Intelligent Audit Systems: A Systematic Review of Fundamental Scientific Challenges

Raphael KPOGHOMOU* [1], David TCHOFFA [1], A.EL. MHAMEDI [1],
Alidor M. Mbayandjambe [2], Mamadi. Binko. TOURE [3]
[1]IUT de Montreuil – Université Paris 8, QUARTZ Laboratory, France
[2]Department of Mathematics, Statistics and Computer Science, University of Kinshasa, DR Congo
[3]Université Gamal Abdel Nasser de Conakry, Guinea

Corresponding author*: r.kpoghomou@iut.univ-paris8.fr

***Abstract*—The integration of Artificial Intelligence, Blockchain, and Process Mining into auditing systems promises improvements in automation, transparency, and analytical capability. However, fundamental scientific challenges remain unresolved. This paper presents a systematic literature review of 37 peer-reviewed studies (2023–2026) to identify three structural barriers limiting the development of truly intelligent audit systems: (1) the validity and probative value of digital traces, (2) the faithful reconstruction of real-world processes from imperfect logs, and (3) the detection of complex, rare, and adaptive deviations. Our analysis shows that despite advances in federated learning, deep learning–based anomaly detection, and blockchain audit trails, none fully addresses the foundational data validity problem. The classical "garbage in, garbage out" principle persists across all technological perspectives. Human expertise remains essential for contextual validation, and a persistent trade-off between predictive performance, explainability, and adaptability constrains all current approaches.**

***Index Terms*—Intelligent Audit Systems, Process Mining, Anomaly Detection, Concept Drift, Federated Learning, Blockchain Audit, Scientific Barriers, Explainable AI (XAI)**

I. Introduction

The rapid digitalization of enterprise systems has generated unprecedented growth in transactional data, event logs, and digital traces. Auditing is consequently evolving from a sampling-based, retrospective activity toward a continuous, data-driven practice in which automation and advanced analytics play a central role [1]–[3]. We define *intelligent audit systems* as socio-technical frameworks combining data collection, process analysis, anomaly detection, and human validation to support continuous or near-real-time auditing.

Despite rapid technological development, a central challenge remains unresolved: how can intelligent audit systems produce reliable conclusions when digital traces may be incomplete or biased, reconstructed models only partially reflect reality, and anomalous behaviors evolve over time? Machine learning demonstrates strong capabilities for large-scale fraud identification [4], [5]; blockchain offers immutable transaction records [6]; process mining enables workflow reconstruction for compliance verification [2]. Yet fraud detection models degrade under concept drift [5], blockchain does not guarantee initial data correctness [6], and process mining depends heavily on event log quality [7].

These observations motivate three *scientific barriers*: (1) validity and probative value of digital traces [8], [9]; (2) faithful reconstruction of real-world processes [10], [11]; (3) detection of complex, rare, and adaptive deviations [12], [13]. Our contribution is threefold: a structured analysis of persistent challenges (2023–2026); a cross-domain synthesis connecting AI, blockchain, and process mining; and architectural implications for robust, explainable, adaptive audit systems.

II. Background

A. AI in Auditing

Machine learning models analyze large volumes of financial data, identify unusual patterns, and assist auditors in fraud detection, enabling continuous monitoring beyond traditional sampling [1], [4], [5]. Broader benefits include reduced information asymmetry and improved audit efficiency [1]. However, effectiveness depends heavily on data quality, and many models lack transparency [14]. Concept drift and evolving fraud strategies further complicate deployment in production environments [12], [13].

B. Process Mining

Process mining reconstructs and analyzes real organizational processes from event logs, allowing auditors to move beyond isolated transactions [8], [9]. Conformance checking reveals deviations and supports compliance verification [7]. Logs are frequently incomplete, inconsistent, or distributed across systems, however, producing inaccurate models and requiring expert interpretation [10], [11], [15].

C. Blockchain Audit

Blockchain records transactions in an immutable distributed ledger, preserving audit trail integrity and reducing manipulation risk [2], [6]. Its key limitation is that immutability applies only after registration: incorrect or fraudulent data entered initially becomes permanently preserved [3]. Blockchain should therefore be viewed as a trace-securing mechanism, not a validating one.

This work has been carried out within the QUARTZ Laboratory (EA 7393), IUT de Montreuil, Université Paris 8, France.

III. Research Methodology

This study follows a systematic narrative review based on PRISMA 2020 guidelines [16], synthesizing research from Process Mining, Blockchain auditing, and AI-driven anomaly detection. The search was conducted between January and March 2026 across IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Web of Science, and MDPI. The temporal scope (2023–2026) captures the integration of large language models and federated learning into audit analytics, the emergence of the EU AI Act (Regulation 2024/1689), and recent empirical evidence on concept drift and adversarial robustness. Boolean queries combined terms such as "process mining AND audit", "blockchain AND auditing", "fraud detection AND machine learning", and "explainable AI AND process monitoring" (see Table I).

TABLE I
Search Keywords by Technological Domain

Domain	Keywords
Process Mining	process mining AND audit; event log AND compliance; conformance checking AND financial
Blockchain	blockchain AND auditing; immutability AND audit trail; smart contract AND compliance
AI / ML	fraud detection AND machine learning; anomaly detection AND deep learning; explainable AI AND process monitoring
Concept Drift	concept drift AND anomaly detection; streaming AND fraud; adaptive learning AND audit
Governance	human-in-the-loop AND audit; EU AI Act AND auditing; algorithmic accountability

The initial search returned 126 records. After removing 22 duplicates, 104 articles were screened on title and abstract; 48 were excluded for insufficient audit relevance. Of the 56 full-text articles assessed, 19 were excluded for insufficient methodological rigor or absence of peer review. The final corpus comprised **37 peer-reviewed studies**, evaluated against four criteria: methodological transparency, thematic relevance, source credibility, and analytical framing. Figure 1 presents the PRISMA 2020 flow diagram.

IV. Barrier 1: Validity and Probative Value of Digital Traces

The first barrier concerns whether digital traces constitute scientifically reliable and legally probative audit evidence. Werner et al. [8] show that process mining improves analytical coverage in financial audits, but only recorded transactions can be analyzed, making audit quality directly dependent on log completeness. Föhr et al. [9], [17] acknowledge that event logs rarely exist in ready-to-use form and must be reconstructed via SQL queries, introducing subjectivity. From a blockchain perspective, Zhang et al. [18] confirm that immutability prevents post-registration alteration but does not validate correctness at entry: errors or malicious inputs become permanently preserved. Combining blockchain with AI still requires extensive preprocessing, confirming that blockchain mitigates alteration risks without eliminating the "garbage in, garbage out" problem [19].

On the AI side, Lai [20] reports that AI reduces audit costs yet algorithmic opacity and manipulation risks persist. A systematic review of 83 publications identifies five major bias sources in AI auditing (data deficiencies, demographic bias, spurious correlations, improper comparators, and design-related cognitive biases), noting that explainability tools (SHAP, LIME) address model interpretation but not data provenance [21], [22]. Interviews with 22 audit professionals further identify transparency, algorithmic bias, and robustness as dominant AI adoption barriers [23]. Across all domains, no technology guarantees the initial validity of digital traces; human expertise remains indispensable for contextual validation.

V. Barrier 2: Faithful Reconstruction of Real-World Processes

The second barrier concerns the gap between discovered process models and operational reality. Silva et al. [10] reveal a critical fitness–precision paradox: the Inductive Miner achieves very high fitness (median 0.98) in agile environments while precision drops to 0.23, meaning the model generates behaviors never occurring in practice. This demonstrates that conformance metrics can conceal substantial structural overgeneralization. Zimmermann et al. [11] identify 23 challenges faced by process mining analysts, showing that model validation frequently relies on subjective expert interpretation with no universal reliability metrics. Schuster et al. [15] document that algorithms incorrectly infer parallelism between medically sequential activities, producing structurally misleading models, while Johannssen et al. [24] identify an explainability–performance–adaptability trade-off constraining model interpretability in dynamic environments.

Existing conformance metrics are therefore insufficient to guarantee faithful process reconstruction. As process flexibility increases, so do model complexity and uncertainty, requiring expert validation that limits the scalability of automated auditing.

VI. Barrier 3: Detection of Complex, Rare, and Adaptive Deviations

The third barrier concerns detecting behaviors that are rare, adaptive, and potentially adversarial. Al-Muqarm et al. [13] propose a hybrid framework addressing class imbalance, adversarial robustness, concept drift, and explainability simultaneously: recall improves from 35% to 85% and attack success rate drops from 35% to 5%, yet generalization to unseen adversarial strategies remains limited. Baesens et al. [12] introduce a Human-in-the-Loop framework for evolving fraud patterns; continuous learning improves adaptability but vulnerability to novel attack vectors persists. Ghorbanali et al. [25] observe substantial AUC degradation (>0.2) under concept drift, particularly for local anomalies, and even adaptive models struggle to maintain stable performance across dynamic distributions [26], [27]. Oliveira et al. [28] demonstrate that different explainability techniques may produce contradictory explanations for identical predictions.

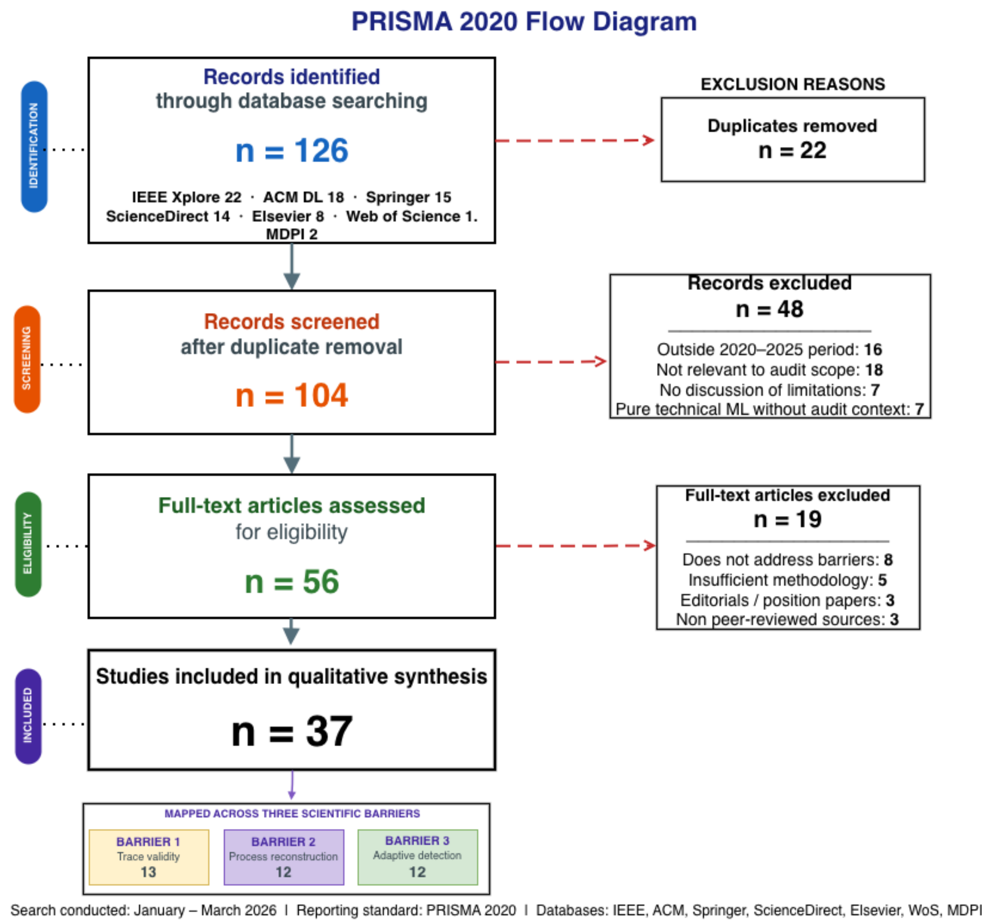

Fig. 1. PRISMA 2020 flow diagram illustrating the systematic literature selection process.

The literature reveals a structural trilemma: improving predictive performance often reduces interpretability; increasing explainability may constrain adaptability; adaptive mechanisms may introduce instability under adversarial pressure. No current approach simultaneously guarantees robust detection across all three dimensions.

A. Cross-Domain Synthesis

Table II summarizes findings across the three barriers. All three technologies encounter similar structural limitations: Process Mining depends on log reliability, Blockchain ensures immutability but not initial correctness, and AI relies on training data quality. The three barriers reflect not isolated weaknesses but deeper structural dependencies that, together, define the minimum scientific foundation for a reliable intelligent audit system.

The barriers emerge inductively from recurring limitations across all reviewed domains. Barrier 1 is foundational: all downstream reasoning depends on trace quality, and incomplete or manipulated data undermines even sophisticated analytical systems. Barrier 2 reflects that auditing requires understanding actual process execution, yet event logs provide only partial representations of operational reality. Barrier 3 acknowledges that fraud patterns are sparse, heterogeneous, and evolving, requiring simultaneous management of class imbalance, concept drift, adversarial strategies, and explainability constraints. Together, these three barriers define the minimum scientific foundation for a truly intelligent, reliable, and trustworthy audit system.

The choice to study these three technologies together is deliberate. AI provides advanced detection for hidden patterns and rare fraud scenarios in large-scale data. Process Mining contributes a process-oriented perspective essential for assessing compliance within real workflow execution. Blockchain strengthens trace integrity through immutability and distributed traceability, without guaranteeing initial data correctness. Together, they address three complementary audit dimensions: analytical detection, operational process understanding, and trace integrity, enabling identification of structural limitations that persist despite their apparent complementarity.

VII. Proposed Intelligent Audit Architecture

Figure 2 presents a four-layer architecture designed to address the three barriers through a sequential, feedback-enabled pipeline. The evolution from rule-based compliance engines to AI-driven adaptive architectures introduces structural challenges related to scalability, reliability, and epistemic

TABLE II
TABLE I: CROSS-SYNTHESIS OF THE THREE SCIENTIFIC BARRIERS

SCIENTIFIC BARRIER 1 – Validity and Probative Value of Digital Traces				
Dimension	**Process Mining**	**Blockchain**	**Artificial Intelligence**	**Conclusion**
Representative Works	Föhr (2025), Kamdjoug (2024)	Qader (2024), Shevchuk (2025)	Shivram (2024), Nguyen (2025), Sultan (2026)	Cross-technology limitation
Focus	Log-based audit reconstruction	Immutability and transparency	Automated anomaly detection	Data-centric dependency
Critical Limitation	Manual log extraction and preprocessing bias	GIGO principle; errors preserved immutably	Model opacity; dependence on training data quality	No guarantee of initial trace validity
GIGO Resolved?	NO	NO	NO	Unresolved structural issue
SCIENTIFIC BARRIER 2 – Faithful Reconstruction of Real-World Processes				
Dimension	**Silva (2025)**	**Zimmermann (2024)**	**Schuster (2024)**	**Johannssen (2025)**
Context	Agile software processes	PM analyst challenges	Healthcare process mining	AI-based statistical monitoring
Key Issue	Fitness–precision paradox	Subjective model validation	Sequentiality loss	Explainability–performance–adaptation tension
Quantitative Result	0.98 fitness / 0.23 precision	23 structural challenges	Model distortion risks	XAI gap in monitoring systems
Human Validation Required?	YES	YES	YES	YES
SCIENTIFIC BARRIER 3 – Rare, Adaptive and Adversarial Deviations				
Metric	**Al-Muqarm (2025)**	**Baesens (2024)**	**Ghorbanali (2024)**	**Angel (2026) / Nguyen (2025)**
Fraud Recall	35% $\rightarrow$ 85%	Not reported	N/A	Improved detection reported
Attack Success Rate	35% $\rightarrow$ 5%	Not addressed	N/A	Not quantified
Generalization to Novel Threats	LIMITED	NOT PROVEN	MISSING	UNCERTAIN
Core Structural Issue	Adversarial adaptation	Drift complexity	Performance degradation under streaming	ML instability and regulatory concerns

robustness. Contemporary systems integrating Process Mining [29], blockchain logging [18], and ML-based detection [12] amplify dependency on data pipelines and automated learning, increasing sensitivity to concept drift, adversarial manipulation, and data inconsistencies, which motivates an architecture that addresses these challenges holistically. Hybrid architectures combining statistical monitoring, deep learning, and explainable modules show improved adaptability over classical methods [24], and embedding explainability at design stage rather than post-hoc improves transparency and compliance with emerging regulatory frameworks [30].

Layer 1 – Data Validation and Trace Integrity: Raw ERP event logs undergo structured validation checking completeness (missing timestamps, orphan cases), logical consistency, cross-system reconciliation, and duplicate detection. Filtering inconsistent or manipulated traces prior to model ingestion directly addresses Barrier 1.

Layer 2 – Hybrid Process Reconstruction: Validated logs are processed using procedural discovery (Inductive Miner) combined with declarative constraints. Conformance checking quantifies deviations while limiting over-generalized behaviors, mitigating the fitness–precision paradox (Barrier 2).

Layer 3 – Adaptive Anomaly Detection: Given severe class imbalance typical of financial fraud (below 1%), the detection engine integrates supervised learning (gradient boosting) with density-based anomaly scoring (Local Outlier Factor). Concept drift detectors such as ADWIN monitor distribution shifts in streaming environments, while adversarial robustness testing evaluates stability under perturbations (Barrier 3).

Layer 4 – Explainability and Human-in-the-Loop: Feature attribution (SHAP) combined with rule-based violation summaries provides transparent explanations for flagged cases. Expert feedback is reintegrated into model updates, establishing a controlled learning cycle balancing performance and accountability.

The architecture is implementable using PM4Py (process mining), Scikit-learn or PyOD (classification and anomaly detection), River (drift monitoring), and SHAP (explainability) [22], [28], [31]. Evaluation combines classification metrics (precision, recall, F1-score, ROC-AUC) with process mining metrics (fitness and precision). Expected gains include improved audit coverage, detection recall under drift, and interpretability of anomaly explanations. From a governance perspective, integration of explainability and human oversight enhances regulatory compliance with the EU AI Act. Graph-based representations, temporal embeddings, and object-centric process features improve detection sensitivity beyond traditional transactional attributes [32]. Federated feature learning [33] further offers promising directions for improving detection sensitivity while preserving data confidentiality across institutional boundaries. The primary contribution lies not only in predictive accuracy, but in epistemic robustness and accountable automation.

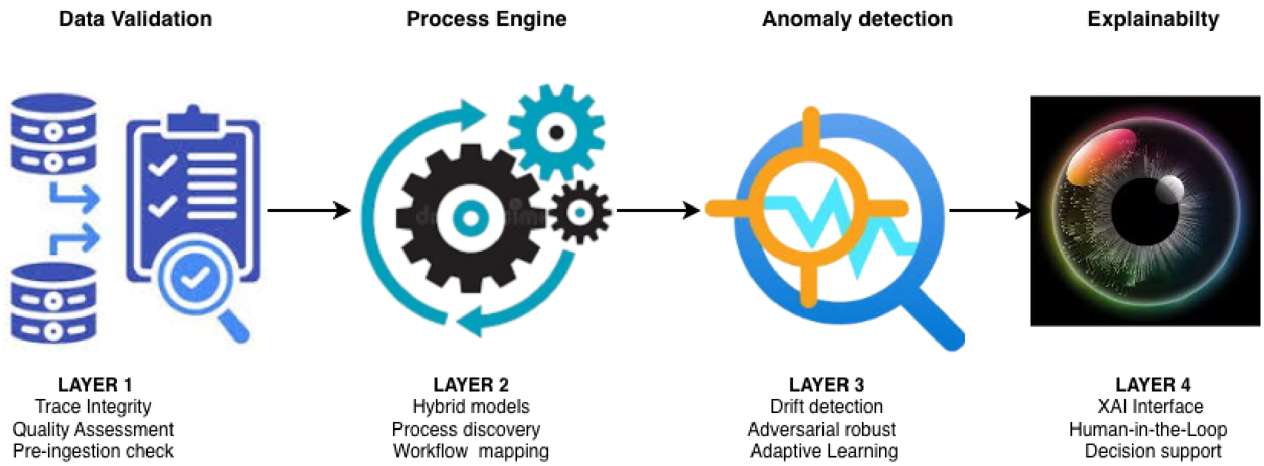

Fig. 2. Proposed four-layer intelligent audit architecture integrating trace validation, hybrid process reconstruction, adaptive anomaly detection, and explainable human-in-the-loop oversight.

VIII. Discussion

The synthesis of three barriers reveals a structural convergence transcending technological domains: no current approach, whether process mining, blockchain, or AI-based detection, resolves the foundational tension between automation and evidentiary validity.

A. Regulatory Pressure and the EU AI Act

The EU AI Act (Regulation 2024/1689) constitutes a pivotal regulatory development for intelligent audit systems [34]. Financial fraud detection and audit automation fall within the high-risk category (Annex III), imposing requirements on data governance, transparency, human oversight, and post-deployment monitoring, thereby directly reinforcing all three barriers: data quality mandates address Barrier 1, conformance documentation relates to Barrier 2, and explainability requirements correspond to Barrier 3 [35]. Resolving scientific barriers is therefore no longer merely academic, as systems failing to document data provenance, explain predictions, or demonstrate distributional robustness face penalties reaching 7% of global annual turnover.

B. The Unstructured Data Gap

Most reviewed studies focus on structured event logs, largely excluding the semi-structured and unstructured information prevalent in enterprise ecosystems, such as management narratives, audit opinions, contracts, and regulatory disclosures. NLP and large language models offer promising integration paths but amplify Barrier 1: textual audit evidence raises additional epistemological challenges beyond structured logs, including semantic ambiguity, jurisdictional variation in financial language, and LLM output opacity. Dedicated validation frameworks beyond standard process mining quality metrics are therefore required.

C. Algorithmic Accountability and Human Oversight

The persistence of human indispensability across all three barriers reflects a structural reality: validating audit evidence, interpreting discovered models, and judging anomaly significance require contextual expertise that automated systems cannot substitute. This aligns with the Human-in-the-Loop (HITL) governance paradigm, positioning human judgment as a constitutive element of accountable AI [36]. The proposed architecture operationalizes this principle in Layer 4. Nevertheless, scaling HITL mechanisms to high-volume, real-time conditions remains an open research challenge; structured escalation protocols, where automated systems handle routine cases and experts review uncertain instances, represent a promising direction.

D. Toward a New Research Agenda

The three barriers collectively suggest a reorientation beyond incremental performance gains on benchmarks. Future work should prioritize: (1) formal frameworks for assessing the epistemic reliability of digital audit traces, analogous to legal chain-of-custody requirements; (2) hybrid discovery algorithms incorporating declarative process knowledge to constrain overgeneralization; and (3) evaluation protocols integrating adversarial robustness, concept drift resilience, and explainability consistency into unified benchmarks [37]. Progress requires interdisciplinary collaboration among computer scientists, accounting researchers, legal scholars, and organizational theorists, as the scientific legitimacy of intelligent audit systems ultimately depends on epistemological rigor that no single discipline can address alone.

IX. Conclusion and Future Works

This paper identified three fundamental scientific barriers limiting the development of intelligent audit systems through a systematic review of 37 peer-reviewed studies spanning Process Mining, Blockchain, and AI-based anomaly detection.

First, the validity and probative value of digital traces remain uncertain: technologies can process and secure data but cannot guarantee correctness at source. Second, reconstructing real-world processes from execution logs does not always ensure faithful representation, particularly in dynamic environments. Third, detecting rare, adaptive, and adversarial deviations remains difficult due to concept drift, class imbalance, and explainability constraints.

These findings confirm that intelligent audit systems must not pursue full automation without safeguards. Human oversight, data validation, and explainability must remain central architectural components. Future research should focus on formal data validation frameworks, stronger adaptive detection mechanisms, and more consistent explainability methods, which collectively represent the essential foundations for audit systems that are reliable, transparent, and suitable for real-world governance. Achieving this requires sustained interdisciplinary collaboration among computer scientists, accounting researchers, legal scholars, and organizational theorists, since the scientific legitimacy of intelligent audit systems depends on epistemological rigor that no single discipline can provide alone.

REFERENCES

[1] K. S. Qader and K. Cek, "Influence of blockchain and artificial intelligence on audit quality: Evidence from turkey," *Heliyon*, vol. 10, p. e30166, 2024.

[2] V. Shivram, "Auditing with ai: A theoretical framework for enhanced anomaly detection, process mining and blockchain integration," *Journal of Information, Communication and Ethics in Society*, 2024.

[3] A. Sayal, "Optimizing audit processes through open innovation: integrating ai, blockchain, and data analytics," *International Journal of Accounting and Information Management*, vol. 43, pp. 1–20, 2025.

[4] C. Nguyen Thanh, "Predicting financial report fraud by machine learning," *Cogent Economics & Finance*, vol. 13, p. 2510556, 2025.

[5] I. I. Esmeralda and N. H. K. Fadhilah, "Fraud detection and machine learning in auditing: A systematic literature review," *Educational Studies and Research Journal*, vol. 3, no. 1, pp. 37–46, 2026.

[6] R. Shevchuk, "Anomaly detection in blockchain: A systematic review of methods and challenges," *Applied Sciences*, vol. 15, no. 15, p. 8330, 2025.

[7] J. R. K. Kamdjoug, H. D. Sando, J. R. Kala, A. O. Teutio, S. Tiwari, and S. F. Wamba, "Data analytics-based auditing: a case study of fraud detection in the banking context," *Annals of Operations Research*, vol. 340, pp. 1161–1188, 2024.

[8] M. Werner, M. Wiese, and A. Maas, "Embedding process mining into financial statement audits," *International Journal of Accounting Information Systems*, vol. 41, p. 100514, 2021.

[9] T. L. Föhr *et al.*, "Advancing process mining in auditing: An apm framework," *International Journal of Accounting Information Systems*, vol. 56, p. 100727, 2025.

[10] K. O. A. Silva *et al.*, "Discovering rules for agile software development with process mining," *Information and Software Technology*, vol. 181, p. 107680, 2025.

[11] L. Zimmermann *et al.*, "What makes life for process mining analysts difficult?" *Software and Systems Modeling*, vol. 23, 2024.

[12] B. Baesens *et al.*, "Concept drift in fraud detection," *Decision Support Systems*, vol. 173, p. 113974, 2024.

[13] A. Al-Muqarm *et al.*, "Robust ai for financial fraud detection in the gcc," *Ingeniare*, vol. 20, no. 2, 2025.

[14] S. H. M. Sultan, "Enhancing audit effectiveness through machine learning and deep learning techniques," *Audit and Finance Review*, 2026.

[15] D. Schuster *et al.*, "Analyzing healthcare processes with incremental process discovery," *Journal of Healthcare Informatics Research*, vol. 8, 2024.

[16] S. K. Kasereka, A. M. Mbayandjambe, I. G. Bazie, H. F. Zeufack, O. V. Ocama, E. Hassan, K. Kyamakya, and T. Tashev, "From iot to aiot: Evolving agricultural systems through intelligent connectivity in low-income countries," *Future Internet*, vol. 18, no. 2, 2026. [Online]. Available: https://www.mdpi.com/1999-5903/18/2/82

[17] T. Föhr, M. Jans, and J. Vanthienen, "Audit process mining: A systematic literature review and research agenda," *International Journal of Accounting Information Systems*, vol. 49, p. 100617, 2023.

[18] Y. Zhang, Z. Ma, and J. Meng, "Auditing in the blockchain: a literature review," *Frontiers in Blockchain*, vol. 2, p. 1549729, 2025.

[19] N. Rajpal and D. Rai, "Blockchain-ai based intrusion detection," *Sustainable Computing*, vol. 47, p. 101178, 2025.

[20] J. Lai, "Ai applications and audit fees: An empirical study," *International Review of Economics and Finance*, vol. 103, p. 104421, 2025.

[21] W. Murikah, J. K. Nthenge, and F. M. Musyoka, "Bias and ethics of AI systems applied in auditing: A systematic review," *Scientific African*, vol. 25, p. e02281, 2024.

[22] J. Cação *et al.*, "Explainable ai for data-driven process control," *Computers & Industrial Engineering*, vol. 204, p. 110869, 2025.

[23] J. Kokina, S. Blanchette, T. H. Davenport, and D. Pachamanova, "Challenges and opportunities for artificial intelligence in auditing: Evidence from the field," *International Journal of Accounting Information Systems*, vol. 56, p. 100734, 2025.

[24] A. Johannssen *et al.*, "Ai-based control charts for statistical process monitoring," *Computers & Industrial Engineering*, vol. 204, 2025.

[25] M. Ghorbanali *et al.*, "Revisiting streaming anomaly detection," *Artificial Intelligence Review*, 2024.

[26] F. Hinder, V. Vaquet, and B. Hammer, "One or two things we know about concept drift – a survey on monitoring in evolving environments," *Frontiers in Artificial Intelligence*, vol. 7, p. 1330257, 2024.

[27] Y. Cao, Y. Ma, Y. Zhu *et al.*, "Revisiting streaming anomaly detection: Benchmark and evaluation," *Artificial Intelligence Review*, vol. 58, p. 8, 2025.

[28] R. Oliveira *et al.*, "Explainable machine learning for defect detection in industrial processes," *Computers & Industrial Engineering*, vol. 192, p. 110214, 2024.

[29] H. K. Duan, M. A. Vasarhelyi, and M. Codesso, "Integrating process mining and machine learning for advanced internal control evaluation in auditing," *Journal of Information Systems*, vol. 39, no. 1, pp. 55–75, 2025.

[30] Y. Nugrahanti *et al.*, "Financial statement fraud detection through an integrated machine learning and explainable ai framework," *Journal of Risk and Financial Management*, vol. 19, no. 1, p. 13, 2025.

[31] C. Zhong and S. Goel, "Transparent ai in auditing through explainable ai," *Current Issues in Auditing*, vol. 18, no. 2, pp. A1–A14, 2024.

[32] A. Niro and M. Werner, "Detecting anomalous events in object-centric business processes via graph neural networks," *arXiv*, 2024. [Online]. Available: https://arxiv.org/abs/2403.00775

[33] S. Mashiko, Y. Kawamata, T. Nakayama, T. Sakurai, and Y. Okada, "Anomaly detection in double-entry bookkeeping data by federated learning system with non-model sharing approach," *arXiv*, 2025. [Online]. Available: https://arxiv.org/abs/2501.12723

[34] European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," Official Journal of the European Union, Tech. Rep. OJ L, 2024/1689, 2024.

[35] A. Mahmutovic, "The EU AI Act: A proactive framework for comprehensive AI regulation," *International Journal of Law and Information Technology*, vol. 33, p. eaaf028, 2025.

[36] V. Damen, M. Wiersma, G. Aydin *et al.*, "Explainable AI for EU AI Act compliance audits," *Maandblad voor Accountancy en Bedrijfseconomie*, vol. 99, no. 4, pp. 231–242, 2025.

[37] D. Hartmann, J. de Pereira *et al.*, "Addressing the regulatory gap: Moving towards an EU AI audit ecosystem beyond the AI Act by including civil society," *AI & Ethics*, 2025.