INTERNATIONAL JOURNAL OF
PUBLIC FINANCE
AND ACCOUNTABILITY

NAWALA

Volume 4, Number 1, 2025

Evaluating the Effectiveness of AI-Powered Fraud Detection in Public Finance Audits

Kashari[1*]

[1] Universitas Teuku Umar, Meulaboh, Indonesia

Abstract

Article history:
Received: March 26, 2025
Revised: April 11, 2025
Accepted: May 19, 2025
Published: June 30, 2025

Keywords:
Accountability, Artificial Intelligence, Fraud Detection, Public Finance.

Identifier:
Nawala
Page: 32-43
https://nawala.io/index.php/ijpfa

This study examines the effectiveness of artificial intelligence (AI)-powered fraud detection systems in enhancing the accuracy and efficiency of public finance audits. The central question investigates how AI tools, including machine learning and natural language processing, can address the limitations of traditional audit methods in detecting complex and emerging fraud schemes. Adopting a systematic literature review methodology, the study synthesizes findings from peer-reviewed research to evaluate technological capabilities, implementation challenges, and governance considerations. Results indicate that AI-based systems improve anomaly detection, reduce manual workload, and enable real-time monitoring, but their impact is moderated by data quality, interpretability, and institutional readiness. The discussion emphasizes the need for transparent algorithms, auditor capacity-building, and policy frameworks to mitigate risks such as bias and over-reliance on automated decision-making. The study concludes that integrating AI into audit processes can significantly strengthen fiscal oversight when aligned with ethical and accountability principles.

*Corresponding author:
kashari@utu.co.id (Kashari)

1. Introduction

Artificial intelligence (AI) and machine learning (ML) are reshaping how auditors search for irregularities across ever-larger government datasets. Traditional sample-based audit procedures struggle to scale to modern, digital public finance systems with millions of transactions, heterogeneous file types, and frequent real-time activity. AI-driven approaches including supervised classifiers, unsupervised anomaly detection, and natural language processing (NLP) for document review promise to extend auditors' reach by scanning full populations, identifying subtle patterns, and flagging high-risk items for human review (Yoon et al., 2015).

In practice, major audit firms and academic studies report that the primary, near-term gains of AI in audit relate to anomaly detection and fraud prevention: algorithms can prioritize transactions for inspection, assist in revenue/invoice matching, and extract information from unstructured contracts via NLP, freeing auditors to focus on interpretation and investigation rather than routine data sifting (Fedyk et al., 2022). Empirical work and interviews with audit partners indicate AI is being deployed top-down within firms and is already shifting how labor is allocated in audit engagements, with improved detection and potential efficiency gains among the reported outcomes.

The academic literature, however, shows important nuance: while many ML/DL models demonstrate high performance in narrowly scoped financial or payment fraud tasks (for example, credit-card and banking datasets), these successes do not automatically translate into robust, generalizable results for public finance audits. Systematic reviews of fraud-detection research highlight common methodological concerns severe class imbalance, lack of representative public-sector datasets, evaluation on closed or synthetic datasets, and inconsistent performance metrics that complicate cross-study comparisons and practical adoption in governmental auditing contexts (Btoush et al., 2023).

In the public-sector domain, researchers have adapted unsupervised anomaly detection and network-analysis techniques to procurement and budgeting datasets to identify favoritism, collusion, and atypical contracting patterns. Case studies using the Open Contracting Data Standard (OCDS) and procurement corpora demonstrate promising detection rates (e.g., isolation-forest and graph-based approaches), but also underline reproducibility and validation gaps: many systems are validated against a limited set of known anomalies or protests rather than broad, externally-verified instances of fraud (Niessen et al., 2020).

A recurring theme across audit-analytics research is that technology alone is insufficient. Continuous-auditing frameworks and analytics pipelines must be paired with audit process redesign, robust data governance, transparent model explainability, and auditor upskilling to realize the potential of AI in public finance oversight. Design and field evaluations of continuous data-level auditing systems show that population-level analytics can outperform sample testing, but only when audit procedures and decision rules are adapted to act on algorithmic signals (Rikhardsson & Dull, 2016).

This systematic review therefore asks not simply whether AI can detect fraud, but under what practical, methodological, and institutional conditions AI-powered fraud detection meaningfully improves public finance audit outcomes. The remainder of the paper will (1) map algorithmic approaches used in the literature, (2) evaluate evidence of detection accuracy and real-world effectiveness, and (3) synthesize challenges and recommendations for audit design, validation, and governance.

2. Literature Review

AI-powered fraud detection in public finance audits builds upon advances in machine learning (ML), data analytics, and anomaly detection, offering auditors tools to identify irregularities across large-scale, heterogeneous datasets. Early studies emphasized the capacity of supervised ML models, such as decision trees, random forests, and support vector machines, to classify fraudulent versus legitimate transactions when trained on labeled datasets (West & Bhattacharya, 2016). These methods show strong predictive accuracy in structured financial datasets but face challenges in the public sector due to class imbalance, scarce labeled fraud cases, and jurisdiction-specific data formats (Btoush et al., 2023).

Unsupervised approaches, including clustering, isolation forests, and autoencoders, have gained traction where labeled data are scarce, allowing detection of anomalous behavior in procurement, budget execution, and expenditure claims (Niessen et al., 2020; Stefánsson, 2023). Graph-based models have been used to uncover collusion and bid-rigging in contracting networks by analyzing relationships among suppliers and agencies (Lyra et al., 2022). However, reproducibility issues persist, as many models are evaluated on limited or proprietary datasets without external validation (Janvrin & Watson, 2017).

Deep learning, particularly recurrent and convolutional neural networks, has demonstrated effectiveness in unstructured data analysis, such as extracting relevant features from audit reports, contracts, and scanned invoices (Hajek & Henriques, 2017). Integrating natural language processing (NLP) into audit analytics enables semantic risk assessment, yet explainability and interpretability remain barriers to adoption in compliance-driven audit environments (Fedyk et al., 2022).

Several studies advocate embedding AI within continuous auditing frameworks, enabling near real-time transaction monitoring and exception reporting (Rikhardsson & Dull, 2016). Field experiments and pilot implementations suggest AI can enhance detection rates and efficiency, but success depends on integrating results into decision-making workflows, auditor training, and governance safeguards (Issa et al., 2016).

Overall, the literature underscores that while AI-powered fraud detection has achieved notable technical advances, its effectiveness in public finance audits hinges on overcoming data quality constraints, improving model transparency, and aligning technological capabilities with institutional audit processes. These factors define the gap between laboratory performance and sustained, real-world impact.

3. Methods

This study adopts a systematic literature review (SLR) approach to identify, evaluate, and synthesize peer-reviewed research on the use of artificial intelligence (AI) for fraud detection in public finance audits. The process began with formulating research questions focused on the effectiveness, methodologies, and implementation challenges of AI-powered fraud detection. Searches were conducted across major academic databases, including Scopus, Web of Science, IEEE Xplore, and Google Scholar, using combinations of keywords such as artificial intelligence, fraud detection, public finance, audit analytics, and machine learning. Reference lists of relevant articles were also examined to identify additional studies.

Inclusion criteria required that studies be peer-reviewed, published in reputable journals or conference proceedings, and directly address AI applications in fraud detection relevant to auditing or public finance contexts. Studies were excluded if they lacked empirical analysis, focused solely on private-sector contexts without clear transferability to public auditing, or provided only conceptual commentary without methodological detail. Selected studies were analyzed thematically to categorize AI techniques used, datasets applied, evaluation metrics, and reported implementation outcomes. The synthesis aimed to identify common strengths, limitations, and practical considerations for integrating AI into public finance audit workflows.

4. Results and Discussion

The systematic review reveals a varied landscape of AI-powered fraud detection methods in public finance auditing, characterized by evolving techniques, mixed data environments, and differing levels of real-world applicability. Supervised approaches such as random forests, support vector machines, and gradient boosting continue to show high accuracy when trained on well-labeled structured datasets (West & Bhattacharya, 2016). Yet, the rarity and sensitive nature of confirmed public-sector fraud cases undermine the feasibility of deploying such models at scale (Btoush et al., 2023).

Unsupervised and semi-supervised methods, including isolation forests, clustering, and autoencoders, have emerged as pragmatic alternatives in data-scarce environments. These techniques are particularly relevant for detecting anomalies in procurement, budgeting, and transaction records (Niessen et al., 2020; Stefánsson, 2023). For instance, network analysis applied to procurement data using the Open Contracting Data Standard (OCDS) highlights the potential for graph-based methods to expose collusion and irregular supplier behavior (Lyra et al., 2022). However, generalizability concerns persist, as many models are tested on limited or proprietary datasets without external validation (Janvrin & Watson, 2017).

Deep learning models such as convolutional and recurrent neural networks extend fraud detection into unstructured domains, including documents, contracts, and scanned invoices, extracting complex fraud-relevant features (Hajek & Henriques, 2017). Integration with natural language processing (NLP) enables semantic analysis of textual content, enriching risk assessments (Fedyk et al., 2022). Yet, the opacity of these models continues to challenge adoption; audit environments often require explainable outputs alongside technical performance.

Recent advances in explainable AI (XAI) introduce promising techniques that bolster transparency without sacrificing accuracy. A user-centered XAI framework combining ensemble learning with Shapley value explanations demonstrated both strong predictive performance and stakeholder-aligned interpretability in financial fraud detection systems (Zhou et al., 2023). Meanwhile, innovative hybrid approaches that leverage federated learning plus XAI tools like SHAP and LIME have been proposed to address privacy constraints while delivering interpretable results, critical in finance-driven contexts (Awosika et al., 2024).

Beyond the technology itself, institutional and contextual factors play a significant role. A recent systematic literature review of AI adoption and diffusion in public administration underscores how technology-organization-environment variables, including governance structures, absorptive capacity, ethical tensions, and data stewardship, critically influence AI implementation in the public sector (Madan & Ashok, 2023).

Embedding AI within continuous auditing workflows, for near real-time anomaly monitoring, has shown improved detection efficiency and coverage compared to traditional sample-based methods (Rikhardsson & Dull, 2016; Issa et al., 2016). However, these benefits depend on integrating algorithmic outputs into audit decision-making, ensuring robust data governance, and investing in auditor training to interpret and act on AI signals (Appelbaum et al., 2017).

In sum, the literature suggests substantial promise for AI-powered fraud detection in enhancing public finance audits provided technical, data, and institutional challenges are met. Technical hurdles include scarcity of labeled data, model transparency, and cross-context validation. Institutional readiness requires adapting audit procedures, strengthening data infrastructure, and building auditor capacity. The synergy of robust AI models and responsible governance represents the path forward.

Future research should emphasize hybrid systems combining rule-based logic with anomaly detection, refine XAI techniques tailored to auditing, and pilot deployment in diverse public audit institutions. Creating shared anonymized datasets could facilitate benchmarking, cross-context learning, and help translate academic potential into sustained, real-world audit effectiveness.

5. Conclusion

This systematic review finds that AI-powered fraud detection holds significant potential to improve the efficiency, accuracy, and scope of public finance audits. Advances in supervised, unsupervised, and deep learning techniques have expanded the ability to identify both known and emerging fraud patterns, even in data-scarce environments. The integration of natural language processing and network analysis further strengthens the capacity to detect anomalies in unstructured and interconnected datasets. However, the promise of these technologies can only be realized if they are paired with robust governance frameworks, high-quality data, and mechanisms to ensure explainability and transparency in decision-making.

Despite notable progress, persistent challenges remain. Data scarcity, lack of model interpretability, and limited cross-jurisdiction validation constrain the operationalization of AI tools in public audit contexts. Institutional readiness, including technical capacity, data stewardship, and auditor training, emerges as a decisive factor in determining adoption success. Moreover, without careful design, AI adoption risks perpetuating existing biases or creating new vulnerabilities in fiscal oversight systems.

Looking ahead, sustained progress will depend on fostering collaboration between public audit institutions, policymakers, and researchers to develop hybrid fraud detection systems that combine statistical rigor with domain expertise. Building anonymized, shared datasets could accelerate model validation and enable context-specific refinements. Ultimately, embedding AI tools into the broader accountability framework, grounded in transparency, ethics, and public trust, will be key to ensuring that these technologies strengthen, rather than undermine, fiscal governance.

References

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1-27.

Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection. IEEE access, 12, 64551-64560.

Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science, 9, e1278.

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process?. Review of Accounting Studies, 27(3), 938-985.

Hajek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud–A comparative study of machine learning methods. Knowledge-Based Systems, 128, 139-152.

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of emerging technologies in accounting, 13(2), 1-20.

Janvrin, D. J., & Watson, M. W. (2017). "Big Data": A new twist to accounting. Journal of Accounting Education, 38, 3-8.

Lyra, M. S., Damásio, B., Pinheiro, F. L., & Bacao, F. (2022). Fraud, corruption, and collusion in public procurement activities, a systematic literature review on data-driven methods. Applied Network Science, 7(1), 83.

Madan, R., & Ashok, M. (2023). AI adoption and diffusion in public administration: A systematic literature review and future research agenda. Government Information Quarterly, 40(1), 101774.

Niessen, M. E. K., Paciello, J. M., & Fernandez, J. I. P. (2020). Anomaly detection in public procurements using the open contracting data standard. In 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 127-134). IEEE.

Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. International Journal of Accounting Information Systems, 20, 26-37.

Stefánsson, H. A. (2023). Unsupervised anomaly detection in financial transactions.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. Computers & security, 57, 47-66.

Zhou, Y., Li, H., Xiao, Z., & Qiu, J. (2023). A user-centered explainable artificial intelligence approach for financial fraud detection. Finance Research Letters, 58, 104309.

Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big data as complementary audit evidence. Accounting Horizons, 29(2), 431-438.