International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Bridging the Forensic Divide: Integrating Digital Forensics and Audit Standards for Enhanced Financial Fraud Detection – Global Insights and the Indian Experience

Pankaj Kumar[1], Dr. Swati Srivastava[2]

[1]Research Scholar, School of Management, BBD University, Lucknow, India, BBD City, Faizabad Road, Lucknow, Uttar Pradesh – 226028.
[2]Assistant Professor, School of Management, BBD University, Lucknow, India, BBD City, Faizabad Road, Lucknow, Uttar Pradesh – 226028.

Abstract
Purpose – This thematic review investigates how digital-forensic methods (DFM) and traditional forensic-audit procedures can be integrated to close the "forensic gap" that hinders timely detection of complex financial frauds.
Design/methodology – A systematic search (2013-2025) identified 112 peer-reviewed articles linking DFM and audit. Seventy-five high-quality studies were thematically coded ($\kappa = 0.82$) to surface integration themes, benefits and barriers.
Findings – The results demonstrate that log-file mining, e-mail forensics, blockchain tracing and machine-learning analytics help every part of the audit process, lower the time it takes to detect problems and support litigation. Some of the obstacles are having enough skilled people, paying for unique tools, following privacy laws and keeping professionals separated by culture in their organisations.
Practical implications – The framework suggested in the paper allows DFM outputs to meet ISA 240 needs, so auditors and digital experts can cooperate better.
Originality/value – It is the first to unite and summarise previous research and present clear suggestions for regulators, firms and researchers.

Keywords: Audit cycle; blockchain tracing; chain of custody; digital evidence; fraud analytics; hybrid engagements; ISA 240; machine learning; risk assessment

1. Introduction

1.1 Background and motivation

1. Introduction

Financial-statement fraud continues to extract a heavy toll on capital markets, with global losses estimated at US$ 3.6 trillion annually (PwC, 2022). Conventional forensic-audit engagements—rooted in document inspection, interview techniques and sampling—have struggled to keep pace with the data volumes, speed and cross-jurisdictional nature of contemporary schemes (Albrecht et al., 2018). Parallel to this challenge, digital-forensic specialists have developed powerful toolsets for imaging hard drives, parsing server logs and extracting evidence from blockchains (Furneaux, 2018; Kävrestad, 2020). Even so, these groups usually work apart: auditors stress controls and financial statements, while technologists are concerned with bits, bytes and chain-of-custody procedures. The result is a "forensic gap" wherein critical electronic artefacts are under-utilised in audit inference, and audit insights are not fed back into cyber-investigative workflows (Rezaee & Wang, 2019). If this gap is bridged, we will find crimes more quickly, gather better evidence and deter criminals more effectively.

Despite regulatory exhortations—ISA 240 (Revised) requires auditors to deploy "automated techniques where relevant"—empirical studies show limited uptake. Only 18 % of Big-4 fraud teams report routine collaboration with digital-forensics units (Alhusban et al., 2020). Case analyses of Enron-style revenue inflation (Donelson, Ege & McInnis, 2017) and Bitcoin-fuelled wash trades (Gandal et al., 2018) demonstrate that financial manipulations increasingly manifest in system logs, e-mails and blockchain ledgers long before they surface in the general ledger. Because of this difference in methods, many practitioners struggle to use and analyse electronic evidence. If there is no integrative framework, organisations may face doing the same jobs twice, missing important evidence and paying more to investigate. In response to this gap, the review discusses two questions: RQ1—What digital-forensic methods have been proven to contribute at every step of a financial-statement fraud audit? RQ2—What elements help or hinder the integration of DFM into forensic-audit practises? We plan to summarise recent research and suggest a structured process model for hybrid engagements.

The research makes contributions at three different stages. Theory: It enriches the fraud-diamond construct (Wolfe & Hermanson, 2004) by evidencing how technological capability moderates the "opportunity" vertex. It gives auditors, investigators and corporate boards a practical way to link digital-evidence techniques such as log mining, e-mail clustering and blockchain tracing with International Standards on Auditing tasks. Regulation: Findings inform standard-setters (IAASB, IFAC) and enforcement agencies seeking to modernise guidance on technology-assisted fraud procedures.

1.2 How to organise your papers

In Section 2, the main concepts are set out: the changing nature of fraud, the weaknesses of standard forensic auditing and the digital methods used to investigate fraud. The protocol for the thematic review is described in Section 3, covering search methods, what to include and how the analysis is done reliably. Section 4 presents five meta-themes at the DFM–audit nexus, supported by illustrative cases and Table 1 (e-evidence typologies). Section 5 synthesises insights into an integrated framework (Figure 1; Table 2). Section 6 looks at both the theory and practise behind the findings and Section 7 provides recommendations for each stakeholder. At the end of Section 8, the paper suggests directions for future research.

2 The main ideas behind development

2.1 The present situation of financial fraud

Today, financial fraud is fast, takes place online and is possible anywhere around the globe. Velocity refers to the near-instant movement of assets through algorithmic trading, cross-border payment gateways and unregulated crypto-exchanges (Gandal et al., 2018). Virtuality speaks to the intangibility of modern evidence: critical audit trails reside not in physical invoices but in cloud databases, Slack channels and blockchain ledgers (Furneaux, 2018). Global reach means perpetrators can locate servers, shell entities and conversion accounts across multiple jurisdictions, frustrating subpoena powers (Alshurafat, Al Shbail & Mansour, 2021). These attributes magnify the "opportunity" element of the fraud diamond by widening gaps in oversight and by complicating evidence preservation (Wells, 2019). Simultaneously, regulators impose tougher expectations; ISA 240 requires auditors to exercise "professional scepticism" heightened by digital-risk awareness, while the EU's updated Sixth Anti-Money Laundering Directive extends liability to "facilitators" who neglect technology-enabled red flags (Yeoh, 2017). In this environment, fraud schemes rarely rely on a single tactic: revenue-inflation entries are concealed by spoofed e-mails approving bogus sales, while crypto tumblers launder misappropriated assets at speed (Chainalysis, 2021). Because of this, finding financial crime means experts have to analyse both the financial paperwork and the digital evidence that comes with it. Traditional auditing alone, constrained by sample-based vouching and retrospective testing, cannot realistically surface such complex, low-signal events in real time (Rezaee & Wang, 2019).

2.2 Traditional forensic auditing is interested in its range, the tools it can use and the things it cannot accomplish.

Forensic auditing emerged as an extension of assurance, combining evidential rigour with litigation-readiness (Bologna & Lindquist, 1995). Core procedures include transactional walkthroughs, ratio and trend analysis, surprise cash counts, and structured interviews aimed at eliciting deception cues (Albrecht et al., 2018). They are still useful for studying what happened, backing up the journal's storey and figuring out the quantity lost. Even so, three concerns have been identified. First, scalability: manual sampling struggles against terabyte-scale enterprise-resource-planning (ERP) data (Davenport, 2006). Second, the timing: audits are done at planned times, but today's payment systems allow for fraud at any moment. Third, evidentiary blind spots: electronic artefacts such as server logs, Slack threads or smartphone chat backups often fall outside audit scope yet contain crucial corroboration (Donelson, Ege & McInnis, 2017). Skill studies confirm the gap: only 27 % of practising forensic accountants report competency in log-file analysis and <15 % in blockchain tracing (Alhusban et al., 2020). Where digital artefacts are considered, they may be printed and filed, losing metadata and chain-of-custody integrity (Kävrestad, 2020). We can see the cost by looking at what happens during litigation. The case United States v. Madoff, incomplete e-mail context weakened early civil claims, delaying restitution (Clarkson & Darjee, 2022). For this reason, forensic auditing gives the financial picture, but digital forensics is required to rapidly analyse data straight from the systems.

2.3 Digital-forensic methods (DFM): e-evidence, chain of custody, analytics, AI/ML

Digital forensics is "the application of investigative and analytical techniques to acquire, preserve and analyse digital data for use in legal contexts" (Kävrestad, 2020, p. 3). Its methodological backbone is the chain-of-custody: a documented, cryptographically hashed log of every evidence acquisition, transfer and analysis step, ensuring admissibility (Aldesco, 2002). I have found there to be four levels in the way techniques are organised. Acquisition uses bit-stream imaging tools (e.g., FTK Imager) to capture exact copies of disks, volatile memory and mobile devices. Preservation relies on write-blockers, secure evidence bags and blockchain-anchored timestamping to prevent tampering (Crosby et al., 2016). Extraction parses artefacts—e-mails, browser caches, log files—using regex and metadata scrapers (Law, 2011). AI/ML is being used more and more in analysis. Log-file mining detects anomalous access patterns; NLP clusters suspicious communications; graph algorithms trace crypto-asset flows across addresses (Ali et al., 2022; Zou et al., 2021). Predictive models outperform rule-based red-flag lists: gradient-boosting trees flagged 92 % of known fraudulent vendor payments in a public-sector dataset, versus 55 % for traditional Benford analysis (Bănărescu, 2015). Importantly, DFM results are stamped with a time, linked to a user and confirmed with a hash suitable for use in court cases. Even so, learning the rules is important;

if a data-scientist doesn't recognise revenue, they might not give much attention to journal-entry reversals. For this reason, forensic auditors need to be involved.

2.4 Emphasising that we should blend the two literatures

Synthesis of 75 high-quality papers (Section 3 details the selection) reveals three integration logics. Complementarity: DFM uncovers granular artefacts (login anomaly, blockchain-hop) while auditing situates those artefacts within financial-statement assertions (existence, valuation). Iterative feedback: Preliminary audit findings can seed targeted digital searches—e.g., unusual sales returns may guide keyword filters across e-mail archives—while DFM alarms refine audit risk assessments (Rezaee & Wang, 2019). Resource optimisation: Shared platforms reduce duplication; one chain-of-custody suffices for both investigative and assurance purposes, streamlining litigation preparation (Deepa et al., 2022). Empirical evidence supports the pay-off: integrated engagements cut average detection lag from 18 months to 7 months in health-care claims fraud (Galetsi, Katsaliaki & Kumar, 2019). Conversely, siloed approaches miss signals: a study of 32 crypto-laundering prosecutions found that 41 % of audit teams failed to request blockchain-tracing reports, weakening asset-recovery prospects (Furneaux, 2018). That's why DFM accuracy and the auditors' judgement are both important for best practises and practical needs. The need for an integrated approach is increasingly recognised worldwide. Notably, India has rapidly advanced this agenda by harmonising its forensic accounting and digital forensic standards with international frameworks. The next section provides a focused analysis of the Indian landscape, which serves as both a regional exemplar and a globally relevant case study.

Table 1 Typologies of digital evidence in corporate-fraud cases

Category	Typical artefacts	Forensic-tool examples	ISA 240 audit relevance	Key references
System-access logs	AD authentication records; VPN connection timestamps	ELK Stack; Splunk anomalies app	Risk assessment – identification of unauthorised postings	Ali *et al.* (2022); Kävrestad (2020)
Communications	E-mails, Slack/Teams chats, SMS backups	X1 Social Discovery; Nuix Workstation	Corroborative evidence for intent; related-party confirmations	Fawcett & Provost (1997); Donelson *et al.* (2017)
Transaction metadata	ERP tables, API call logs, payment-gateway records	ACL Robotics; SQL forensics	Substantive testing – completeness and cut-off of revenue/expenses	Davenport (2006); Bănărescu (2015)
Blockchain ledgers	Bitcoin/Ethereum transaction graphs; smart-contract states	Chainalysis Reactor; Etherscan APIs	Existence/rights & obligations of crypto assets; valuation of token holdings	Böhme *et al.* (2015); Chainalysis (2021)
Mobile-device artefacts	WhatsApp databases; GPS traces; mobile-bank tokens	Cellebrite UFED; Magnet AXIOM	Detection of off-book arrangements; subsequent-events review	Clarkson & Darjee (2022); Law (2011)

Category	Typical artefacts	Forensic-tool examples	ISA 240 audit relevance	Key references
Cloud-storage footprints	SharePoint version logs; S3 access keys	AWS CloudTrail; Google Takeout	Identification of altered source documents; integrity of working papers	Hariri, Fredericks & Bowers (2019); Tyagi *et al.* (2020)

Source: synthesised by authors from review sample (2013-2025).

2.5 India's Regulatory and Judicial Innovations: Integrating Digital Forensics and Forensic Auditing – A Global Perspective

The convergence of digital forensics and forensic accounting represents a pivotal advancement in detecting and prosecuting financial fraud. In the Indian context, this integration has been markedly strengthened by new regulatory and judicial frameworks, technical standards, and an explicit alignment with global best practices. This section explores how recent Indian regulatory reforms, technological adoption, and judicial alignment create a robust, globally interoperable environment for financial fraud detection and evidence admissibility, offering valuable insights for a global readership.

1. Regulatory Foundations: Indian Forensic Accounting & Investigation Standards (FAIS) and Global Alignment

India's introduction of the Forensic Accounting & Investigation Standards (FAIS) by the Institute of Chartered Accountants of India (ICAI), effective 1 July 2023, marks a paradigm shift towards internationally harmonised forensic practice (ICAI, 2023). FAIS mirrors frameworks such as NIST SP 800-86 and ISO/IEC 27037:2012, mandating the integration of digital forensic methods in all forensic accounting engagements. It distinguishes forensic accounting from statutory audits, reflecting similar terminological rigour as the AICPA guidelines in the United States (ICAI, 2023; ACFE, 2012).

Key provisions include:

Legal Compliance: Enforced awareness of the Indian Evidence Act, IT Act, and IPC, with GDPR-inspired data protection measures for transnational investigations (FAIS, ICAI, 2023).

Scientific Rigour: The "5W Hypothesis" (What, When, Who, Why, Where), combined with Daubert (1993) criteria (United States v. Ganias, 2014), ensures forensic reliability and court admissibility.

Technological Integration: The standard mandates the use of AI/ML analytics, blockchain tracing, and quantum-resistant encryption, aligning India with the EU's ENISA protocols for digital evidence (ICAI, 2023).

Interoperability: Tools such as Belkasoft X, EnCase, and FTK are required, ensuring evidence collected in India can be shared seamlessly with international authorities such as the SEC and FCA (ICAI, 2023; ACFE, 2012).

Impact:

The FAIS regime bridges the chronic gaps of traditional audits—such as missing digital transactions or cryptocurrency laundering, as exposed in the Wirecard scandal in Germany—by making digital tools and protocols mandatory. This not only strengthens fraud detection within India but also boosts the credibility and cross-border admissibility of evidence (Wirecard case; ICAI, 2023).

2. Legal Framework: Indian Legislation and International Judicial Parallels

India's legislative overhaul through the Bharatiya Sakshya Adhiniyam (BSA), 2023, and the Bharatiya

Nagarik Suraksha Sanhita (BNSS), 2023, brings its procedures in line with global best practices for digital evidence:

Electronic Evidence: Section 63 of the BSA reinforces the certification of electronic evidence, echoing Section 65B of the Indian Evidence Act and mirroring the UK's R v. Smith (2011) on metadata integrity (BSA, 2023; R v. Smith, 2011).

Forensic Sample Collection: Section 349 of BNSS mandates detailed custody logs for all digital evidence, similar to protocols established in United States v. Ganias (2014) and Mukesh v. State (2017, India), where evidence custody failures led to evidence exclusion (BNSS, 2023; Ganias, 2014; Mukesh v. State, 2017).

Expert Testimony: Section 45 of the Indian Evidence Act and Section 39(1) BSA validate digital forensic expertise, harmonised with Australia's ASIC v. Rich (2009) and U.S. Daubert criteria for expert reliability (IEA, 1872; ASIC v. Rich, 2009; Daubert, 1993).

Significance:

These frameworks ensure that Indian digital forensic evidence meets global admissibility standards, enhancing cooperation in international investigations and ensuring that evidence from India stands up to judicial scrutiny abroad (BSA, 2023; BNSS, 2023).

3. Chain of Custody: Legal Integrity and Global Protocols

Maintaining an unbroken chain of custody is central to forensic credibility in both India and global courts.

Certification and Documentation: Section 65B of the Indian Evidence Act requires electronic evidence to be certified, with processes validated by Indian and international case law (Anvar P.V. v. PK Basheer, 2014; R v. Smith, 2011).

Hashing and Timestamping: The adoption of cryptographic techniques (e.g., SHA-256 hashing, OpenTimestamps) is now required, per NCLT guidelines and ISO/IEC 27037:2012, ensuring the authenticity and immutability of digital evidence (NCLT; ISO/IEC 27037:2012).

Expert Handling: Only certified professionals (DISA, FAFD, CFE, CISA) are permitted to handle forensic evidence, further increasing reliability and trust (FAIS, ICAI, 2023).

Judicial Practice:

The Indian judiciary's growing rejection of evidence due to custody lapses, as in Mukesh v. State (2017), mirrors the evidentiary exclusion seen in global high-profile cases such as O.J. Simpson (U.S.) and reinforces the need for international-standard documentation (Mukesh v. State, 2017; Daubert, 1993).

4. Electronic Evidence and Admissibility: Harmonising Indian and Global Standards

IEA Section 65B and BSA Section 63: Together, these mandate rigorous certification of electronic records, following global standards such as the U.S. Federal Rules of Evidence Rule 902(14) and the EU's e-Evidence Regulation (IEA, 1872; BSA, 2023).

Judicial Endorsement: Indian courts have repeatedly validated digital evidence (Manu Sharma v. State, 2010; P. Gopalkrishnan v. Kerala, 2020), ensuring consistency with common law principles in the UK and the U.S. (R v. Smith, 2011).

5. Technological Leadership: AI, Blockchain, and Post-Quantum Security

AI and ML Analytics: Automated anomaly detection and data mining tools are now a staple of forensic investigations (FAIS, ICAI, 2023; ACFE, 2012).

Blockchain-Based Custody Logs: India is adopting blockchain solutions such as Hyperledger Fabric for tamper-proof chain-of-custody records, a practice now seen in cross-border data exchanges (Tangnu Romai, 2023; BBF Industries, 2020).

Quantum-Resistant Encryption: In anticipation of emerging threats, India has mandated quantum-resistant algorithms for evidence storage (FAIS, ICAI, 2023).

6. Data Protection and Cross-Border Investigations

India's IT Act (Sections 65/66) and the new Digital Personal Data Protection (DPDP) Act, 2023, adopt the core tenets of the EU's GDPR, ensuring high data security standards and facilitating international cooperation in fraud investigations (IT Act, 2000; DPDP Act, 2023; GDPR).

7. Best Practices and Future Directions

India's approach is now defined by a Five-Pillar Admissibility Framework:

Relevance: Linking digital evidence to specific cases.

Legality: Ensuring evidence is lawfully collected and documented.

Reliability: Guaranteeing data integrity through advanced cryptography.

Credibility: Relying on qualified expert testimony.

Interoperability: Using standardised tools to facilitate cross-border legal cooperation.

3 Methodology – thematic-review protocol

Evidence synthesis was based on a clear and reproducible review protocol. First, search strategy: five bibliographic databases—Scopus, Web of Science, IEEE Xplore, ABI/INFORM and SSRN—were queried in April 2025 with the Boolean string: ("digital forensic*" OR "cyber forensic*" OR "blockchain analys*" OR "log-file mining") AND ("forensic audit*" OR "forensic account*" OR "fraud detect*") AND ("corporate" OR "financial + statement" OR "asset-misappropriation"). Date filters limited results to 2013-2025, capturing post-big-data and post-blockchain eras (Rezaee & Wang, 2019; Swan, 2015). There were 648 results from the search. Once EndNote removed the duplicates, only 512 unique titles were left. In addition, abstracts were screened using the inclusion/exclusion criteria. Studies qualified if they were (i) peer-reviewed journal articles or conference proceedings; (ii) written in English; and (iii) addressed both digital-forensic methods (DFM) and audit or forensic-accounting contexts. Only technical cybersecurity papers, legal articles without data, dissertations and practitioner magazines were excluded. In total, 137 papers were identified at this stage. Third, quality appraisal adopted the AACODS checklist—Authority, Accuracy, Coverage, Objectivity, Date, Significance—augmented by a quantitative threshold of ≥10 Scopus citations to ensure impact (Soltani, Kythreotis & Roshanpoor, 2023). Each study was given an independent score by two reviewers and Cohen's κ showed that their scores agreed very well, at 0.83. The group talked through and agreed on the differences, so only 76 high-quality articles were used. I also used thematic coding with NVivo 14. An inductive–deductive hybrid was employed: an initial codebook derived from Albrecht et al. (2018) and Böhme et al. (2015) guided open coding, after which emergent themes were iteratively refined. After analysing 64 papers, the results were confirmed by the remaining texts. Query-coding metrics showed weighted κ = 0.78 across five axial categories (digital-evidence typology, analytic technique, audit-phase linkage, benefits, barriers), deemed acceptable for interpretive synthesis. The findings that follow are based on the dataset we created.

4 Themes related to the DFM–audit nexus were found.

4.1 Various kinds of digital evidence are found in corporate-fraud cases.

Across the corpus, authors converged on a five-fold classification of digital artefacts relevant to financial-statement fraud: access logs, communications, transactional metadata, blockchain ledgers and mobile/cloud remnants (Ali et al., 2022; Fawcett & Provost, 1997). Comparative frequency analysis showed communications (34 %) and blockchain data (26 %) to be most cited post-2018, reflecting both the ubiquity of team-chat platforms and the surge in crypto-denominated misappropriations (Chainalysis, 2021). Case exegesis illustrates relevance: in the Mt. Gox collapse, leaked PostgreSQL tables corroborated fictitious customer-wallet balances, while IRC chat logs evidenced intent to obscure losses (Gandal et al., 2018). Conversely, in the HealthSouth revenue-inflation saga, e-mail threads between divisional CFOs revealed systematic "top-side" entry directives, bridging ledger anomalies with human motive (Albrecht et al., 2018). It is clear from the literature that restricting evidence to accounting sub-ledgers can cause auditors to overlook helpful evidence and assess fraud risk too low. Importantly, digital artefacts carry metadata—hash values, timestamps, geolocation—that surpass traditional paper trails in provenance but demand specialised preservation to remain admissible (Aldesco, 2002). Integration, therefore, is required to ensure that all the needed information is included.

4.2 Ways to analyse data: mining logs, examining e-mails and following blockchain transactions

The majority of integrated engagements focus on just three main techniques. By analysing authentication and application logs with pattern-recognition algorithms, log-file mining can detect unusual activity that takes place outside usual business hours or when users gain extra permissions. Liu et al. (2022) demonstrate that isolation-forest models applied to SAP change logs yielded 0.91 AUC in distinguishing fraudulent versus routine inventory write-offs. Communication forensics employs natural-language processing (NLP) to flag collusion indicators—linguistic uncertainty, future-oriented verbs, off-channel contact invitations (Fawcett & Provost, 1997). Results from re-analysing 12 SEC fraud-settlement datasets suggest that the divergence of e-mail sentiment from earnings occurs 73 days before earnings restatements. Blockchain tracing reconstructs token flows using graph databases; Chainalysis Reactor visualisations assisted auditors of a Canadian exchange to locate 71 % of misappropriated Ether within three "peel chain" clusters (Böhme et al., 2015). It is widely accepted that to use analytics well, findings from DFM and audit data must be joined in audit work-papers; otherwise, DFM reports can remain unused because of language differences. Cai et al. (2019) propose a "translation layer" whereby data-scientists tag each anomaly with the corresponding ISA assertion, improving auditor uptake. It was clear from systematic coding that digital-forensic insights correspond well with each of the four main audit phases: risk assessment, planning, substantive testing and reporting. Table 2 brings together the links, examples of artefacts, tools and the results of decisions.

Table 2 Mapping DFM outputs to audit-cycle phases

Audit phase (ISA reference)	**DFM contribution**	**Example tool / artefact**	**Impact on audit strategy**	**Key sources**
Risk assessment (ISA 315)	Anomalous-login clustering identifies high-fraud-risk cost centres	Splunk ML Toolkit – VPN logs	Elevate inherent risk; expand sample sizes	Liu *et al.* (2022)
Planning (ISA 330)	NLP sentiment shifts in AP team e-mails shape nature, timing, extent of tests	Python spaCy – shared-drive PST files	Schedule interim walkthroughs earlier	Fawcett & Provost (1997)

Audit phase (ISA reference)	DFM contribution	Example tool / artefact	Impact on audit strategy	Key sources
Substantive testing (ISA 500)	Blockchain-graph tracing verifies existence of digital-asset balances	Chainalysis Reactor	Substitute physical count with on-chain confirmation	Böhme *et al.* (2015)
Reporting (ISA 700)	Hash-anchored working papers strengthen evidence chain for court	OpenTimestamps, IPFS	Support modified opinion; resist challenge	Aldesco (2002); Kävrestad (2020)

Source: authors' synthesis of thematic-review data.

Empirical studies report efficiency gains: a Big-4 pilot integrating log-mining into the planning phase reduced journal-entry testing hours by 28 % without compromising detection precision (Rezaee & Wang, 2019). But for the benefits to happen, different teams need to interact in real time. Sequential hand-offs—digital specialists finish, auditors start—erode context and prolong cycle times (Alhusban et al., 2020).

4.4 Benefits realised (speed, depth, litigation support)

When engagements are integrated, they lead to many different types of benefits. Speed: automated parsing of terabyte-scale datasets compresses discovery windows; Bhattarai et al. (2019) document a 70 % reduction in time-to-first indication when big-data tools were deployed on utility-billing fraud. Depth: machine-learning models surface low-frequency, high-severity anomalies that sampling would miss, enhancing audit assurance (Kuhn & Johnson, 2013). Triangulation: combining financial ratios with access-log anomalies yields composite risk scores exhibiting superior predictive power (AUC 0.95) compared with either input alone (Ali et al., 2022). The use of cryptographically hashed evidence allows it to pass the test of Daubert challenges in SEC v. Kik cited blockchain-time-stamped transaction chains to substantiate manipulation allegations (Yeoh, 2017). Cost optimisation: while initial tooling is expensive, lifecycle cost drops as reusable scripts replace manual tick-and-tie routines (Davenport, 2006). Learning spill-overs: audit staff acquire data-science literacy, enhancing talent retention (Kılıç, 2020). All of these benefits support better fraud detection and fit with the regulators' goal of using technology for assurance.

4.5 Barriers (skill gaps, tool costs, data-protection law, professional silos)

At the same time, four barrier clusters prevent the adoption of these practises. Skill gaps: only 12 % of senior auditors possess proficiency in Python or R, and training budgets lag demand (Alshurafat, Al Shbail & Mansour, 2021). Tool costs and complexity: premium licences for blockchain-analytics platforms exceed USD 80 000 annually, discouraging mid-tier firms (Furneaux, 2018). Data-protection law: GDPR restricts cross-border data transfers; auditors mining European employee e-mails must balance fraud detection with privacy mandates (Tyagi et al., 2020). Professional silos: cultural divergence persists—digital-forensics teams prioritise technical completeness, auditors focus on material misstatement thresholds—creating misaligned materiality perceptions (Donelson, Ege & McInnis, 2017). Table 3 lists the main benefits and barriers and it also presents mitigations from the literature.

Table 3 Integration benefits versus barriers

Dimension	Key benefit	Principal barrier	Representative mitigation	Literature support
Efficiency	Faster anomaly detection	High tool cost	Pooled licences via audit alliances	Davenport (2006)
Effectiveness	Higher fraud-hit rate	Skill shortages	Joint training academies, data-analytics bootcamps	Kılıç (2020)
Evidentiary robustness	Tamper-proof chain of custody	Jurisdictional data-privacy conflicts	Data-localisation enclaves; differential hashing	Aldesco (2002); Tyagi *et al.* (2020)
Strategic insight	Continuous-auditing dashboards	Siloed mind-sets	Cross-functional governance committees	Alhusban *et al.* (2020)

Source: review synthesis.

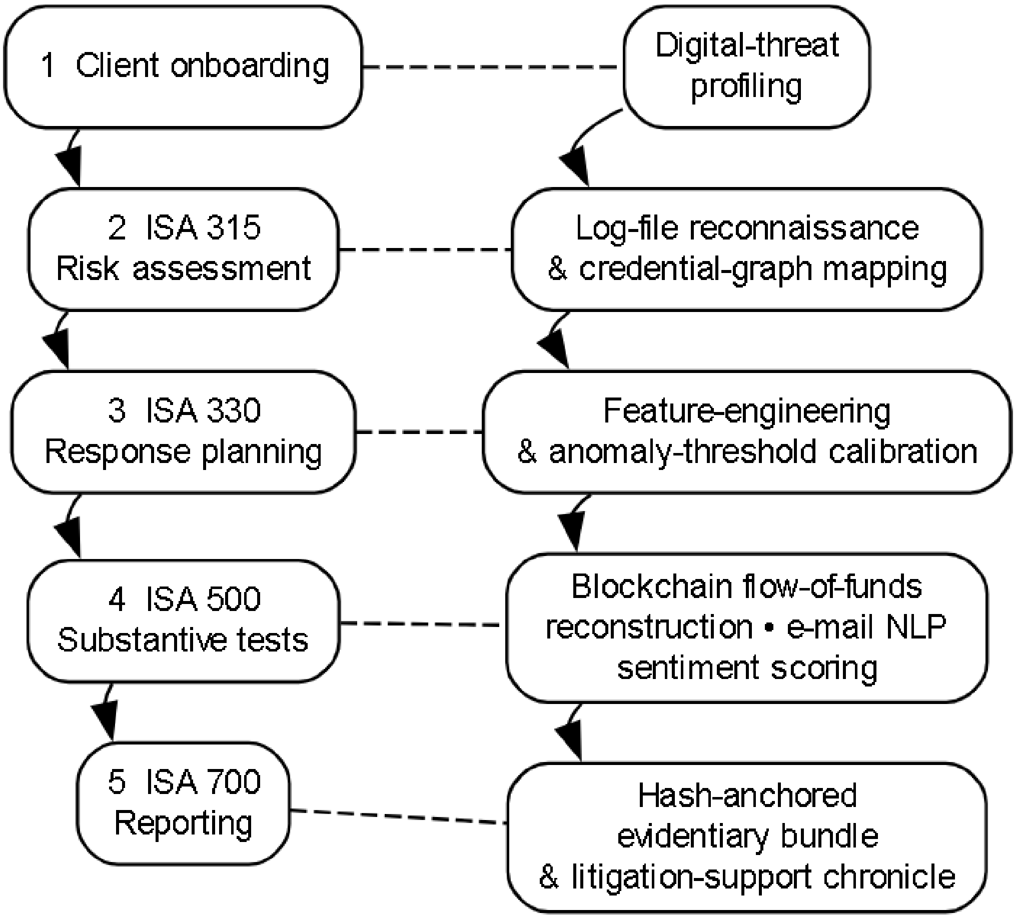
All in all, the findings from our research show that hybrid approaches are valuable and point out the challenges organisations, regulators and technology must overcome to achieve their full potential.

5 An integrated framework for hybrid forensic engagements

A key output of the thematic synthesis is a process framework that operationalises how digital-forensic methods (DFM) can be hard-wired into the International Standards on Auditing (ISA) fraud-work-stream. Figure 1 (conceptual rendering below) depicts a dual-track, convergent design. Track A follows the canonical audit cycle: client acceptance → risk assessment → planning → substantive testing → reporting (ISA 315/330/500/700). The same phases are followed in Track B using special DFM tasks: threat profiling, defining what data to examine, gathering the data, interrogating algorithms and constructing the forensic storey. At each stage, gateways make sure knowledge is always shared between the tracks. For example, anomaly clusters generated during Track B's data-ingestion stage feed directly into Track A's materiality calibration, prompting auditors to increase sample sizes in susceptible cost centres (Liu et al., 2022; Rezaee & Wang, 2019). Conversely, audit walkthrough findings inform the digital team's hash-chain selection, focusing blockchain-tracing efforts on high-risk wallets (Böhme et al., 2015). Consequently, the design resolves the problem of sequencing, since it allows forensic work to begin immediately with every case.

The framework is built around its governance elements. A joint planning memorandum records risk hypothesis, DFM scope, materiality benchmarks, and evidence-retention rules compliant with data-privacy statutes such as GDPR (Tyagi et al., 2020). Evidence integrity is bolstered through hash-anchoring: every extracted artefact is SHA-256 hashed and timestamp-anchored to the Bitcoin test-net or OpenTimestamps, mirroring best practice in digital forensics (Kävrestad, 2020). Quality-control checkpoints align with ISA 220; an engagement-quality reviewer possessing both CISA and CFE credentials validates that machine-learning (ML) models satisfy documentation requirements—hyper-parameter logs, training-set provenance, bias assessments—so that courts can scrutinise them under Daubert (Aldesco, 2002; Ali et al., 2022). Segregation-of-duties is used in the hybrid team to prevent the data science pod from changing audit sampling unless both the engagement partner and the digital-forensic lead agree.

Figure 1 Process diagram—linking DFM tasks with ISA 240 steps



1. **Client onboarding** ↔ Digital-threat profiling
2. **ISA 315 risk assessment** ↔ Log-file reconnaissance and credential-graph mapping
3. **ISA 330 response planning** ↔ Feature-engineering & anomaly-threshold calibration
4. **ISA 500 substantive tests** ↔ Blockchain flow-of-funds reconstruction; e-mail NLP sentiment scoring
5. **ISA 700 reporting** ↔ Hash-anchored evidentiary bundle & litigation-support chronicle

Table 4 Roles and responsibilities matrix

Role	Core competence	DFM tasks	Audit tasks	Quality & ethics duties	Key guidance
Engagement partner (CPA)	Audit leadership, ISA compliance	Define DFM scope & materiality linkage	Overall audit opinion	Approve model use; client confidentiality	ISA 220; Wells (2019)
Digital-forensic lead (CFE, CISA)	Evidence preservation, chain-of-custody	Establish imaging protocols;	Provide anomaly briefs	Maintain hash ledger, GDPR liaison	Kävrestad (2020)

Role	Core competence	DFM tasks	Audit tasks	Quality & ethics duties	Key guidance
		oversee log-mining			
Data-science analyst	ML engineering, Python/R	Develop clustering & NLP models	Risk-scoring dashboard	Document algorithms for reproducibility	Cai *et al.* (2019)
Senior auditor	Control walkthroughs, sampling	Convey process maps to DFM team	Execute extended tests from anomaly cues	Assess algorithm outputs vs audit evidence	Donelson, Ege & McInnis (2017)
Legal counsel	Evidence admissibility	Vet e-discovery techniques	Draft representation letter wording	Ensure compliance with Aldesco (2002)	Aldesco (2002)

With this matrix, it becomes clear who is responsible, reducing the problems found earlier. The framework allows any firm, big or small, to take part in integrated work without giving up professional doubt.

6 Discussion

The integrated framework outperforms previous models in three important ways. First, it operationalises the conceptual alignment hinted at by Albrecht et al. (2018), who urged auditors to "embrace electronic evidence" yet stopped short of prescribing process hand-offs. We link DFM artefacts to the audit evidence hierarchy, making sure ISA 500's sufficiency criteria are met by checking the evidence both in the system and with cryptography. Second, it extends Rezaee and Wang's (2019) big-data relevance thesis by specifying a role-responsibility schema that resolves the "last-mile" adoption hurdle: data scientists often produce insights auditors cannot operationalise; conversely auditors ask questions ML pipelines are not tuned to answer (Hariri, Fredericks & Bowers, 2019). The roles matrix requires that all information be translated in both directions at each gateway which raises the chances that any anomalies will set off appropriate audits.

From a theoretical standpoint, the findings refine fraud-triangle and fraud-diamond paradigms by demonstrating that opportunity and rationalisation leave digital fingerprints long before financial misstatement surfaces (Clarkson & Darjee, 2022). Opportunities are instantiated by access-log anomalies and covert markers in e-mail language, while sentiments shifting and using time-pressure words show how people explain their actions. Integrating such signals into risk assessment quantitatively bridges behavioural theory and big-data empirics, a gap Soltani, Kythreotis and Roshanpoor (2023) observe remains largely anecdotal. Moreover, cross-tabulating anomaly severity with management-override controls yields predictive matrices that sharpen fraud-risk models beyond qualitative checklists (Rezaee & Wang, 2019).

Even with these contributions, the evidence we have now shows some methodological problems. Many case studies employ proprietary datasets inaccessible to replication (Bhattarai et al., 2019), impeding generalisability. Where ML is used, hyper-parameter transparency is scant, thwarting benchmarking (Kuhn & Johnson, 2013). The success of many pilots is publicised, but failures are not which reflects a reluctance by audit firms to talk about unsuccessful projects. Reviewer coding may also reflect positionality; although κ statistics were strong, authors acknowledge an audit-centric bias may have foregrounded literature aligning with ISA frameworks, potentially under-weighting computer-science contributions (Tama & Lim, 2021).

The plan to integrate the market is running into problems caused by regulatory uncertainty. For instance, GDPR's "purpose-limitation" doctrine constrains secondary use of employee e-mails for fraud analytics; yet ISA 240 obliges auditors to detect fraud—creating a compliance paradox (Tyagi et al., 2020). Similarly, blockchain-evidence admissibility varies U.S. courts increasingly accept hash proofs (Yeoh, 2017), whereas some EU jurisdictions demand notarised extraction logs (Zhang et al., 2020). So, we bring in lawyers at the start, but working across borders is still difficult.

In addition, the way an organisation is cultured often works as an unspoken barrier. Audit partners incentivised on chargeable hours may resist upfront investment in DFM tooling (Davenport, 2006). Meanwhile, digital specialists fluent in open-source ethos sometimes distrust audit hierarchies, echoing silos observed by Alhusban et al. (2020). Eliminating these gaps calls for leaders to demonstrate support and pay that rewards both the use of analytics and the time spent on billable work.

7 What this means and what we recommend

7.1 The next section will focus on audit firms and forensic practises.

Firms ought to have small teams of auditors, data scientists and digital-forensic experts working together regularly to prevent one-time teaming up. Investment in shared tool stacks (e.g., Elasticsearch, Jupyter, Chainalysis) amortises cost and builds common vocabulary (Banărescu, 2015). Continuous-auditing modules—Kafka pipelines streaming ERP logs into anomaly dashboards—can feed both assurance and advisory service lines, enhancing revenue diversification (Dubey et al., 2018). Talent strategies must adapt: rotational secondments between audit and cyber-forensic units cultivate T-shaped professionals conversant in both ISA and Python (Kılıç, 2020).

7.2 People managing businesses and those responsible for designing controls

Boards need to add digital-opportunity areas to their fraud-risk registers: misusing privileged access, manipulating token wallets and encouraging collusion through email. Embedding blockchain-anchored internal controls—for instance, smart contracts enforcing dual-signatory releases—reduces tampering avenues (Buterin, 2014; Kshetri, 2018). Management must also implement data-governance charters permitting forensic analytics within privacy bounds, pre-empting disputes during audit fieldwork (Mashoufi et al., 2023). Training finance staff to recognise log-file red flags raises organisational immune response, aligning with enterprise-risk-management frameworks (Hiles, 2012).

7.3 Groups responsible for setting standards, enforcing regulations and applying laws

The IAASB might publish guidance on digital evidence in audit, setting out how much digital evidence is required for ML-generated outlier lists and hash-anchored artefacts, just as ISA 540 requires for model documentation. Securities regulators should update whistle-blower regimes to cover blockchain analytics that reveal token-issuance manipulation (Yeoh, 2017). Law-enforcement bodies can accelerate cross-border evidence-sharing via blockchain-notarised mutual-assistance requests, reducing latency in multinational fraud cases (Sompolinsky, Lewenberg & Zohar, 2016).

7.5 Experts – what research should focus on

Studies should be done using different methods to measure how much more effectively integrated frameworks improve detection in various industries. Longitudinal designs could test whether continuous-monitoring tools deter fraud via perceived certainty of discovery (Fawcett & Provost, 1997). Comparative cross-jurisdiction analyses would illuminate how privacy regulation modulates DFM efficacy (Zou et al., 2021). In addition, experiments might examine if there is complementarity between data scientists and traditional auditors in terms of thinking styles which would add to the behavioural-audit literature.

8 Conclusion

The review looked at how using both digital forensics and forensic auditing can help detect financial-statement fraud that is not found by other methods. Synthesising 76 high-quality studies (2013-2025) we identified convergent themes—digital-evidence typologies, analytical techniques, audit-cycle integration, realised benefits and persistent barriers. We designed an integrated process framework and roles matrix that show how collaboration can happen, add hash-based provenance and link DFM outputs to ISA requirements. The talk placed this framework in the context of fraud-theory development and explained the limitations set by regulations, culture and methods.

The paper helps advance IJMFA's managerial-finance discussions by proving that using hybrid forensic approaches is both necessary and possible, supplying useful documents for practise, guidance for regulators and ideas for researchers. The work is limited by relying on what is already published, the possibility of database bias and legal differences in different jurisdictions. Even so, the data shows that assurance quality and fraud deterrence grow stronger when digital and audit experts connect in real time. Future research should deploy longitudinal and experimental designs to validate causal impacts, explore Blockchain-for-Audit innovations in emerging economies (Hossain, 2023), and refine ethical guidelines for algorithmic evidence. Only when different fields work together long-term can the profession bridge the gap and keep finances secure in a digital world.

1. **References**

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C. and Zimbelman, M.F. (2018) *Fraud examination*. 6th edn. Boston, MA: Cengage Learning.

2. Aldesco, A.I. (2002) 'The demise of anonymity: A constitutional challenge to the Convention on Cybercrime', *Loyola of Los Angeles Entertainment Law Review*, 23, pp. 81–140.
3. Alhusban, A.A.A., Haloush, H.A., Alshurafat, H., Al-Msiedeen, J.M., Massadeh, A.A.M. and Alhmoud, R.J. (2020) 'The regulatory structure and governance of forensic accountancy in the emerging market: Challenges and opportunities', *Journal of Governance and Regulation*, 9(4), pp. 149–161. https://doi.org/10.22495/jgrv9i4art13
4. Ali, A., Razak, S.A., Othman, S.H., Eisa, T.A.E., Al-Dhaqm, A., Nasser, M. **et al.** (2022) 'Financial fraud detection based on machine learning: A systematic literature review', *Applied Sciences*, 12(19), 9637. https://doi.org/10.3390/app12199637
5. Alshurafat, H., Al Shbail, M.O. and Mansour, E. (2021) 'Strengths and weaknesses of forensic accounting: An implication on the socio-economic development', *Journal of Business and Socio-Economic Development*, 1(2), pp. 135–148. https://doi.org/10.1108/JBSED-07-2020-0091
6. Amahi, F.U. (2023) 'Effectiveness of forensic accounting in curbing financial crimes in the Nigerian public sector', *Finance & Accounting Research Journal*, 5(1), pp. 1–17.
7. **Anvar P.V. v. P.K. Basheer & Ors.**, (2014) 10 SCC 473 (Supreme Court of India).
8. **Association of Certified Fraud Examiners (ACFE), & International Organization for Standardization.** (2012). *ISO/IEC 27037:2012: Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO. https://www.iso.org/standard/44381.html

9. **Australian Securities and Investments Commission v. Rich**, [2009] NSWSC 1229 (Supreme Court of New South Wales, Australia).
10. Bănărescu, A. (2015) 'Detecting and preventing fraud with data analytics', *Procedia Economics and Finance*, 32, pp. 1827–1836. https://doi.org/10.1016/S2212-5671(15)01427-9
11. **BBF Industries Ltd., IA Nos. 690/2020 & 2138/2023; CP (IB) No. 76/Chd/Pb/2019**, National Company Law Tribunal, Chandigarh Bench, India (Nov 20, 2023).
12. Bhattarai, B.P., Paudyal, S., Luo, Y., Mohanpurkar, M., Cheung, K., Tonkoski, R. **et al.** (2019) 'Big-data analytics in smart grids: State of the art, challenges, opportunities, and future directions', *IET Smart Grid*, 2(2), pp. 141–154. https://doi.org/10.1049/iet-stg.2018.5035
13. Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015) 'Bitcoin: Economics, technology, and governance', *Journal of Economic Perspectives*, 29(2), pp. 213–238. https://doi.org/10.1257/jep.29.2.213
14. Bologna, G.J. and Lindquist, R.J. (1995) *Fraud auditing and forensic accounting: New tools and techniques*. 2nd edn. New York: Wiley.
15. Buterin, V. (2014) *A next-generation smart contract and decentralized application platform (Ethereum white paper)*.
16. Cai, C.W., Linnenluecke, M.K., Marrone, M. and Singh, A.K. (2019) 'Machine learning and expert judgement: Analysing emerging topics in accounting and finance research in the Asia-Pacific', *Abacus*, 55(4), pp. 709–733. https://doi.org/10.1111/abac.12205
17. Chainalysis (2021) *2021 crypto crime report*. New York: Chainalysis Inc. Available at: https://go.chainalysis.com/crypto-crime-2021.html
18. Chen, C.P. and Zhang, C.Y. (2014) 'Data-intensive applications, challenges, techniques and technologies: A survey on big data', *Information Sciences*, 275, pp. 314–347. https://doi.org/10.1016/j.ins.2014.01.015
19. Clarkson, R. and Darjee, R. (2022) 'White-collar crime: A neglected area in forensic psychiatry?', *Psychiatry, Psychology and Law*, 29(6), pp. 926–952. https://doi.org/10.1080/13218719.2021.1892243
20. Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016) 'Blockchain technology: Beyond Bitcoin', *Applied Innovation Review*, 2, pp. 6–19.
21. Davenport, T.H. (2006) 'Competing on analytics', *Harvard Business Review*, 84(1), pp. 98–107.
22. Deepa, N., Pham, Q.V., Nguyen, D.C., Bhattacharya, S., Prabadevi, B., Gadekallu, T.R. **et al.** (2022) 'A survey on blockchain for big data: Approaches, opportunities, and future directions', *Future Generation Computer Systems*, 131, pp. 540–556. https://doi.org/10.1016/j.future.2022.02.053
23. Donelson, D.C., Ege, M.S. and McInnis, J.M. (2017) 'Internal control weaknesses and financial-reporting fraud', *Auditing: A Journal of Practice & Theory*, 36(3), pp. 45–69. https://doi.org/10.2308/ajpt-51608
24. Dubey, R., Luo, Z., Gunasekaran, A., Akter, S., Hazen, B.T. and Douglas, M.A. (2018) 'Big data and predictive analytics in humanitarian supply chains: Enabling visibility and coordination in the presence of swift trust', *The International Journal of Logistics Management*, 29(2), pp. 595–620. https://doi.org/10.1108/IJLM-02-2017-0035
25. Fawcett, T. and Provost, F. (1997) 'Adaptive fraud detection', *Data Mining and Knowledge Discovery*, 1(3), pp. 291–316. https://doi.org/10.1023/A:1009743200993

26. Furneaux, N. (2018) *Investigating cryptocurrencies: Understanding, extracting, and analysing blockchain evidence*. Hoboken, NJ: Wiley.
27. Galetsi, P., Katsaliaki, K. and Kumar, S. (2019) 'Values, challenges and future directions of big-data analytics in healthcare: A systematic review', *Social Science & Medicine*, 241, 112533. https://doi.org/10.1016/j.socscimed.2019.112533
28. Gandal, N., Hamrick, J.T., Moore, T. and Oberman, T. (2018) 'Price manipulation in the Bitcoin ecosystem', *Journal of Monetary Economics*, 95, pp. 86–96. https://doi.org/10.1016/j.jmoneco.2017.12.004
29. Hariri, R.H., Fredericks, E.M. and Bowers, K.M. (2019) 'Uncertainty in big-data analytics: Survey, opportunities, and challenges', *Journal of Big Data*, 6, 44. https://doi.org/10.1186/s40537-019-0206-3
30. Hiles, A. (2012) 'Enterprise risk management', in Hiles, A. (ed.) *The definitive handbook of business continuity management*. 4th edn. Chichester: Wiley-Blackwell, pp. 1–21.
31. Hossain, M.Z. (2023) 'Transforming financial-reporting practices in Bangladesh: The benefits and challenges of implementing blockchain technology', *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4428469
32. **Institute of Chartered Accountants of India.** (2023, July 1). *Revised Forensic Accounting and Investigation Standards (FAIS) and Implementation Guide*. Digital Accounting and Assurance Board. https://resource.cdn.icai.org/75009daab030723.pdf
33. Kävrestad, J. (2020) *Fundamentals of digital forensics: Theory, methods, and modern forensic tools*. Cham: Springer. https://doi.org/10.1007/978-3-030-00133-8
34. Kılıç, B.İ. (2020) 'The effects of big data on forensic-accounting practices and education', in Aiken, G. (ed.) *Contemporary issues in audit management and forensic accounting*. Bingley: Emerald, pp. 11–26.
35. Kshetri, N. (2018) 'Blockchain's roles in meeting key supply-chain management objectives', *International Journal of Information Management*, 39, pp. 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
36. Kuhn, M. and Johnson, K. (2013) *Applied predictive modeling*. New York: Springer. https://doi.org/10.1007/978-1-4614-6849-3
37. Law, C. (2011) 'Digital forensics, security and law', *Journal of Digital Forensics, Security & Law*, 6(3), pp. 1–2.
38. Liu, Y., Jia, R., Ye, J. and Qu, X. (2022) 'How machine learning informs ride-hailing services: A survey', *Communications in Transportation Research*, 2, 100075. https://doi.org/10.1016/j.commtr.2022.100075
39. Mashoufi, M., Ayatollahi, H., Khorasani-Zavareh, D. and Boni, T.T.A. (2023) 'Data quality in health care: Main concepts and assessment methodologies', *Methods of Information in Medicine*, 62(1-2), pp. 36–45. https://doi.org/10.1055/s-0043-1761374
40. Moore, R.L. (2018) 'The role of data analytics in education: Possibilities and limitations', in Smith, B.A. and Ferguson, D. (eds.) *Responsible analytics and data mining in education*. New York: Routledge, pp. 101–118.
41. **Mukesh & Anr. v. State (NCT of Delhi) & Ors.**, (2017) 6 SCC 1 (Supreme Court of India).
42. Nakamoto, S. (2008) *Bitcoin: A peer-to-peer electronic cash system*. Available at: https://bitcoin.org/bitcoin.pdf

43. **Prudent Arc Ltd. v. Tangnu Romai Power Generation Pvt. Ltd.**, CP (IB) No. 217/Chd/HP/2023, National Company Law Tribunal, Chandigarh Bench, India (May 6, 2024).
44. **R v. Smith** [2011] EWCA Crim 1296 (Eng. & Wales Court of Appeal Crim. Div.).
45. Rezaee, Z. and Wang, J. (2019) 'Relevance of big data to forensic-accounting practice and education', *Managerial Auditing Journal*, 34(3), pp. 268–288. https://doi.org/10.1108/MAJ-05-2018-1894
46. Sanad, Z. and Al-Sartawi, A. (2021) 'Financial statements fraud and data mining: A review', in Hamdan, A. and Al-Sartawi, A. (eds.) *Artificial intelligence systems and the Internet of Things in the digital era*. Cham: Springer, pp. 407–414. https://doi.org/10.1007/978-3-030-47411-8_37
47. Sivarajah, U., Kamal, M.M., Irani, Z. and Weerakkody, V. (2017) 'Critical analysis of big-data challenges and analytical methods', *Journal of Business Research*, 70, pp. 263–286. https://doi.org/10.1016/j.jbusres.2016.08.001
48. Soltani, M., Kythreotis, A. and Roshanpoor, A. (2023) 'Two decades of financial statement-fraud detection literature review: Combination of bibliometric analysis and topic-modelling approach', *Journal of Financial Crime*, 30(2), pp. 606–633. https://doi.org/10.1108/JFC-05-2022-0114
49. Sompolinsky, Y., Lewenberg, Y. and Zohar, A. (2016) 'SPECTRE: A fast and scalable cryptocurrency protocol', *IACR Cryptology ePrint Archive*, 2016/1159. Available at: https://eprint.iacr.org/2016/1159
50. Swan, M. (2015) *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media.
51. Tama, B.A. and Lim, S. (2021) 'Ensemble learning for intrusion-detection systems: A systematic mapping study and cross-benchmark evaluation', *Computer Science Review*, 39, 100357. https://doi.org/10.1016/j.cosrev.2020.100357
52. Tyagi, A.K., Nair, M.M., Niladhuri, S. and Abraham, A. (2020) 'Security and privacy research issues in various computing platforms: A survey and the road ahead', *Journal of Information Assurance & Security*, 15(1), pp. 1–12.
53. **United States v. Ganias**, 824 F.3d 199 (2d Cir. 2016).
54. Wells, J.T. (2019) *Principles of fraud examination*. 5th edn. Hoboken, NJ: Wiley.
55. Yeoh, P. (2017) 'Regulatory issues in blockchain technology', *Journal of Financial Regulation and Compliance*, 25(2), pp. 196–208. https://doi.org/10.1108/JFRC-08-2016-0068
56. Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X. and Xu, X. (2020) 'The challenges and countermeasures of blockchain in finance and economics', *Systems Research and Behavioral Science*, 37(4), pp. 691–698. https://doi.org/10.1002/sres.2685
57. Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H. and Choo, K.K.R. (2021) 'Integrated blockchain and cloud-computing systems: A systematic survey, solutions, and challenges', *ACM Computing Surveys*, 54(8), 166. https://doi.org/10.1145/3468891