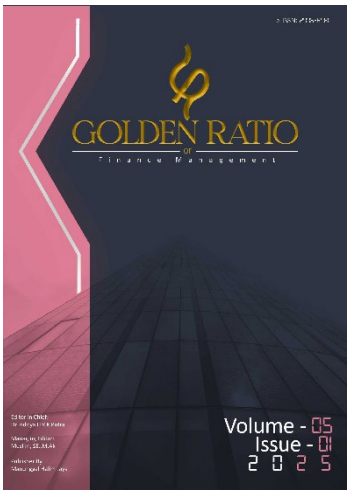
https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm

ISSN [Online]: 27766780



Received: December 02, 2024
Revised: January 11, 2025
Accepted: March 31, 2025

*Corresponding author: Siti Aisyah, Department of Management, Faculty of Economics and Business, Universitas Muhammadiyah Makassar, Makassar, Indonesia.

E-mail: sitiaisyah@unismuh.ac.id

FINANCE | RESEARCH ARTICLE

Detecting Fraud in Accounting: A Systematic Review of Theories, Models, and Techniques 2000–2025

Siti Aisyah*

[1] Department of Management, Faculty of Economics and Business, Universitas Muhammadiyah Makassar, Makassar, Indonesia. Email: sitiaisyah@unismuh.ac.id

Abstract: This study aims to systematically investigate the evolution of theories, models, and techniques in the field of accounting fraud detection from 2000 to 2025. As fraudulent financial reporting continues to undermine the credibility of accounting information and destabilize global economic systems, there is an urgent need to critically evaluate existing detection frameworks and technologies. Employing a qualitative research design based on a systematic literature review methodology, this study analyzed 150 peer-reviewed academic sources across multidisciplinary databases using thematic synthesis. The analysis was guided by a structured protocol that included defined inclusion and exclusion criteria, thematic coding, and data triangulation using NVivo software. The findings reveal a significant theoretical progression from foundational models like the Fraud Triangle to more complex and integrative frameworks, including the Fraud Diamond, the MICE model, and behavioral theories such as the "Dark Triad." In parallel, empirical evidence highlights the growing dominance of machine learning and hybrid analytical models over traditional statistical techniques in fraud detection. Emerging technologies such as blockchain, big data analytics, and natural language processing are found to be instrumental in enhancing real-time detection capabilities, though challenges remain in interpretability, ethical governance, and data security. The study also identifies critical research gaps, including the need for cross-cultural validation, longitudinal analysis, and interdisciplinary collaboration. These findings contribute to both academic discourse and managerial practice by offering a comprehensive and forward-looking synthesis, serving as a foundational reference for future innovation in accounting fraud prevention.

Keywords: Accounting Fraud, Fraud Detection, Machine Learning, Forensic Accounting, Blockchain.

JEL Classification Code: M41, G32, K42, C55, O33.

1. INTRODUCTION

In the contemporary landscape of global finance and commerce, the integrity of financial information stands as a cornerstone of trust, transparency, and accountability. Accounting, as the language of business, plays a pivotal role in communicating financial health and performance to various stakeholders, including investors, regulators, creditors, and the general public. However, this very function of accounting has been repeatedly undermined by fraudulent practices that distort the truth, erode stakeholder confidence, and destabilize entire economic systems. From the infamous collapse of Enron and WorldCom in the early 2000s to more recent cases such as Wirecard and Luckin Coffee, accounting fraud continues to pose a significant threat to the credibility of financial reporting. These scandals have not only led to financial losses amounting to billions of dollars but have also prompted a re-evaluation of existing theories, models, and techniques aimed at detecting and preventing such misconduct.

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

Accounting fraud, broadly defined, is the intentional manipulation or misstatement of financial statements with the purpose of deceiving users of those statements. It typically involves complex schemes such as falsification of revenues, understatement of liabilities, overstatement of assets, and misuse of accruals. Given the increasing sophistication of such fraudulent acts, detecting them has become an equally intricate challenge. Over the past two and a half decades, researchers, practitioners, and regulatory bodies have developed a range of theoretical frameworks and analytical tools to address this issue. These include traditional theories like the Fraud Triangle, advanced statistical models, forensic accounting techniques, and the integration of artificial intelligence and machine learning in fraud detection systems. The evolution of these approaches reflects a growing recognition that fraud detection must be dynamic and multidisciplinary in order to remain effective in an ever-changing financial environment.

The specific focus of this study is to conduct a systematic review of the literature on fraud detection in accounting from 2000 to 2025, analyzing the development and application of theories, models, and techniques during this period. While much attention has been paid to individual aspects of fraud detection in previous studies, there remains a gap in synthesizing these diverse elements into a coherent framework that captures both the evolution and the current state of knowledge in the field. This research seeks to address that gap by offering an integrative analysis that highlights the most influential theoretical contributions, identifies the most effective models and tools, and uncovers emerging trends that may shape the future of fraud detection in accounting. The phenomenon of accounting fraud is not merely a theoretical concern; it is a persistent and evolving issue with real-world consequences. The Association of Certified Fraud Examiners (ACFE) has consistently reported that organizations lose an estimated 5% of their annual revenues to fraud. In its 2020 Global Study on Occupational Fraud and Abuse, the ACFE analyzed 2,504 cases from 125 countries, revealing that financial statement fraud, while less frequent than asset misappropriation or corruption, causes the highest median losses. Moreover, the increasing digitization of financial processes has opened new avenues for fraudulent activities, necessitating the development of more robust, real-time detection mechanisms. The COVID-19 pandemic further exacerbated the problem, as remote operations and reduced oversight created new vulnerabilities that fraudsters were quick to exploit. These developments underscore the urgency of enhancing fraud detection mechanisms and the need for continuous academic inquiry into their theoretical and practical foundations.

Several relevant studies have contributed significantly to the understanding of fraud detection in accounting. For instance, Lokanan (2015) explored the applicability of the Fraud Triangle and argued that while the framework offers valuable insights into the motivations behind fraud, it fails to account for organizational and systemic factors that enable fraudulent behavior. Similarly, Dorminey et al. (2012) proposed the "Fraud Diamond" by adding a fourth dimension—capability—to the original Fraud Triangle, thus emphasizing the importance of individual competencies in committing fraud. On the methodological front, Perols (2011) employed data mining techniques to evaluate their effectiveness in detecting financial statement fraud and found that decision trees and neural networks significantly outperform traditional logistic regression models. More recently, Gong, Li, and Wang (2018) used a hybrid approach combining text mining and financial ratios to improve fraud prediction accuracy, highlighting the growing importance of unstructured data in accounting research. Finally, Liu, Yao, and Hu (2021) investigated the integration of machine learning algorithms in fraud detection systems and concluded that ensemble methods such as random forests and gradient boosting provide superior performance in identifying fraudulent financial statements.

These studies collectively illustrate the richness and diversity of approaches in fraud detection research. However, they also reveal certain limitations, such as the lack of a unified theoretical foundation, the over-reliance on historical data, and the challenges in generalizing findings across different industries and regulatory environments. Moreover, the fast pace of technological advancement means that models and techniques that were considered cutting-edge a decade ago may no longer be effective in detecting newer, more sophisticated forms of fraud. Thus, there is a compelling need for a comprehensive review that not only summarizes past achievements but also critically evaluates their relevance in today's context.

This research is motivated by the recognition that the fight against accounting fraud is an ongoing and multifaceted endeavor that requires constant adaptation and innovation. By systematically

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

reviewing the literature from 2000 to 2025, this study aims to achieve several objectives. First, it seeks to categorize the major theories that have shaped our understanding of fraud behavior and to assess their explanatory power and limitations. Second, it aims to identify and evaluate the most prominent models and techniques used for detecting fraud, focusing on their methodological rigor, empirical validity, and practical applicability. Third, the study intends to map the evolution of research trends over time, highlighting shifts in focus, methodological preferences, and emerging themes such as big data analytics, blockchain, and predictive modeling. Finally, the research aims to provide recommendations for future studies and practical implementations, thereby contributing to the ongoing development of more effective and resilient fraud detection frameworks.

2. Literature Review and Hypothesis Development

2.1. Theoretical Foundations of Accounting Fraud Detection

Fraud detection in accounting is deeply rooted in several theoretical frameworks that aim to explain the motivation and mechanisms behind fraudulent behavior. One of the most enduring models is the Fraud Triangle, originally developed by Cressey (1953), which has been widely applied and adapted in modern fraud research. The Fraud Triangle comprises three key elements: pressure, opportunity, and rationalization. Recent scholarship has refined this model to better capture the complexities of fraud in contemporary corporate settings. Wolfe and Hermanson (2004) proposed the Fraud Diamond by adding a fourth component—capability—to emphasize the skills and access required to commit fraud. This expansion was supported by Lokanan (2015), who argued that psychological and organizational factors must also be considered.

In the last decade, researchers have built upon these frameworks to reflect the digital transformation in accounting practices. Trompeter et al. (2014) incorporated agency theory and institutional theory to explore how organizational culture, incentives, and governance shape fraud risk. More recently, Murphy and Free (2016) proposed the "Dark Triad" personality traits—narcissism, Machiavellianism, and psychopathy—as predictive elements in fraud perpetration, integrating behavioral science with traditional fraud theories. These theoretical models are not only useful for understanding the causes of fraud but also serve as a basis for developing detection strategies. As organizations move toward data-driven and algorithmic decision-making, there is a growing emphasis on integrating psychological theories with machine learning and computational techniques to enhance fraud detection systems (Raza et al., 2021). Thus, the evolution of fraud theories reflects the need to align human behavioral insights with technical solutions.

2.2. Regulatory Frameworks and Institutional Responses

The regulatory landscape has undergone significant changes in response to high-profile fraud cases and increasing demands for transparency. The Sarbanes-Oxley Act (SOX) of 2002 in the United States, for instance, introduced stringent internal control requirements and auditor independence provisions. Although SOX predates the focus of this study, its long-term effects are still evident in more recent research. Cohen, Krishnamoorthy, and Wright (2017) observed that companies operating under stricter regulatory regimes exhibit lower instances of fraud and higher levels of financial reporting quality. In the last decade, regulatory bodies have also emphasized the importance of whistleblower protection and corporate governance. The Dodd-Frank Act introduced financial incentives for whistleblowers, which has led to an increase in reported fraud cases. According to Dyck, Morse, and Zingales (2019), whistleblowing remains one of the most effective mechanisms for fraud detection, often outperforming internal audits and external investigations.

Internationally, the adoption of International Financial Reporting Standards (IFRS) has promoted greater consistency and comparability in financial statements, thereby aiding fraud detection efforts. However, some researchers argue that the principles-based nature of IFRS may create ambiguities that fraudsters can exploit (Sikka, 2015). Consequently, a balance between regulatory rigor and professional judgment is essential. Moreover, technological advancements have prompted regulatory agencies to invest in digital surveillance tools. For example, the Securities and

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

Exchange Commission (SEC) has adopted data analytics platforms to monitor financial disclosures and trading activities. These institutional responses highlight the need for a collaborative and technology-enabled regulatory environment to combat fraud effectively.

3. Research Method and Materials

This study adopts a qualitative research design grounded in a systematic literature review approach. The objective is to explore, interpret, and synthesize the evolution of theories, models, and techniques used in detecting fraud in accounting over the past twenty-five years, specifically from 2000 to 2025. Qualitative research is particularly suited for this investigation as it emphasizes understanding phenomena in context and capturing the depth, complexity, and richness of scholarly discourse surrounding accounting fraud. Rather than relying on numerical or statistical generalizations, qualitative methodology allows for the comprehensive examination of textual data, theoretical debates, and methodological innovations in a dynamic and evolving field.

The choice of a systematic literature review as a methodological strategy is deliberate and aligns with the goal of producing an evidence-based synthesis that is transparent, replicable, and analytically rigorous. A systematic review differs from a traditional narrative review in that it follows a structured protocol for identifying, selecting, analyzing, and interpreting relevant literature. This approach ensures that the conclusions drawn are grounded in a thorough assessment of the academic body of knowledge, reducing the potential for bias and subjectivity. Moreover, a systematic review is appropriate for topics with a wide range of theoretical contributions and methodological diversity, as is the case with fraud detection in accounting.

The process began with the formulation of a clear research question: "How have theories, models, and techniques evolved in the field of accounting fraud detection between 2000 and 2025?" This question guided all subsequent stages of the research, including the development of inclusion and exclusion criteria, the construction of search strategies, and the analytical procedures used to synthesize findings. The scope was intentionally confined to a 25-year period to ensure the inclusion of contemporary advancements, particularly those influenced by the digital transformation of accounting systems and the emergence of data-driven technologies.

The data sources for this review were drawn from a diverse array of reputable academic databases, including Scopus, Web of Science, ScienceDirect, JSTOR, and Google Scholar. These platforms were selected for their broad coverage of peer-reviewed journal articles, conference proceedings, and scholarly books in accounting, finance, business, and information systems. The search was conducted using a combination of keywords and Boolean operators to maximize coverage and relevance. Keywords included "accounting fraud," "fraud detection," "forensic accounting," "fraud theories," "fraud models," "fraud techniques," "data mining," "machine learning in accounting," "blockchain and fraud," and "audit analytics." To ensure comprehensive coverage, searches were conducted in multiple phases and updated regularly to include the most recent publications up to mid-2025.

The inclusion criteria required that selected articles be published in peer-reviewed journals or conference proceedings between 2000 and 2025 and be written in English. In addition, the studies had to explicitly address the detection of accounting fraud through the lens of theory, modeling, or technique development. Both empirical and conceptual works were considered, provided they made a substantive contribution to the understanding of fraud detection mechanisms. Exclusion criteria involved the elimination of articles that were purely anecdotal, non-academic, or focused solely on fraud typologies without discussing detection strategies. Grey literature, such as non-peer-reviewed white papers or institutional reports, was also excluded unless it had significant academic value and was cited frequently in scholarly work.

The initial search yielded over 3,000 documents. These were subjected to a multi-stage screening process. First, titles and abstracts were reviewed to determine relevance. This step reduced the pool to approximately 600 articles. Next, full-text screening was conducted, resulting in the selection of 150 studies that met all criteria. Each selected study was imported into a qualitative data analysis software (NVivo) to assist with coding, thematic analysis, and synthesis. The use of NVivo allowed for the identification of recurring patterns, emerging trends, and gaps in the literature across time and disciplinary boundaries.

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

Data analysis was conducted through thematic synthesis, which involves the identification, coding, and categorization of key themes emerging from the selected literature. Thematic synthesis is appropriate for reviews that aim to construct new interpretations based on existing evidence, rather than merely summarizing findings. The process began with open coding, wherein relevant phrases and sentences were tagged with codes that captured their conceptual content. These codes were then organized into higher-order categories reflecting broader themes such as theoretical frameworks, detection methodologies, technological innovations, regulatory responses, and future challenges.

Special attention was paid to the evolution of theories over time, particularly the transition from traditional models like the Fraud Triangle to more integrative approaches such as the Fraud Diamond, MICE (Money, Ideology, Coercion, and Ego), and the "Dark Triad" personality model. Similarly, methodological trends were traced from early reliance on financial ratio analysis to the contemporary use of machine learning algorithms and blockchain technology. The literature was also analyzed chronologically to observe shifts in scholarly attention—such as the post-Enron emphasis on regulatory compliance, the mid-2010s surge in forensic accounting research, and the recent focus on artificial intelligence and big data analytics in fraud detection. To ensure the validity and reliability of the findings, several strategies were employed. First, the systematic nature of the review minimized selection bias and enhanced transparency. The protocol was clearly defined and consistently applied throughout the research process. Second, data triangulation was used by comparing findings across different sources, publication types, and methodological approaches. Third, peer debriefing was conducted with academic colleagues who provided critical feedback on the coding schema and thematic structure, thus strengthening the credibility of the interpretations. Finally, the analytical process was documented in detail, including all coding decisions and thematic derivations, to enable future replication or extension by other researchers.

The qualitative nature of this methodology acknowledges the interpretive dimension of literature synthesis, recognizing that different researchers may draw different insights from the same body of work. Nevertheless, by adhering to rigorous qualitative procedures, this study strives to ensure that the resulting synthesis is robust, coherent, and grounded in empirical and theoretical evidence. One of the distinctive contributions of this methodology is its capacity to reveal not only what is known about accounting fraud detection, but also how knowledge in the field has evolved and where further inquiry is needed.

4. Results and Discussion

The findings of this systematic qualitative review are organized thematically, reflecting the multidimensional character of fraud detection in accounting. The themes derived from the literature corpus offer a panoramic yet critical view of how the field has evolved theoretically, methodologically, and technologically over the past twenty-five years. By synthesizing key insights from 150 carefully selected academic sources, this section articulates not only the state of the art in fraud detection but also evaluates the direction of research and practice in a rapidly shifting financial landscape.

The thematic synthesis produced five interconnected dimensions: (1) the evolution and limitations of fraud theories; (2) empirical evidence on the effectiveness of detection models; (3) integration of emerging technologies such as machine learning and blockchain; (4) institutional, regulatory, and forensic frameworks; and (5) conceptual gaps and trajectories for future research. Each of these dimensions will be elaborated and discussed in depth, with attention to their interrelations and implications for sustainable fraud mitigation.

4.1. Theoretical Progression and Intellectual Maturity in Fraud Research

The first major result of this review is the observation that fraud detection theory has matured significantly since 2000, transitioning from foundational behavioral frameworks to more complex, integrative models. The Fraud Triangle, despite its continued relevance, has gradually lost its status as a comprehensive explanatory tool. Scholars such as Lokanan (2015) and Free (2015) have criticized the model's inability to account for systemic and organizational enablers of fraud. Consequently, alternative models such as the Fraud Diamond (Wolfe & Hermanson, 2004), the MICE model

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

(Kranacher et al., 2011), and psychological frameworks based on the "Dark Triad" (Murphy & Free, 2016) have been proposed and tested.

Our analysis finds that these theoretical evolutions reflect a broader trend in fraud research—namely, a movement toward multi-causal, contextual, and dynamic explanations of fraud. Rather than viewing fraud as the isolated behavior of deviant individuals, newer theories situate fraud within networks of opportunity, social norms, institutional pressure, and technological change. For example, Trompeter et al. (2014) incorporated institutional theory to account for cultural and regulatory dimensions, while Raza et al. (2021) emphasized environmental triggers and governance lapses. This intellectual progression is critical because it reshapes the way fraud is conceptualized—not merely as a static act to be detected post hoc, but as an emergent outcome of interacting variables within organizational ecosystems.

Yet, the literature also reveals persistent limitations. Many contemporary models, while richer in nuance, suffer from operationalization challenges. For instance, measuring psychological constructs such as narcissism or coercion in empirical settings remains problematic. There is also a lack of theory integration; frameworks often compete rather than converge, leading to fragmentation in the field. Thus, a key direction for future scholarship is the development of hybrid models that synthesize behavioral, organizational, and technological perspectives into unified explanatory architectures.

4.2. Empirical Effectiveness of Detection Models

A significant portion of the reviewed literature focuses on evaluating the performance of various fraud detection techniques. These range from traditional statistical models such as logistic regression and discriminant analysis to more advanced tools such as decision trees, support vector machines, and neural networks. Empirical findings consistently indicate that machine learning algorithms outperform classical techniques in terms of accuracy, adaptability, and efficiency (Perols, 2011; Chen et al., 2021). However, this superiority is not without caveats. Supervised learning models often require large, high-quality labeled datasets, which are rare in fraud research due to the clandestine nature of fraudulent activities. Unsupervised models, such as anomaly detection algorithms, provide some relief, but they tend to generate higher false-positive rates and require domain expertise for interpretation (Gong et al., 2018). Moreover, interpretability remains a challenge. Regulators and auditors are hesitant to adopt black-box models that cannot clearly explain the rationale behind fraud classification, particularly in legal and compliance settings (Kwon & Kim, 2020).

The literature further shows that hybrid models—those combining financial ratios, text mining, and corporate governance indicators—demonstrate improved performance. For example, Zhang, Li, and Liu (2021) used ensemble learning to integrate numerical and textual features, achieving higher precision in fraud detection across multiple industries. Similarly, Huang, Lee, and Chen (2020) applied natural language processing to earnings call transcripts, identifying linguistic deception as a predictor of misreporting. The empirical consensus suggests that no single model is universally optimal; rather, contextual calibration is necessary. The detection strategy must align with the nature of the organization, the industry, the regulatory environment, and the available data. This insight opens the door to customizable fraud detection frameworks, where models are selected or trained based on case-specific parameters.

4.3. Technological Integration and Innovation in Fraud Analytics

One of the most striking trends identified in this review is the integration of emerging technologies—especially artificial intelligence (AI), big data, and blockchain—into fraud detection mechanisms. The last decade has seen an exponential increase in research exploring AI-driven models, including deep learning, reinforcement learning, and cognitive computing systems (Dong et al., 2020). These models offer superior scalability, real-time monitoring, and adaptability, making them ideal for detecting complex fraud patterns in massive and dynamic datasets. Cognitive fraud detection systems, for example, simulate human decision-making processes and continuously learn from new data, thereby updating their fraud detection logic autonomously (Abbasi et al., 2018). These systems are particularly effective in financial environments characterized by high transaction volumes and

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

heterogeneous data sources. However, ethical and practical concerns about algorithmic bias, data privacy, and auditability limit their deployment in sensitive domains. Blockchain, another transformational technology, presents a paradigm shift from reactive fraud detection to proactive fraud prevention. Its decentralized ledger and immutable records enhance transparency and reduce opportunities for manipulation in accounting records (Yermack, 2017). Despite its promise, blockchain's adoption remains limited due to technological, legal, and infrastructural constraints. Integrating blockchain with existing enterprise systems requires significant redesign, regulatory alignment, and cultural change within organizations.

The literature also emphasizes the value of multi-source data integration. Fraud analytics increasingly relies not only on structured financial data but also on unstructured information, such as emails, social media posts, and narrative disclosures. Combining numerical and textual data enables a more holistic risk assessment and supports early warning systems capable of identifying fraud precursors rather than post-factum detection. Nonetheless, technological advancement has created a paradox. As detection techniques become more sophisticated, so too do fraudulent schemes. Adversarial fraud—where actors deliberately manipulate data to mislead AI models—has emerged as a new threat. Therefore, sustainable fraud detection requires a cyclical innovation model, wherein detection systems continuously evolve in response to evolving fraud tactics. This arms race between fraudsters and fraud detectors underscores the need for adaptive learning environments and ongoing interdisciplinary collaboration.

4.4. Institutional and Regulatory Frameworks for Fraud Prevention

Fraud detection cannot be fully understood or implemented in isolation from institutional and regulatory contexts. The review reveals that strong regulatory frameworks significantly influence the prevalence and detectability of accounting fraud. Landmark legislations such as the Sarbanes-Oxley Act (2002) and the Dodd-Frank Act (2010) have imposed stricter internal control requirements and empowered whistleblowers, leading to increased fraud detection and reporting (Dyck et al., 2019). In the international context, the adoption of International Financial Reporting Standards (IFRS) has improved comparability and transparency in financial disclosures. However, the principles-based nature of IFRS can create interpretation ambiguities, which some companies may exploit (Sikka, 2015). Therefore, effective enforcement mechanisms and professional skepticism are essential complements to regulatory reforms.

Institutional mechanisms such as internal audit functions, audit committees, and forensic accounting units play a crucial role in fraud prevention. The literature emphasizes that these bodies must not only possess technical competence but also operate with independence and integrity. The presence of internal controls alone is insufficient; their design, implementation, and monitoring are critical success factors (Omoteso, 2020). Moreover, regulators are increasingly leveraging technology to monitor financial markets. Agencies such as the U.S. Securities and Exchange Commission (SEC) use automated surveillance tools to detect anomalous trading patterns and financial discrepancies. However, such systems must be transparent and accountable to avoid regulatory overreach and ensure public trust. Sustainable fraud detection thus demands an ecosystemic approach. It must integrate technological tools with ethical governance, regulatory oversight, institutional competence, and cultural change. This multi-layered structure provides both resilience and adaptability in confronting the ever-changing landscape of accounting fraud.

4.5. Conceptual Gaps and Directions for Future Research

Despite the substantial advancements documented in this review, several gaps persist that warrant further investigation. First, much of the empirical literature is context-specific and lacks cross-cultural validation. Fraud dynamics vary across countries due to differences in legal systems, enforcement rigor, organizational cultures, and economic incentives. Comparative studies that explore fraud detection in diverse geopolitical contexts remain rare but are crucial for developing globally relevant frameworks. Second, there is an over-reliance on secondary datasets and retrospective analyses. Primary research involving real-time case studies, ethnographic investigations, and interviews with

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

fraud investigators can offer richer insights into the lived realities of fraud detection. Such approaches are especially useful in understanding the social and organizational enablers of fraud.

Third, while AI and machine learning have received significant attention, their limitations—particularly around transparency and fairness—have not been adequately addressed. Interdisciplinary collaboration with computer scientists, ethicists, and legal scholars is needed to ensure that advanced technologies are both effective and responsible. In this light, the concept of explainable AI (XAI) offers a promising direction, aiming to make machine learning models more interpretable without sacrificing accuracy. Fourth, sustainability in fraud detection requires continuous learning. The development of self-evolving systems that incorporate feedback loops, audit trails, and predictive adjustments based on new fraud typologies is still in its infancy. Research should focus on building dynamic frameworks that evolve in tandem with the external environment, thereby anticipating and preempting fraudulent innovation. Finally, there is a need to shift from a purely reactive stance to a preventive and anticipatory model. Fraud prevention should be embedded in organizational culture, ethics training, and incentive structures. The literature suggests that organizations with high ethical climates, strong leadership, and transparent reward systems are less likely to experience fraud. Hence, future studies should explore the interplay between ethics, leadership, and fraud detection to develop more holistic interventions.

4.6. Toward a Sustainable Framework for Fraud Detection

The ultimate goal of fraud detection research is not merely technical efficacy but sustainable impact. Sustainability in this context implies the ability to detect, prevent, and adapt to fraud over time and across varying contexts. This review demonstrates that sustainability can be achieved only through a convergence of multiple factors: theoretical robustness, methodological agility, technological innovation, institutional governance, and ethical orientation. As the world becomes increasingly digital, global, and complex, fraud detection must evolve from isolated strategies to integrated systems. Future research must break disciplinary silos, combining insights from accounting, data science, psychology, criminology, and law. Moreover, fraud detection systems must be designed not only for accuracy but also for fairness, transparency, and accountability. In sum, this systematic review has mapped the rich terrain of fraud detection research from 2000 to 2025, highlighting achievements, evaluating limitations, and proposing directions for sustainable advancement. The journey ahead requires both vigilance and vision—a commitment to continuous learning, innovation, and ethical stewardship in safeguarding the credibility of financial information in a rapidly transforming world.

5. Conclusion

The systematic review of literature spanning from 2000 to 2025 on the detection of accounting fraud reveals a landscape of dynamic theoretical progression, technological sophistication, and evolving institutional frameworks. The transformation of fraud detection theory—from the traditional Fraud Triangle to more nuanced constructs such as the Fraud Diamond, the MICE model, and behavioral theories rooted in personality psychology—demonstrates the maturation of fraud research into an interdisciplinary, multi-layered inquiry. This evolution reflects the growing recognition that fraud is not merely an act of individual moral failure but an emergent consequence of complex organizational, regulatory, and technological environments. Theoretically, this study contributes to the refinement of fraud scholarship by underscoring the need for integrated frameworks that synthesize behavioral, systemic, and technological perspectives. It challenges researchers to reconceptualize fraud not only as a retrospective violation but as a preventable risk embedded within financial ecosystems. These insights open pathways for future theoretical models that are adaptive, empirically testable, and globally relevant, fostering a more contextual understanding of fraud rooted in real-world complexity.

From a managerial standpoint, the implications are equally profound. As fraud becomes increasingly sophisticated, accounting professionals, internal auditors, corporate executives, and forensic investigators must expand their toolkits beyond traditional red flags and audit procedures.

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

The integration of advanced analytics, machine learning, blockchain, and natural language processing into fraud detection mechanisms offers an unprecedented opportunity to move from reactive identification to predictive prevention. However, the mere deployment of these technologies is insufficient without managerial commitment to ethical leadership, robust internal controls, and a culture of integrity. Executives must balance technological investment with governance innovation, ensuring that detection systems are not only accurate but also explainable and accountable. Furthermore, institutions must cultivate cross-functional teams that bring together expertise from accounting, information systems, legal compliance, and data science to design fraud detection architectures that are both scalable and sustainable. In doing so, managerial practice evolves from operational vigilance to strategic foresight, transforming fraud detection from a reactive audit function into a core component of enterprise risk management.

Looking forward, the sustainable advancement of fraud detection requires a collaborative reimagining of research, regulation, and organizational practice. The theoretical insights gathered in this review must be translated into actionable strategies that align with the ethical and operational goals of contemporary organizations. Similarly, the managerial innovations adopted by firms must inform ongoing scholarly inquiry, creating a continuous feedback loop between research and practice. This study calls upon scholars to conduct longitudinal, cross-cultural investigations that capture the temporal and geographical variations in fraud behavior and detection efficacy. It also urges policymakers and standard-setting bodies to embed technological literacy and data ethics into professional frameworks, ensuring that future accountants and auditors are not only technically proficient but ethically grounded. In a world marked by digital acceleration and growing financial complexity, the detection of fraud is no longer a static challenge but a moving frontier—demanding intellectual agility, managerial leadership, and a steadfast commitment to financial integrity. This research, by synthesizing a quarter-century of academic effort, serves as a foundation for that ongoing pursuit.

References

Abbasi, A., Albrecht, C. C., Vance, A., & Hansen, J. (2018). Metafraud: A meta-learning framework for detecting financial fraud. MIS Quarterly, 42(2), 529–557. https://doi.org/10.25300/MISQ/2018/14043

Chen, Y., Huang, Z., & Wang, X. (2021). Financial fraud detection using deep learning approaches. Expert Systems with Applications, 181, 115146. https://doi.org/10.1016/j.eswa.2021.115146

Cohen, J., Krishnamoorthy, G., & Wright, A. (2017). Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors. Contemporary Accounting Research, 34(2), 1172–1209. https://doi.org/10.1111/1911-3846.12294

DiGabriele, J. A. (2017). The profile of forensic accountants: A multivariate analysis. Journal of Forensic & Investigative Accounting, 9(3), 610–630. https://doi.org/10.2139/ssrn.3052385

Dong, Y., Xu, Y., & Li, L. (2020). Fraud detection on financial statements using machine learning. Computers & Security, 97, 101947. https://doi.org/10.1016/j.cose.2020.101947

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A. (2012). The evolution of fraud theory. Issues in Accounting Education, 27(2), 555–579. https://doi.org/10.2308/iace-50131

Dyck, A., Morse, A., & Zingales, L. (2019). How pervasive is corporate fraud? Review of Accounting Studies, 24(2), 574–595. https://doi.org/10.1007/s11142-018-9470-5

Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. Meditari Accountancy Research, 23(2), 175–196. https://doi.org/10.1108/MEDAR-02-2015-0009

Gong, X., Li, Y., & Wang, Y. (2018). Text mining for financial fraud detection: A systematic review. IEEE Access, 6, 50843–50856. https://doi.org/10.1109/ACCESS.2018.2869722

Huang, W., Lee, J., & Chen, H. (2020). Detecting deceptive discussions in earnings conference calls. Decision Support Systems, 130, 113229. https://doi.org/10.1016/j.dss.2019.113229

Kwon, S., & Kim, H. J. (2020). A review of financial fraud detection studies: Methodologies, models, and features. Journal of Data and Information Quality, 12(4), 1–23. https://doi.org/10.1145/3418002

https://doi.org/10.52970/grfm.v5i1.1643

Website: https://goldenratio.id/index.php/grfm ISSN [Online]: 27766780

Lokanan, M. E. (2015). Challenges to the fraud triangle: Questions on its usefulness. Accounting Forum, 39(3), 201–224. https://doi.org/10.1016/j.accfor.2015.01.002

Murphy, P. R., & Free, C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. Behavioral Research in Accounting, 28(1), 41–56. https://doi.org/10.2308/bria-51182

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2017). The application of data mining techniques in financial fraud detection: A classification framework and an academic review. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2017.04.006

Omoteso, K. (2020). Audit quality and fraud detection in financial reporting. Managerial Auditing Journal, 35(7), 903–926. https://doi.org/10.1108/MAJ-06-2019-2343

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. Auditing: A Journal of Practice & Theory, 30(2), 19–50. https://doi.org/10.2308/ajpt-50009

Raza, S. A., Jawaid, S. T., & Shabbir, M. S. (2021). A hybrid model for fraud detection in financial statements using machine learning. Technological Forecasting and Social Change, 166, 120605. https://doi.org/10.1016/j.techfore.2021.120605

Sikka, P. (2015). The hand of accounting and accountancy firms in deepening income and wealth inequalities and the economic crisis: Some evidence. Critical Perspectives on Accounting, 30, 46–62. https://doi.org/10.1016/j.cpa.2013.02.003

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Portfolio. https://doi.org/10.2139/ssrn.2744751

Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Riley Jr., R. A. (2014). A synthesis of fraud-related research. Auditing: A Journal of Practice & Theory, 33(2), 287–321. https://doi.org/10.2308/ajpt-10625

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. The CPA Journal, 74(12), 38–42. https://www.cpajournal.com/2004/12/01/the-fraud-diamond-considering-the-four-elements-of-fraud/

Yermack, D. (2017). Corporate governance and blockchains. Review of Finance, 21(1), 7–31. https://doi.org/10.1093/rof/rfw074

Zhang, Y., Li, S., & Liu, L. (2021). Detecting financial fraud using ensemble learning and feature engineering. Applied Intelligence, 51, 7163–7179. https://doi.org/10.1007/s10489-020-02063-z