessible in full text article; d) Are duplicates or overlapping publications.

Data Sources and Search Strategy

A comprehensive search will be conducted across major academic database such as scopus, ScienceDirect, Springelink, wiley online using combination of keywords including:

a. Financial statement fraud
b. Machine Learning
c. Deep Learning
d. Fraud Detection
e. Data Mining
f. Neural Networks
g. Financial Anomalies

Data Extraction and Synthesis

The extracted data will be analyzed using meta-sythesis allowing for a structured comparison and the emergence of conceptual themes. The goal is to develop an integrative understanding of which ML DL techniques have proven most effective in what context and what conditions.

Selected articles will undergo a systematic data extraction process, capturing:

a. Authors, Year and Country
b. Methodology
c. Dataset Characteristic
d. Key Findings
e. Strength and limitation of the approach

This research is purposed to build a holistic model for fraud detection by combining different approaches. This study will synthesize existing research, using classification models, and leveraging data visualization tools. By merge findings from multiple studies, we'll attain in-depth knowledge of prevailing financial statement fraud detection methods. The Taksonomi Model will help us break down fraud detection into three key area that are consists of data types, algorithms, and evaluation. This will ensure us to take a structured approach to choosing the right techniques for different fraud schemes. We will also use a Fraud Detection Matrix to map how different approaches perform among different data types and types of fraud, giving us a clear picture of which approaches work best in each case.

RESULTS AND DISCUSSION

We perform Systematic Literature Review (SLR) based on PRISMA guidelines 2020 for SLR. We perform selection process by using inclusion and exclusions related to the topic of research.

The inclusions are: 1) Publication Type: Peer-reviewed journal articles; 2) Publication Period: 2015–2024; 3) Language: English; 4) Studies explicitly focusing on financial statement fraud detection (FSFD) or corporate accounting fraud; 5) Methodological Approach:) Empirical study, or 7) model-based studies using machine learning (ML), deep learning (DL), or hybrid techniques.

The exclusions are: 1) Non-journal documents: conference papers, dissertations, book chapters, or reviews; 2) Non-data-driven approaches: purely theoretical or conceptual frameworks without empirical or computational implementation; 3) Incomplete or inaccessible full text; 4) Limited methodological transparency.

Selection Process

We perform selection process of studies from selected sources, Emerald, Sciencedirect and springerlink as follows:

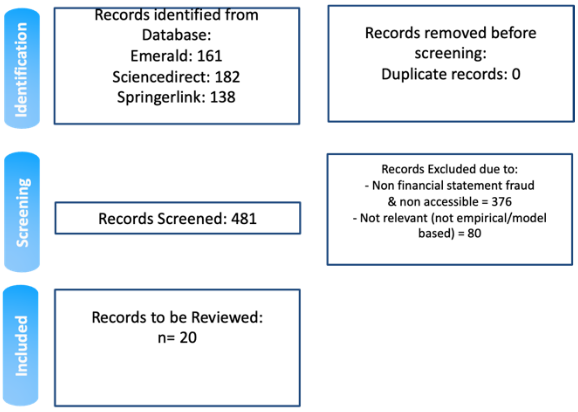

Image 2. Data Selection Process

We build data extraction based on the purpose of this research and to be able answer the research question, so we decide to collect and extract from each of studies: the algorithm, dataset, features, accuracy and challenge. Algorithm is like a machine to drive a detection the object that we called as dataset. Dataset has various type, like text, number and graph. Different dataset will needs different algorithm to read and processed. However, to answer the research question we perform data synthesize. The process are explained by the image 2.

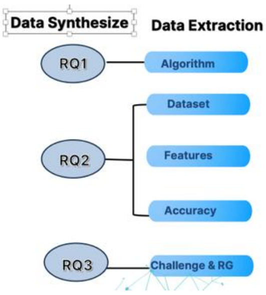

Image 3. Data Sythesice & Extraction Process

General Overview

Based on data extraction and data synthesize process, we found that there are 13 algorithms used in fraud detection in financial statement. The most used algorithm are Super Vector Machine (SVM), General Neural Network (GNN) and Random forest. Each of them have different function for different dataset of detection.

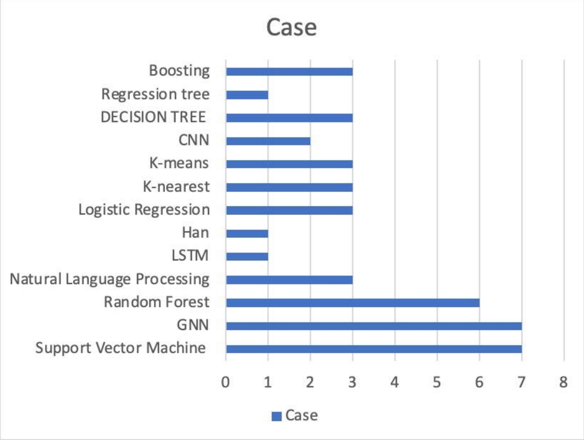

Image 3. Types of Algorithms used

SVM has a function to Separates fraudulent and non-fraudulent cases through optimal hyperplane classification. identify the numeric anomaly or unusual pattern. They can identify abnormal revenue recognition patterns compared to similar companies.

This result in line with previous research by Putri (2024), among 30 peer-reviewed articles (2014-2024), supervised learning algorithms were predominant, especially: Support Vector Machine (SVM), Logistic Regression (LR), and XGBoost (11).

GNN able to Learns relational structures among entities such as firms, directors, and transactions (12). They also analyze hidden relation that could be a pattern of fraud. The study demonstrates that the GNN-model achieves superior performance, attaining improved recall and simultaneously maintaining low false positive levels (13).

Random Forest Ensemble of decision trees that enhances prediction stability and reduces overfitting. They group based on probability of fraud with recognizing multi factor analysis.

Random forest outperformed several parametric models; conclude RF significantly improves detection efficiency (14). Random Forest improves generalization by averaging predictions from many weak decision-tree learners trained on slightly different datasets (15).

The Super dominance of SVM, GNN, and Random Forest indicates that current research models that combine high predictive power, interpretability, and adapt emphasizes ability to structured financial data. Meanwhile, LSTM, HAN, and CNN—though less frequent—represent the next frontier, focusing on sequential, textual, and multimodal fraud indicators that mirror real-world complexity (3). LSTM (Long Short-Term Memory), s a special kind of recurrent neural network (RNN) designed to overcome the vanishing-gradient problem, by using special "memory cells" and gates (input, forget, output) to remember or forget information over long sequences.

Answer to Research Question 2: What are the characteristics of the data and evaluation metrics?

From 20 studies, the features of dataset used to detect financial statement fraud can be grouped into several main categories, in attachment 1.

Type of data-driven approaches used to detect Financial Fraud

Various data-driven approaches have been used to detect financial statement fraud. Smith et al. (2020) used machine learning methods such as Random Forest and Support Vector Machine on a dataset of 200 companies, with key features being financial ratios like ROA and Debt Ratio, achieving up to 92% accuracy despite a relatively limited dataset. The study by (2022), utilized annual reports and MD&A text, as well as financial indicators from 208 companies with a fraud: non-fraud ratio of 1:250. A Hierarchical Attention Network (HAN) method was used to capture linguistic and financial features, resulting in a baseline accuracy of 82.81%, with HAN performing better, although the F1-score was not specifically reported. Meanwhile, Lokanana and Sharma (2025) used the SEC AAERs dataset from 1982–2022, with 4,278 cases, processed using various machine learning algorithms such as Logistic Regression, Random Forest, Gradient Boosting, and CatBoost.

Xinyi Zheng et al. (16) developed a K-Means–based data-mining approach to identify accounting fraud in corporate annual reports. Their study integrates unsupervised clustering with smart-city information technology and applies it to 641 annual reports from 146 companies listed on the Shanghai and Shenzhen Stock Exchanges between 2012 and 2021

In a broader review of the literature, Waleed Hilal et al. (17) surveyed a wide range of data-driven techniques used for financial fraud detection across various studies. The reviewed methods include classical machine-learning techniques such as Decision Trees, Support Vector Machines, Logistic Regression, K-Means clustering, K-Nearest Neighbors, and ensemble methods like Random Forests, as well as more advanced deep-learning models including CNNs, LSTMs, Autoencoders, and GANs.

Meanwhile, Junjie Qian and Guoxiang Tong (18) proposed a metapath-guided Graph Neural Network (Metapath-GNN) specifically designed for fraud detection in complex financial transaction networks. Their work uses graph-structured datasets such as Elliptic and T-Finance—where nodes represent participants, accounts, users, or products, and edges represent relationships or financial transactions. Each node and edge is associated with attributes such as transaction amount, type, and frequency, and metapath sequences capture meaningful patterns of interactions across the network.

Finally, Huy Tran Tien et al. (19) reviewed the integration of blockchain technology with data-mining techniques for financial anomaly detection. Their study highlights how immutable blockchain ledger data—such as cryptocurrency transactions, smart-contract execution records, or blockchain-linked financial statements—can be combined with machine-learning methods to enhance accuracy and enable earlier detection of financial irregularities.

Shahana et al. (20)examined statistical and machine-learning approaches used across historical fraud cases, including firms such as Enron, Satyam, and WorldCom, as well as non-fraudulent control firms. The reviewed studies utilized data-driven approaches ranging from traditional statistical models to modern machine-learning techniques. While Lu et al.(12) introduced a contrastive multimodal dialogue network (CMMD) designed to detect financial statement fraud using conference call transcripts, audio recordings, and firm-level financial ratios. Motie and Raahemi (21) conducted a systematic review of 33 studies involving Graph Neural Networks (GNNs) for financial fraud detection.

Characteristics of the data, modelling methods, and evaluation metrics employed in prior studies?

The features used included financial ratios, binary/categorical indicators, and feature selection and PCA techniques to strengthen predictions. As a result, Logistic Regression achieved 84% accuracy, while the combined model and predictive modeling (Gradient Boosting/CatBoost) achieved >88–90%. In general, the data characteristics in these studies include a combination of financial and text data, modeling methods using machine learning or deep learning capable of handling class imbalance, and evaluation using accuracy and F1-score. The main challenges include dataset limitations and the adaptive complexity of fraudsters' behavior.

CONCLUSION

This systematic literature review, conducted in accordance with the PRISMA framework and supported by meta-analysis, provides an integrated understanding of how data-driven approaches have been applied in detecting financial statement fraud. The evidence synthesized from prior studies shows a clear progression from traditional analytical procedures toward increasingly sophisticated techniques, including supervised and unsupervised machine learning, deep learning architectures, graph neural networks, anomaly detection algorithms, and emerging blockchain-enhanced analytical tools. These methods utilize diverse forms of financial and transactional data—ranging from conventional financial ratios and earnings indicators to complex graph-structured networks and immutable blockchain records. Collectively, these approaches have demonstrated strong potential in improving detection accuracy, uncovering hidden fraud patterns, and enhancing early-warning capabilities.

However, the review also highlights several persistent challenges. These include the scarcity of labeled fraud data, high levels of class imbalance, inconsistencies in evaluation metrics across studies, limited generalizability, and the complexity or opacity of some advanced models that may reduce interpretability for auditors. Despite these limitations, the growing body of evidence confirms that data-driven fraud detection techniques can substantially outperform traditional rule-based or manual audit procedures when implemented appropriately.

The implications for the auditing and accounting profession in the digital era are profound.

First, as financial reporting becomes increasingly digitalized and fraud techniques more sophisticated, auditors must adopt advanced data-driven analytics to strengthen fraud risk assessment and enhance substantive testing. Machine learning and network-based models can uncover anomalies, outliers, and relational patterns that are impossible to detect through conventional audit sampling. Second, the digital transformation of business processes demands that auditors develop new competencies in data analytics, programming literacy, and algorithmic interpretation to effectively evaluate AI-assisted audit evidence. Third, technologies such as blockchain, real-time transactional ecosystems, and automated record-keeping systems require auditors to adapt assurance methodologies to environments where data volume, velocity, and variety far exceed traditional audit settings. Finally, organizations and audit firms must invest in modern audit technologies, standardized analytics frameworks, and continuous training to ensure that auditors can responsibly and effectively leverage advanced analytical tools.

Overall, the findings of this review emphasize that data-driven methods are no longer optional but essential for maintaining audit quality, reinforcing public trust in financial reporting, and safeguarding the integrity of capital markets in the digital era. As technology continues to reshape the accounting landscape, the integration of robust, interpretable, and scalable analytical models will be critical in enabling auditors to detect financial statement fraud more accurately and proactively.

Reference

1. Setyawan W. Bridging Between Financial Performance and Government Performance: The Role of Public Sector Accounting in Realizing Good Governance. Oikonomia : Journal of Management Economics and Accounting. 2025 Feb 6;2(2):1–15.
2. Jiang H. Application Technologies and Challenges of Big Data Analytics in Anti-Money Laundering and Financial Fraud Detection. Open Journal of Applied Sciences. 2024;14(11):3226–36.
3. Kao LJ, Chiu CC, Lin HT, Hung YW, Lu CC. Unveiling the dimensions of digital transformation: A comprehensive taxonomy and assessment model for business. J Bus Res [Internet]. 2024;176:114595. Available from: https://www.sciencedirect.com/science/article/pii/S0148296324000997
4. Shakil Islam Account Manager M, Caldic C, Md Rakibuzzaman B, Sultanul Arefin Sourav M. Impact of Digital Transformation on Financial Reporting and Audit Processes [Internet]. Vol. 5, AJEBM. 2022. Available from: https://www.grnjournals.us/index.php/AJEBM
5. Rezaee Z. Causes, consequences, and deterence of financial statement fraud. Critical Perspectives on Accounting. 2005 Apr;16(3):277–98.
6. Huang F, No WG, Vasarhelyi MA, Yan Z. Audit data analytics, machine learning, and full population testing. Journal of Finance and Data Science. 2022 Nov 1;8:138–44.
7. Ali A, Abd Razak S, Othman SH, Eisa TAE, Al-Dhaqm A, Nasser M, et al. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Vol. 12, Applied Sciences (Switzerland). MDPI; 2022.
8. Perols J. Financial statement fraud detection: An analysis of statistical and machine learning algorithms. Auditing. 2011 May;30(2):19–50.
9. West J, Bhattacharya M. Intelligent financial fraud detection: A comprehensive review. Comput Secur [Internet]. 2016;57:47–66. Available from: https://www.sciencedirect.com/science/article/pii/S0167404815001261
10. Guidelines for performing Systematic Literature Reviews in Software Engineering. 2007.
11. Anggi Putri, Nuswantara DA. Artificial Intelligence and Data Mining in Detecting Financial Statement Fraud: A Systematic Literature Review. Journal of Accounting Science. 2025 Jul 25;9(2):204–57.
12. Lu M, Han Z, Rao SX, Zhang Z, Zhao Y, Shan Y, et al. BRIGHT - Graph Neural Networks in Real-time Fraud Detection. In: International Conference on Information and Knowledge Management, Proceedings. Association for Computing Machinery; 2022. p. 3342–51.
13. Takahashi R, Nishimura H, Matsuda K. A Graph Neural Network Model for Financial Fraud Prevention. Frontiers in Artificial Intelligence Research. 2:2025.
14. Liu C, Chan Y, Alam Kazmi SH, Fu H. Financial Fraud Detection Model: Based on Random Forest. Int J Econ Finance. 2015 Jun 25;7(7).
15. Schonlau M, Zou RY. The random forest algorithm for statistical learning. Stata Journal. 2020 Mar 1;20(1):3–29.
16. Zheng X, Abdul Hamid MA, Hou Y. Data mining algorithm in the identification of accounting fraud by smart city information technology. Heliyon. 2024 May 15;10(9).
17. Hilal W, Gadsden SA, Yawney J. Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. Vol. 193, Expert Systems with Applications. Elsevier Ltd; 2022.
18. Qian J, Tong G. Metapath-guided graph neural networks for financial fraud detection. Computers and Electrical Engineering [Internet]. 2025;126:110428. Available from: https://www.sciencedirect.com/science/article/pii/S0045790625003714
19. Tien HT, Tran-Trung K, Hoang VT. Blockchain-Data Mining Fusion for Financial Anomaly Detection: A Brief Review. In: Procedia Computer Science. Elsevier B.V.; 2024. p. 478–83.
20. Shahana T, Lavanya V, Bhat AR. State of the art in financial statement fraud detection: A systematic review. Technol Forecast Soc Change [Internet]. 2023;192:122527. Available from: https://www.sciencedirect.com/science/article/pii/S0040162523002123
21. Motie S, Raahemi B. Financial fraud detection using graph neural networks: A systematic review. Expert Syst Appl [Internet]. 2024;240:122156. Available from: https://www.sciencedirect.com/science/article/pii/S0957417423026581