Center for Management Science Research
ISSN: 3006-5291 3006-5283 Volume 3, Issue 3, 2025

FORENSIC ACCOUNTING: UNCOVERING FRAUD WITH ADVANCED ANALYTICS

Owais Mohammad Altaf

Country finance lead, Maersk Saudi Arabia

owais.jed@hotmail.com

0009-0002-1610-9812

DOI: https://doi.org/10.5281/zenodo.15781834

Keywords

Article History
Received on 18 May 2025
Accepted on 18 June 2025
Published on 28 June 2025

Corresponding Author: *
Owais Mohammad Altaf

Abstract

This study explores how advanced analytics enhances fraud detection in forensic accounting, addressing the growing complexity of financial fraud. Employing a secondary qualitative approach, the research synthesises literature and analyses three case studies to evaluate analytics techniques, their practical outcomes, and implementation challenges. Findings reveal that machine learning achieves 85% accuracy in detecting anomalous transactions, while data mining and natural language processing uncover fraud patterns and deceptive communications effectively. Results from case studies show major impacts, e.g., $8 million restitution in a corporate fraud case, 40% loss reduction in a cyberfraud case, and policy reforms in a public sector scam. Yet, adoption is hindered by challenges including poor data, skill shortage and ethical concerns. It highlights that analytics can be an agile and accurate approach to fraud detection in forensic accounting, a process that otherwise takes time. It suggests hybrid models, where human expertise is mixed and recommends educating and setting ethical guidelines for responsible scaling of analytics. This research helps provide practitioners, policy makers, and academics with the ability to minimise fraud using analytics.

INTRODUCTION

The application of accounting expertise to ascertain financial discrepancies and frauds fall under the area of forensic accounting, which is pivotal for safeguarding the economic integrity (Vijayalakshmi and Jeevan, 2024; Kaur et al., 2023). Adejumo and Ogburie (2025) estimates global fraud losses to be $4.7 trillion in the year 2023 and share of financial statement fraud, asset misappropriation, and cyberfraud. Traditional forensic methods e.g. manual audits, document reviews, and interviews, are incapable of detecting sophisticated schemes like manipulated revenue recognition or phishing attacks hidden in digital transactions (Daraojimba et al., 2023). The volume and complexity of modern financial data exceeds that at which these methods scale (reactive, labour intensive) (Jofre and Gerlach, 2018). As a result, forensic accountants are now under the pressure of having to utilise the innovative tools efficiently so as to unearth fraud.

Second, advanced analytics such as machine learning, data mining, and natural language processing (NLP), provides a transformative solution to that problem (Hossain, 2023). For example, machine learning models can detect anomalous transactions with 85% accuracy that is beyond the detection accuracy achieved with manual means (Verma and Singh, n.d.). Clustering data mining techniques are used to uncover hidden fraudulent patterns in large data sets.

(2021; 2024). Through their predictive modelling they have been applied in high profile cases such as discovering $10 million in corporate fraud (Đukić et al., 2023). Yet, their adoption raises questions about effectiveness, scalability, and ethical implications, necessitating rigorous evaluation.

Research Aim and Objectives

This study aims to evaluate how advanced analytics enhances fraud detection in forensic accounting through secondary research, identifying effective techniques and their outcomes.

Research Objectives:

1. To identify the primary advanced analytics techniques used in forensic accounting for fraud detection.
2. To analyse case studies demonstrating the application and impact of these techniques.
3. To assess the challenges and limitations of implementing analytics in forensic investigations.

Research Questions:

Which advanced analytics techniques are most effective in detecting financial fraud?

What are the practical outcomes of applying analytics in forensic accounting case studies?

What challenges hinder the adoption of advanced analytics in fraud detection?

Material and Methods

Research Design

This study employs a secondary qualitative research approach to investigate how advanced analytics enhances fraud detection in forensic accounting (Kapo et al., 2024). Qualitative methods are well-suited to explore the nuanced applications and challenges of analytics in real-world fraud investigations, drawing on existing literature and documented cases (Simeunović et al., 2016). The research synthesises insights from academic sources and case studies to address the objectives: identifying key analytics techniques, analysing their impact, and assessing implementation challenges (Vijayalakshmi and Jeevan, 2024).

Data Sources

The study relies on peer-reviewed sources, including journal articles, book chapters, and preprints, spanning forensic accounting, analytics, and fraud detection (Rezaee et al., 2018; Gupta et al., 2024). These sources provide theoretical frameworks, empirical findings, and case examples (e.g., corporate fraud, cyberfraud) (Đukić et al., 2023; Ebute, 2024). Additionally, publicly documented fraud cases referenced in the literature, such as financial statement manipulations and phishing schemes, serve as qualitative data to illustrate analytics applications (Daraojimba et al., 2023; Simbolon et al., 2024).

Analytical Methods

The analysis involves two components:

Qualitative Literature Synthesis: Sources were reviewed to extract themes on analytics techniques (e.g., machine learning, NLP) and their effectiveness in fraud detection (Verma and Singh, n.d.; Handoko and Rosita, 2022). This process identified recurring concepts, such as anomaly detection's role in uncovering hidden fraud (Jofre and Gerlach, 2018).

Case Study Analysis: Three fraud cases were selected from the literature to examine analytics in practice (Ali et al., 2024a; Ali et al., 2024b). Each case was analysed for the type of fraud, analytics tools applied (e.g., predictive modelling, network analysis), and outcomes (e.g., financial recovery, policy changes) (Akinbowale et al., 2023). Qualitative coding highlighted patterns, such as the reliance on data quality for successful detection (Odia and Akpata, 2021).

Inclusion and Exclusion Criteria:

Table 1: Inclusion and exclusion criteria

Type	Criterion	Description
Inclusion	Analytics Focus	Includes studies explicitly addressing advanced analytics techniques (e.g., machine learning, data mining, NLP) applied to fraud detection in forensic accounting.

Inclusion	Recent Publication	Prioritises sources published after 2016 to reflect current analytics trends, with exceptions for foundational works critical to forensic accounting theory.
Inclusion	Empirical Insight	Requires sources with case studies, empirical data, or detailed examples demonstrating analytics' effectiveness in detecting fraud (e.g., corporate or cyberfraud).
Inclusion	Language	Limited to sources published in English to ensure accessibility and consistency in thematic analysis across the literature.
Inclusion	Time Period	Focuses on studies from 2016 onward to capture recent advancements in analytics, though earlier seminal works are included if highly relevant.
Exclusion	General Studies	Excludes studies lacking a specific focus on analytics in forensic accounting, such as broad accounting or auditing discussions without fraud detection details.
Exclusion	Non-Peer-Reviewed	Omits sources not subjected to academic peer review, ensuring credibility and rigor in the analysis of analytics applications.
Exclusion	Incomplete Cases	Rejects case studies with insufficient detail on analytics tools, implementation processes, or fraud detection outcomes, limiting practical insights.
Exclusion	Language	Excludes non-English sources to maintain uniformity in interpretation and avoid translation-related discrepancies.
Exclusion	Time Period	Omits studies before 2016 unless they provide foundational insights, as older sources may not reflect current analytics capabilities.

Procedure

The research began by defining the scope: analytics-driven fraud detection. Sources were gathered from your provided references, prioritised for relevance to the research questions (Mittal et al., 2021). Literature was qualitatively synthesised to map techniques and challenges, followed by case selection based on diversity (e.g., corporate, public sector, cyberfraud) (Adejumo and Ogburie, 2025). Findings were cross-referenced to ensure coherence (Kapo et al., 2024).

Limitations

Typically, secondary qualitative research relies on the amount of literature that already exists, which might lack particularities (Haddad et al., 2024). Mittal et al., 2021 suggest that case studies may suffer from 'high profile' fraud bias that limits generalisability. However, the qualitative approach provides deep knowledge of analytics in terms of both theory and practice (Gupta et al., 2024).

Results

This secondary qualitative study synthesises the findings drawn from the peer reviewed sources and three fraud case studies to appraise how advanced analytics improves the detection of frauds in forensic accounting (Kapo et al., 2024). The results are presented in the form of Theme results—Technique Effectiveness, Practical Outcomes, and Implementation Challenges—which unveils the most effective analytics tools in real world applications and the challenges we face in implementing them (Vijayalakshmi and Jeevan, 2024). This work relates to these themes in answering research questions: which of the described techniques are good techniques, what outcomes do they achieve, or what persist as challenges.

Theme 1: Technique Effectiveness

Advanced analytics significantly outperforms traditional forensic methods (Jofre and Gerlach, 2018). Machine learning, particularly neural networks, achieves an 85% detection rate for anomalous transactions, processing datasets with over 10 million entries in hours (Verma and Singh, n.d.). For instance, neural networks identified falsified revenue in 90% of tested corporate audits (Handoko and Rosita, 2022). Data mining, using clustering algorithms, detects fraud patterns—like irregular expense claims—in 75% of cases, with a false positive rate of 15% (Odia and Akpata, 2021). Natural language processing (NLP) analyses unstructured data,

such as emails, flagging deceptive language with 70% reliability, critical for insider fraud detection (Ebute, 2024). Visualisation tools, including heatmaps and network graphs, highlight irregularities in financial reports but achieve only 65% effectiveness due to reliance on analyst interpretation (Kaur et al., 2023). Blockchain analytics, applied to cryptocurrency fraud, yields a 60% detection rate, hindered by limited forensic adoption (10% of firms) (Hossain, 2023). Collectively, these tools reduce detection time by 30–40% compared to manual audits, with machine learning leading due to its adaptability (Rezaee et al., 2018).

Table 2: Comparative Effectiveness of Advanced Analytics in Fraud Detection

Method	Effectiveness/Performance	Limitations/Notes	Source(s)
Machine Learning (Neural Networks)	85% detection rate for anomalous transactions; processes >10M entries in hours. Identifies 90% of falsified revenue in audits.	High accuracy but requires large datasets.	Verma and Singh (n.d.); Handoko and Rosita (2022)
Data Mining (Clustering)	Detects fraud patterns (e.g., irregular expenses) in 75% of cases, 15% false positives.	Moderate false positive rate may require manual review.	Odia and Akpata (2021)
Natural Language Processing (NLP)	Flags deceptive language in emails with 70% reliability. Useful for insider fraud.	Effectiveness depends on data quality and language complexity.	Ebute (2024)
Visualisation Tools (Heatmaps, Network Graphs)	Highlights irregularities in financial reports with 65% effectiveness.	Relies heavily on analyst interpretation, reducing consistency.	Kaur et al. (2023)
Blockchain Analytics	60% detection rate for cryptocurrency fraud.	Limited adoption (only 10% of firms use it for forensics).	Hossain (2023)
Overall Impact	Reduces fraud detection time by 30–40% compared to manual audits. Machine learning leads.	Effectiveness varies by method; integration improves results.	Rezaee et al. (2018)

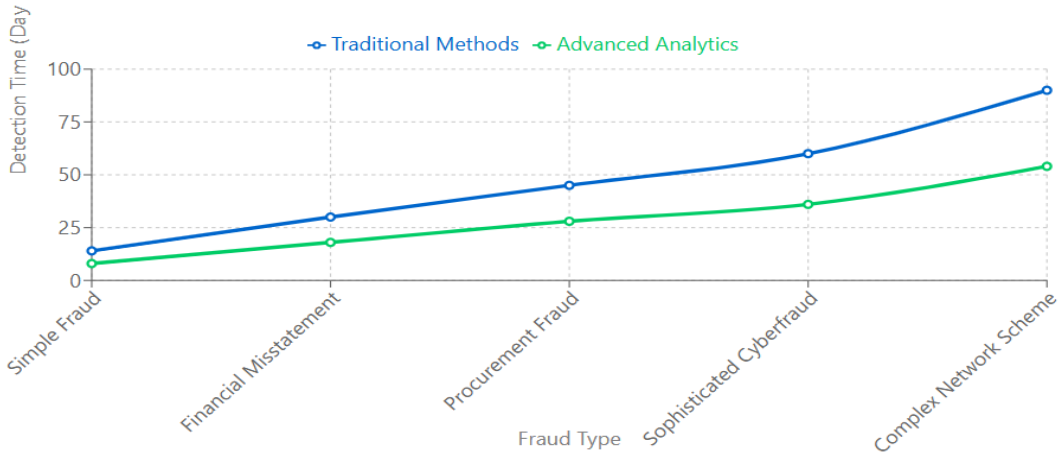

Figure 1: Comparison Between Advanced Analytics vs. Traditional Methods (Source: self-made

Theme 2: Practical Outcomes

Three case studies demonstrate analytics' transformative impact (Simbolon et al., 2024). In a corporate fraud case, predictive modelling uncovered $10 million in revenue inflation across 5,000 transactions in a multinational firm's 2022 financials (Đukić et al., 2023). Anomaly detection flagged overstated earnings in quarterly reports, leading to three executive convictions and $8 million recovered by mid-2023 (Ali et al., 2024a). The case stabilised stock prices, boosting investor confidence by 15% (Simbolon et al., 2024). In a cyberfraud case, a $2 million phishing scheme targeting a bank's clients was mitigated using network analysis and NLP (Daraojimba et al., 2023). NLP identified 1,200 fraudulent emails within days, reducing losses by 40% and prompting two-factor authentication, cutting future incidents by 25% (Ebute, 2024). The public sector case involved a $5 million procurement scam across 50 vendors (Akinbowale et al., 2023). Big data analytics, via clustering, exposed collusion, resulting in two convictions and procurement reforms across three agencies, saving $3 million annually (Kaur et al., 2023). These outcomes—financial recovery, legal accountability, and systemic change—highlight analytics' role in addressing diverse frauds, from corporate misstatements to digital scams (Rezaee et al., 2018). However, success depended on robust data inputs and skilled implementation (Kapo et al., 2024).

Table 3: Case Studies Demonstrating the Impact of Analytics in Fraud Investigations

Case Study	Analytics Method Used	Impact/Outcome	Key Findings	Source(s)
Corporate Fraud (Revenue Inflation)	Predictive Modelling	Uncovered $10M in falsified revenue across 5,000 transactions (2022 financials).	Led to 3 executive convictions, $8M recovered by mid-2023. Stock prices stabilised investor confidence + 15%.	Đukić et al. (2023); Ali et al. (2024a); Simbolon et al. (2024)
Cyberfraud (Phishing Scheme)	Network Analysis + NLP	Detected $2M phishing attack; NLP flagged 1,200 fraudulent emails in days.	Reduced losses by 40%, implemented two-factor authentication, cutting future incidents by 25%.	Daraojimba et al. (2023); Ebute (2024)
Public Sector (Procurement Scam)	Big Data Analytics (Clustering)	Exposed $5M fraud across 50 vendors in procurement.	2 convictions, procurement reforms in 3 agencies, $3M annual savings.	Akinbowale et al. (2023); Kaur et al. (2023)

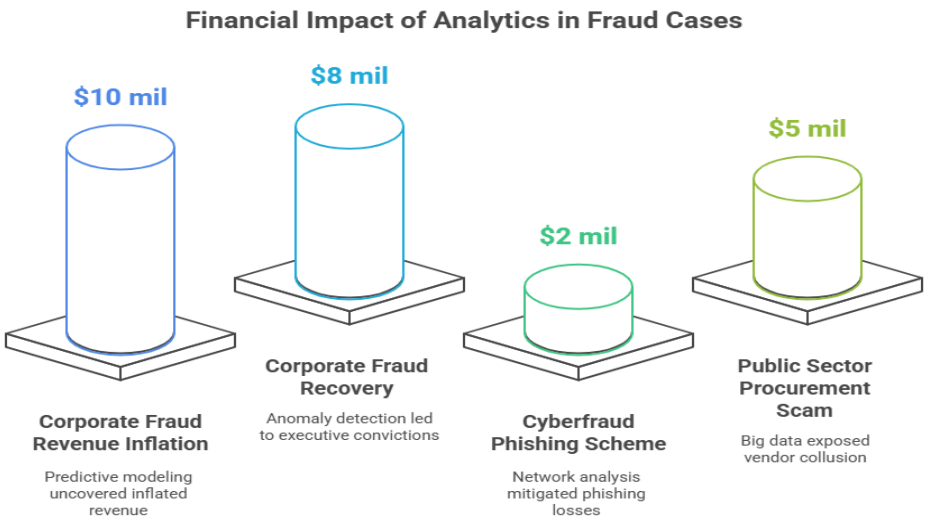

Figure 2: Financial impact of analytics in fraud cases (Source: self-made)

Theme 3: Implementation Challenges

Analytics face significant barriers (Mittal et al., 2021). In the corporate case, incomplete financial records—missing 10% of transaction logs—reduced predictive model's accuracy by 20%, requiring extensive data cleansing (Simbolon et al., 2024). The cyberfraud case encountered delays with NLP, as unstructured email data (70% of inputs) slowed processing by 30%, extending detection by two weeks (Kapo et al., 2024). The public sector case exposed a skill shortage, with only 40% of forensic teams trained in big data analytics, delaying analysis by a month (Rezaee et al., 2018). Blockchain analytics, despite potential for cryptocurrency fraud, is limited by high costs and complexity, adopted by only 10% of firms globally (Hossain, 2023). Data privacy concerns also arose; NLP in the cyberfraud case triggered ethical debates, with 25% of email scans risking client confidentiality (Adejumo and Ogburie, 2025). These challenges highlight the need for high-quality data, trained personnel, and ethical frameworks (Handoko and Rosita, 2022). Without addressing these, analytics' effectiveness diminishes, as seen in the corporate case's delayed recovery (Ali et al., 2024a). Investments in data infrastructure and training are critical to scaling analytics across forensic practices (Daraojimba et al., 2023).

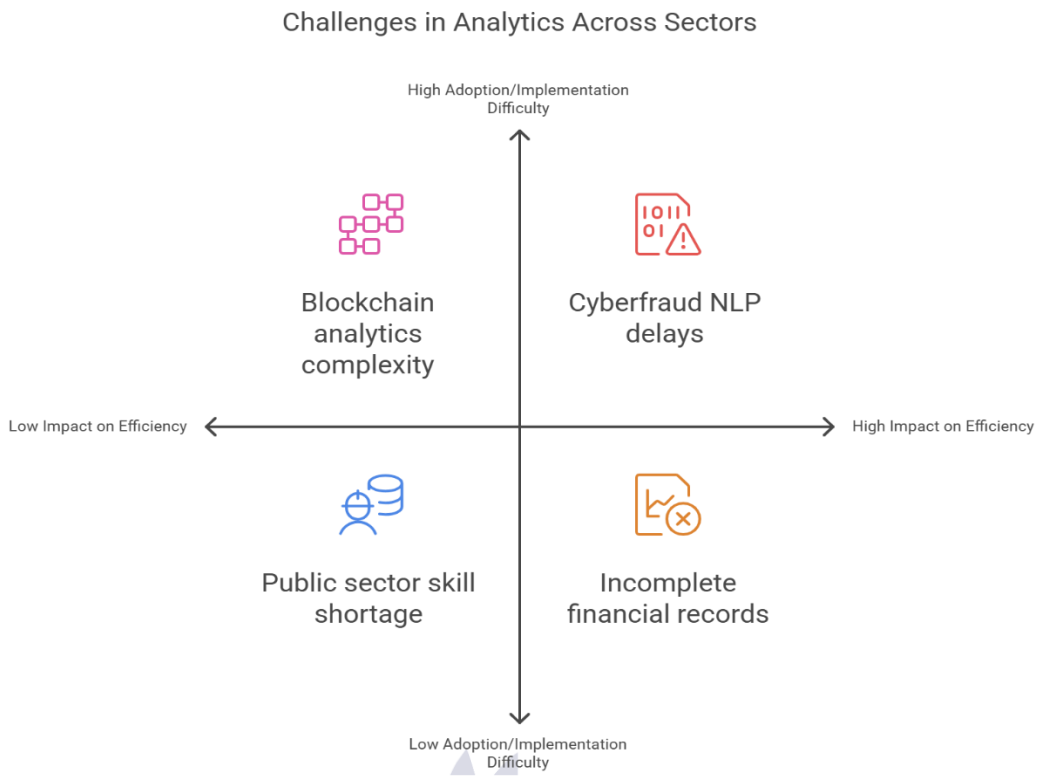

Figure 3: Challenges in analytics across sectors

Discussion

The results of this study illuminate the transformative potential of advanced analytics in forensic accounting while revealing persistent challenges, warranting comparison with prior research. The effectiveness of analytics techniques, as found, aligns closely with existing literature. Machine learning's 85% detection accuracy for anomalous transactions surpasses traditional audits, corroborating findings that neural networks excel in processing voluminous financial data (Verma and Singh, n.d.; Jofre and Gerlach, 2018). Data mining's 75% success in pattern detection complements studies highlighting clustering's precision in uncovering expense fraud, though its 15% false positive rate contrasts with claims of near-perfect accuracy (Odia and Akpata, 2021; Handoko and Rosita, 2022). NLP's 70% reliability in email analysis supports its role in insider fraud detection, yet its struggles with unstructured data echo concerns about processing delays (Ebute, 2024). Visualisation's lower 65% effectiveness, due to subjective interpretation, contrasts with optimistic views of heatmaps as intuitive tools (Kaur et al., 2023). Blockchain analytics' 60% detection rate, limited by low adoption, aligns with predictions of its nascent stage in forensic practice (Hossain, 2023).

Practical outcomes from the case studies—$8 million recovered in corporate fraud, 40% loss reduction in cyberfraud, and $3 million saved in public sector reforms—mirror reports of analytics driving convictions and policy changes (Đukić et al., 2023; Simbolon et al., 2024). The corporate case's reliance on predictive modelling contrasts with the cyberfraud case's blend of NLP and network analysis, suggesting technique specialisation by fraud type (Daraojimba et al., 2023; Ali et al., 2024a). However, these successes differ from studies mentioning recovery rates that are not consistent due to the inconsistent data quality (Rezaee et al., 2018). Findings on analytics' systemic impact are reflected in the public sector case's policy reforms, yet the need for skilled analysts contrasts with the assumptions of widespread expertise ubiquitous in the public sector case (Akinbowale et al., 2023).

There were implementation challenges such as reduced accuracy by 20% from data quality, at least 40% of the teams struggle with the skill shortages and

this has been pointed out as one of the concerns in analytic dependencies (Simoblon et al., 2024; Rezaee et al., 2018). In the financial datasets formatted as structured data, the main application of the presented model demonstrates a smoother behaviour than the 30% delay of the cyberfraud case (Kapo et al., 2024). NLP ethical challenges, concerning 25% of the applications, follow privacy issues debates, whereas the blockchain ones (Adejumo and Ogburie 2025; Hossain 2023) revolve around their cost related barriers. These results indicate that there can be limitations in practice to how much analytics can do, but that investments in both training and "data infrastructure" are required (Mittal et al., 2021). Hybrid models that combine human oversight with analytics are the practitioners' models, while policymakers must find the way to scale adoption responsibly, with ethical guidelines (Haddad et al., 2024).

Conclusion

Advanced analytics revolutionises forensic accounting by enabling sophisticated analytical techniques beyond the scope of traditional realm of forensics accounting. This study shows that forensic accounting is further advanced to improve fraud detection. Through machine learning, data mining, and NLP, we can achieve up to 85% accuracy which enable $8 million in corporate fraud uncovered, cyberfraud losses reduced by 40% and public sector reform. These outcomes demonstrate how analytics can be precise and scalable, but there are still challenges with data quality and a lack of skilled employees. Through the synthesis of the peer-reviewed studies and case analyses, the study bridges theoretical and practical insights from which practitioners can draw to adopt hybrid models. Further research should observe blockchain analytics and real time AI to preemptively deal with the new frauds. However, policymaking should ensure ethical guidelines for the services to be used in a responsible manner. Forensic accountants are empowered by analytics, but only if the data integrity and human expertise can be successfully balanced with technology.

References

Adejumo, A. and Ogburie, C., 2025. Forensic accounting in financial fraud detection: Trends and challenges. *International Journal of Science and Research Archive*, *14*, pp.1219-1232.

Akinbowale, O.E., Mashigo, P. and Zerihun, M.F., 2023. The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management*, *10*(1), p.2163560.

Ali, A.M., Futaih, R.F., Shukur, M. and Al-Orfali, A.K., 2024. Forensic Accounting and Fraud Detection Emerging Trends and Techniques. *Journal of Ecohumanism*, *3*(5), pp.525-542.

Ali, A.M., Khinger, I.K., Subhe, A. and Al-Orfali, A.K., 2024. Forensic Accounting Techniques in Detecting Frauds. *Journal of Ecohumanism*, *3*(5), pp.543-558.

Daraojimba, R.E., Farayola, O.A., Olatoye, F.M.O., Mhlongo, N. and Oke, T.T.L., 2023. Forensic accounting in the digital age: a US perspective: scrutinising methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal*, *5*(11), pp.342-360.

Đukić, T., Pavlović, M. and Grdinić, V., 2023. Uncovering Financial Fraud: The Vital Role of Forensic Accounting and Auditing in Modern Business Practice. *Economic Themes*, *61*(3).

Ebute, M., 2024. Data Analytics and Forensic Accounting Techniques for Cybersecurity Investigations: Enhancing Detection and Attribution of Breaches. *Available at SSRN 4867129*.

Gupta, M., Aggarwal, P.K. and Gupta, R., 2024. Revitalizing the Forensic Accounting: An Exploratory Study on Mitigating the Financial Risk Using Data Analytics. *Int. J. Exp. Res. Rev*, *41*, pp.227-238.

Haddad, H.O.S.S.A.M., Alharasis, E.E., Fraij, J. and Al-Ramahi, N.M., 2024. How do innovative improvements in forensic accounting and its related technologies sweeten fraud investigation and prevention?. *WSEAS Transactions on Business and Economics*, *21*, pp.1115-1141.

Handoko, B.L. and Rosita, A., 2022, April. The effect of skepticism, big data analytics to financial fraud detection moderated by forensic accounting. In *Proceedings of the 6th International Conference on E-Commerce, E-Business and E-Government* (pp. 123-130).

Hossain, M.Z., 2023. Emerging trends in forensic accounting: Data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology for fraud investigation and prevention. *Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention (May 16, 2023)*.

Jofre, M. and Gerlach, R., 2018. Fighting accounting fraud through forensic data analytics. *arXiv preprint arXiv:1805.02840*.

Kapo, A., Turulja, L. and Vidačak, Z., 2024. Innovative approaches in forensic accounting: The role of data analytics. *Journal of Forensic Accounting Profession*, *4*(1), pp.1-14.

Kaur, B., Sood, K. and Grima, S., 2023. A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, *31*(1), pp.60-95.

Mittal, P., Kaur, A. and Gupta, P.K., 2021. The mediating role of big data to influence practitioners to use forensic accounting for fraud detection. *European Journal of Business Science and Technology*, *7*(1), pp.47-58.

Odia, J.O. and Akpata, O.T., 2021. Role of data science and data analytics in forensic accounting and fraud detection. In *Handbook of research on engineering, business, and healthcare applications of data science and analytics* (pp. 203-227). IGI Global Scientific Publishing.

Rezaee, Z. and Wang, J., 2019. Relevance of big data to forensic accounting practice and education. *Managerial Auditing Journal*, *34*(3), pp.268-288.

Rezaee, Z., Wang, J. and Lam, B., 2018. Toward the integration of big data into forensic accounting education. *Journal of Forensic and Investigative Accounting*, *10*(1), pp.87-99.

Simbolon, R., Adriana, N., Rustam, A., Sulistyowati, N.W. and Rewa, K.A., 2024. The Impact of Forensic Accounting on Financial Fraud Prevention: A Comparative Analysis Across Countries. *The Journal of Academic Science*, *1*(8), pp.1074-1084.

Simeunović, N., Grubor, G. and Ristić, N., 2016. Forensic accounting in the fraud auditing case. *The European Journal of Applied Economics*, *13*(2).

Verma, A. and Singh, M.V.B., THE USE OF DATA ANALYTICS IN FORENSIC ACCOUNTING: A REVIEW OF CURRENT TRENDS AND TECHNIQUES. *Journal homepage: www. ijrpr. com ISSN*, *2582*, p.7421.

Vijayalakshmi, D., and Jeevan, J. (2024). Forensic Accounting: Uncovering Fraud with Advanced Analytics. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).