Applying Fraud and Forensic Accounting Investigation Criteria

Cheryl Ann Alexander[1,*] and Lidong Wang[2]

[1]*Institute for IT Innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA*

Abstract: Forensic accounting investigations apply criteria, such as analyzing financial records, detecting unusual entries, and proving fraud, to discover financial crimes, etc. This paper deals with applying fraud and forensic accounting investigation criteria. Advantages of building alignment between cyber forensics and accounting investigation are introduced. Fraud and forensic accounting investigation criteria, as well as relevant tools, are presented. A case study is provided, including forensic accounting in preventing fraud in financial reporting, financial accounting fraud detection based on data mining, forensic accounting based on business intelligence, and integrating big data into forensic accounting and reshaping the fraud detection process. Fraud and forensic accounting investigation criteria and relevant tools in healthcare are presented. Forensic accounting helps prevent fraud in financial reporting. The integration of big data into forensic accounting reshapes the fraud detection process. Forensic accounting can help with litigation, discover damage, and defend against healthcare fraud.

Keywords: Cyber forensics, Fraud detection, Forensic accounting, Big data, Data mining, Healthcare.

1. INTRODUCTION

Forensic accounting can be regarded as the financial equivalent of crime scene investigation. A forensic accountant can uncover financial misconduct by utilizing an analytical methodology and detailed financial information. Investigative models often follow one of two approaches. The first approach is the personal and behavioral characteristics of people with financial misconduct. The second one is based on numbers that investigate reported data for abnormalities. Given the advances in big data technologies, the two approaches can be merged [1].

Forensic accounting can be simplified to two competing concepts: perception and reality. It includes the following subfields [2]: 1) business valuation, 2) economic damage, 3) security and tax fraud, 4) bankruptcy and insolvency, and 5) computer forensics and electronic discovery. A forensic accounting investigation begins with a concern or allegation that a possible accounting irregularity exists and must be evaluated.So forensic accounting decides the following things[3]:1) whether or not the irregularity exists, 2) the irregularity's size or magnitude if it exists, and 3) how to fix the problem due to the irregularity.

Forensic accounting practices are divided into 1) investigative auditing, 2) criminal investigation, and 3) litigation support. The Beneish model and its application in forensic accounting were studied. The Beneish model is one of the methods that aim to detect accounting fraud. It enables a forensic accountant to systematically analyze a firm's financial statements and accounts. According to the Beneish model, the following variables have significant potential to detect financial statement frauds committed by a firm: 1) asset quality index; 2) leverage index; 3) depreciation index; 4) sales growth index; 5) gross margin index; 6) days' sales in receivables index; 7) sales, general, and administrative expenses index; and 8) total accruals to total assets [4].

The why, when, and who of the forensic accountants were studied. A decision to engage (or not) a forensic accountant will commonly be driven by the characteristics of a case (complexity and size) and the budget. The awareness and working knowledge of what makes a successful financial expert (requisite skills), what a court expects (ability to communicate), and why they fail (bias or inability to communicate) cannot be overstated [5].

There were challenges in forensic accounting during the COVID-19 pandemic, which resulted from business disruption, court closures, social distancing, etc. Remote work could disrupt workflow. Virtual interviews based on Zoom and other online meeting platforms were a poor substitute for the real thing. The lack of human contact due to COVID-19 was a major challenge [6].

It is necessary to combine forensic accounting technology with fraud detection due to the advances in intelligent technologies and cloud computing, which is also an important accounting and management issue. When a company's risks are identified and evaluated

*Address correspondence to this author at the Institute for IT Innovation and Smart Health, Mississippi, USA; E-mail: cannalexander68

by a fraud risk assessment (FRA) team, the risks should be prioritized, and an appropriate response to each risk should be given. There are four main risk responses: avoiding the risk, transferring the risk, mitigating the risk, and accepting the risk. The main types of financial and non-financial fraud that occurred in the 21st Century were studied to develop forensic procedures. The types of financial fraud include revenue recognition, expense deferral, risky investments, merger and acquisition abuses, and competitive analysis red flags. The types of non-financial fraud include poor control, risky products, insider share selling, CEO resignation, unethical practices, and Ponzi schemes [7].

Since whistle blowing is a crucial factor of organizational governance, it is significant to find features that lead auditors to select loyalty to the profession over allegiance to an individual in a team. The value of a contentious auditor was studied. The relationships among contentiousness, enjoyment of competition, and power distance were investigated. Results show that two competitiveness dimensions are considerably and divergently associated with whistle blowing likelihood, and power distance is negatively associated with whistleblowing [8].

There has been much published research work in fraud and forensic accounting investigation; however, less practical work has been published on the topic. The efforts in this paper are trying to fill the gap with a case study, including forensic accounting in preventing fraud in financial reporting, financial accounting fraud detection based on data mining, forensic accounting based on business intelligence, and integrating big data into forensic accounting and reshaping the fraud detection process.

2. ADVANTAGES OF BUILDING ALIGNMENT BETWEEN CYBER FORENSICS AND ACCOUNTING INVESTIGATION

Cyber forensics and forensic accounting are useful together for the investigation of financial fraud and other cybercrimes. Cyber forensics involves analyzing data from digital devices to uncover evidence of fraud, detecting anomalies in large data sets using artificial intelligence (AI)/machine learning (ML), tracing the origin and ownership of financial data, and recovering deleted or encrypted financial data. Forensic accounting utilizes digital forensics to uncover irregularities or financial fraud, and can detect unusual trends, financial anomalies, business misconduct, and misappropriation of assets. There are the following common types of fraud that a forensic accountant investigates [9]:

- Insurance fraud: Filing a false insurance claim.
- Corruption: Kickbacks, bribery, and other unethical behaviors.
- Financial statement fraud: Intentionally misrepresenting financial information to deceive an investor.
- Asset misappropriation**:** Theft of company assets (equipment, inventory, and cash) by an employee.

Aligning cyber forensics and accounting investigations provides advantages, including 1) improved evidence collection and accurate assessment of financial losses from cyber breaches, 2) faster detection of fraudulent activities, 3) a more comprehensive understanding of financial crimes, and 4) better mitigation strategies for future risks by leveraging the expertise of both cyber forensics and accounting investigations to fight complicated financial crimes. Specific benefits are summarized as follows [10]:

- Better evidence collection: Cyber forensic evidence (e.g., transaction logs and digital footprints) can be utilized to corroborate financial irregularities detected in accounting investigations, which strengthens a case against potential perpetrators.
- Boosted fraud detection: Investigations can discover more complicated fraudulent schemes by combining financial and digital evidence.
- Enhanced investigation efficiency: Collaboration helps reduce redundancy and streamline the investigative process.
- Precise loss quantification: A cyber forensic expert can decide the scope of a data breach. In contrast, a forensic accountant can translate that information into concrete financial losses, enabling improved decision-making for insurance claims and recovery efforts.
- Better legal case building: A comprehensive view of crime (including both financial and digital evidence) makes legal arguments stronger.

- Improved regulatory compliance: Alignment between accounting investigations and cyber forensics helps meet regulatory requirements regarding cybersecurity and financial reporting.
- Proactive risk mitigation: Working together between cybersecurity and accounting teams helps detect vulnerabilities in financial systems and implement preventative measures to reduce the risk of future financial crimes.

3. FRAUD AND FORENSIC ACCOUNTING INVESTIGATION CRITERIA AND RELEVANT TOOLS

Forensic accounting investigations employ specific criteria, such as analyzing financial records and detecting unusual entries, to uncover financial crimes. Specific investigation criteria and procedures are as follows [11]:

- Collecting evidence: Collecting statements, documents, and electronic data to support a case.
- Analyzing data and financial records: Review and analyze financial statements, tax returns, and cash flow statements; decide whether there are any unusual or suspicious distributions of numbers or money flow between departments and systems.
- Detecting unusual entries: Detect unusual transactions (if there are) and who initiated or approved them.
- Recognizing suspected fraud: Scrutinizing financial records for irregularities (e.g., unusual cash flows and unexplained discrepancies).
- Deciding how a fraud scheme was made: Reveal how fraud was hidden.
- Detecting overrides and bypasses: Discover how internal controls were evaded.
- Proving ill intent: Establish that a suspected fraudster intended to commit fraud.
- Helping to recover losses: Work on recovering money that was lost due to fraud.

Some cyber forensic tools and their functions are listed as follows [12]:

- Autopsy: It can extract the data from raw files, extract timestamps and geo location data, and show the deleted files and data on a computer.
- Network Miner: It can extract information from networks, email attachments, the browser history, etc.
- Volatility Framework: It can extract the RAM information or memory information, and analyze the RAM or memory information even if a computer shuts down. It is used for malware analysis and the investigation of cyber attacks.
- FTK (standing for a forensic toolkit): It provides advanced data analytics; provides features to recover passwords, decrypt files, and analyze network data; and can recover lost or deleted data and files in a system.
- OS Forensics: It helps investigate deeply into the computer, like checking what cybercrime is going on in the device, to provide the proof in court. It is the best tool to search the contents in all the files with any type of format.
- Paladin Forensic Suite: It is a Linux-based software platform that is utilized to recover data.
- Openstego: It can extract the hidden messages present in images, audio files, etc. It is made by the encryption algorithm and provides user-friendly features to help beginners.

Forensic accounting tools are as follows [13]:

- Forensic accounting databases: Accessing industry benchmarks and datasets to compare a company's financial performance with industry standards.
- Data analysis software: Analyzing a large volume of financial data, detecting anomalies, and creating a visualization.
- Financial modeling software: Establishing complicated financial models to simulate various scenarios and detecting possible fraud.
- Digital forensics tools: Software for examining computer files, email communications, and digital records to discover evidence of fraudulent activities.

4. CASE STUDY

4.1. Case 1: Forensic Accounting in Preventing Fraud in Financial Reporting

The utilization of forensic accounting methods and tools can help prevent fraud in financial reporting, even if the risks of fraud have been realized. The objective of financial statement auditing is to decide whether the financial statements of a company "present exactly" its financial position at a given point in time [14]. The differences between forensic accounting and financial auditing are summarized in Table **1**. This table indicates that forensic accounting helps prevent fraud in financial reporting.

4.2. Case 2: Financial Accounting Fraud Detection Based on Data Mining and Forensic Accounting Based on Business Intelligence

Data mining can be used to help financial accounting fraud detection (FAFD). Data mining algorithms, such as neural networks, decision trees, Bayesian networks, regression analysis, etc., for FAFD are illustrated in Figure **1**. The layer with Clustering, Classification, Outlier Detection, etc. is categorized according to various functions. For example, it is easy to identify frauds using Outlier Detection. The outside layer with Neural Network, Naive Bayes, etc. represents specific methods or algorithms. A forensic accounting framework was proposed using business intelligence (BI) with three main data analytics steps for forensic accounting: 1) business analysis, 2) technology and data analysis, and 3) investigative analysis. The framework is illustrated in Figure **2**. The analysis sequence is 1 -> 2 -> 3. The fraud detection process is iterative and dynamic. After step 3 is done and if no fraud is found, the fraud detection process will continue and start from step 1 if new evidence or data is obtained. This is an iterative and dynamic process.

4.3. Case 3: Integrating Big Data into Forensic Accounting and Reshaping the Fraud Detection Process

How to integrate big data into forensic accounting practices and reshape the fraud detection process was studied. Results showed that big data and big data analytics enable significant dispositional affordances

Table 1: A Comparison between Forensic Accounting and Financial Auditing [14]

Aspects	Forensic Accounting	Financial Auditing
Objectives	Get evidence of suspected financial crimes for assessment & judicial decision	Express an opinion on the rationality of financial statements and that they are free of material misstatements
Stakeholders	Those who suspect fraud	External customers of financial statements
Materiality	No	Yes
Fraud scope	Yes	No
Professional regulatory frameworks	No specific standard	International Standards on Auditing
Results	Conclusion through forensic auditor's report	Opinion through the independent auditor's report

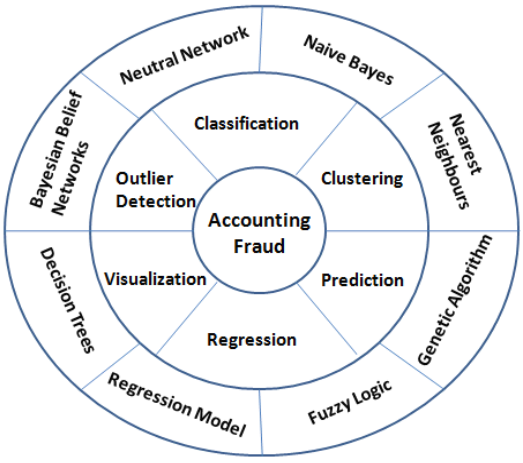

Figure 1: A Conceptual Framework of Data Mining Application in FAFD [15].

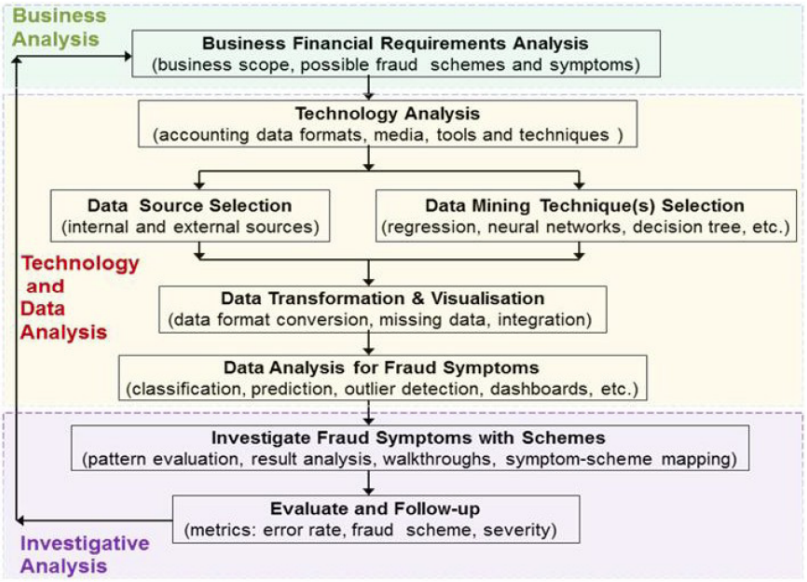

Figure 2: A Forensic Accounting Framework Based on BI [16].

and relational affordances. Dispositional affordances refer to how a user utilizes technologies, which means how forensic accountants exploit technologies (such as big data and big data analytics) to detect fraud. Relational affordances generate a particular relational dynamic associated with properties that technologies bring out, the relationship itself, and how the properties influence relationships. Big data and big data analytics enable a greater depth of analysis. Visual analytics in fraud detection is highlighted in both dispositional and relational affordances [17]. Figure **3** illustrates the dispositional affordance and the relational affordance due to the integration of big data technology (including big data analytics as well) and forensic accounting. Table **2** summarizes big data and big data analytics affordances, which include dispositional affordances, relational affordances, and their details (e.g., functions and benefits).

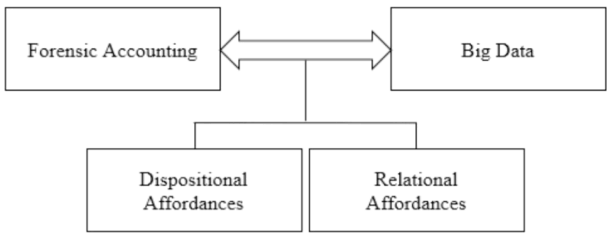

Figure 3: Dispositional and Relational Affordances Resulted from the Integration of Big Data and Forensic Accounting [17].

Fraud detection methods and techniques include discovery sampling, data mining, advanced statistical methods, Benford's Law, outlier detection, internal controls, digital analysis software, computer forensic tools, operational audits, fraud auditing, computer-assisted auditing tools, and whistleblowing policies. A forensic accountant should be well-versed in various areas, including accounting, auditing, statistics, information technology (IT), legal norms, and human skills. Challenges in forensic accounting are illustrated in Figure **4**. The core essential concerns that pose a considerable barrier to the utilization of forensic accounting methods for fraud prevention are legal, political, and educational factors. Acceptability, adaptability, time-consuming legal systems, high cost, technological advancements, and limiting staff decision-making are basic problems in forensic accounting.Lack of organizational resources, expertise, and awareness also slows down the adoption of forensic accounting [18].

5. Fraud and Forensic Accounting Investigation Criteria and Relevant Tools in Healthcare

Cyber forensics needs legal expertise to navigate the gray areas between privacy and the need for evidence. Forensic accounting helps detect fraud in healthcare litigation (e.g., kickbacks, upcoding, and billing for unnecessary services) and identify risks in areas related to fraud and ventures involving other healthcare providers. A forensic accountant employs investigative methods to analyze financial records and reveal fraud in healthcare (such as kickbacks, upcoding, billing for unnecessary services, and COVID-19-related fraud). The forensic accountant can help with litigation, discover damage, and defend against healthcare fraud. Major investigation criteria and procedures are as follows [19-21]:

Table 2: Big Data and Big Data Analytics Affordances [17]

Affordances	Details
Dispositional affordances	Improved operational depth (data triangulation, data scalability & granularity, and a combination of structured & unstructured data) Visualization tools & analytics applications
Relational affordances	Improved team relationships & collaboration Legitimation with customers Functions of visualization tools

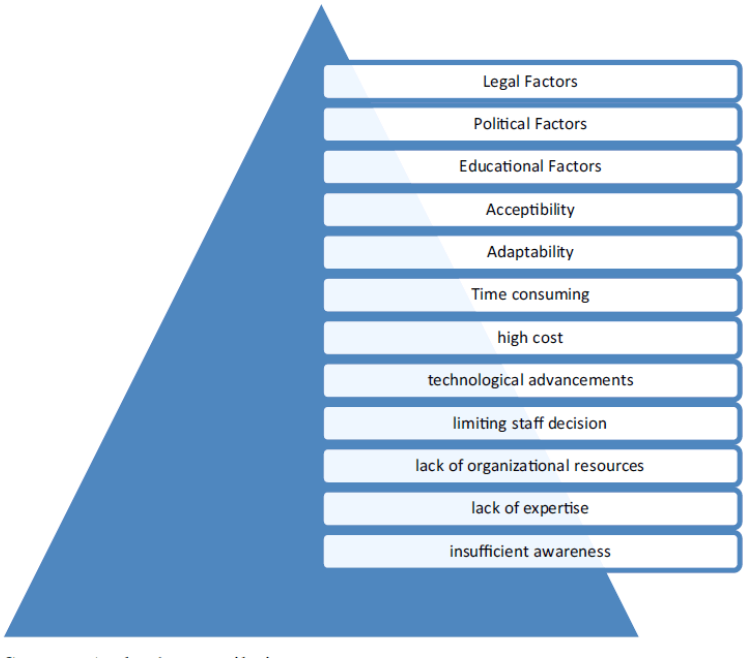

Figure 4: Challenges in Forensic Accounting [18].

- Analyzing a large amount of billing records, claims data, and medical records (e.g., electronic health records) for unusual patterns or inconsistencies.
- Assessing patterns and identifying irregularities in billing reports and billing activities.
- Quantifying financial damages.
- Examining providers and vendors for potential fraud.

In healthcare, cyber forensic tools are used to investigate and prevent cybercrimes, data breaches, etc., by gathering, analyzing, and preserving digital evidence regarding patient data and healthcare systems. Significant considerations for healthcare cyber forensics lie in 1) data sensitivity (sensitive patient data, careful handling, and encryption of data, etc.) and 2) compliance with regulations (adherence to strict data privacy regulations like HIPAA during a cyber forensic investigation). The functions of the tools are described as follows [22]:

- Data analysis: Searching through large amounts of healthcare data (patient records, network traffic, and system logs) and detecting potential anomalies or malicious activity.
- Network analysis: Monitoring and analyzing network traffic; detecting unauthorized access attempts or suspicious patterns.
- Mobile forensics: Analyzing data on mobile devices (e.g., personal cell phones) that may be involved in a breach related to healthcare.
- Timeline analysis: Creating a chronological timeline of events and understanding the sequence of activities that led to a security incident.

- Evidence preservation: Collecting and preserving digital evidence in a forensically sound manner for legal proceedings.

The following cyber forensic tools are often utilized in healthcare [12]:

- EnCase: Gathering, processing, and analyzing digital evidence.
- Wireshark: A tool for network traffic analysis to detect unauthorized access attempts or suspicious patterns.
- Autopsy: A platform with features (such as timeline analysis, keyword search, and file recovery), enabling effective investigation of phone and computer data.
- Cellebrite: Specializing in mobile device forensics and permitting the extraction of data from smartphones and other mobile devices.
- Magnet Axiom: Analyzing data across various platforms (including mobile devices, computers, and cloud environments).
- The Sleuth Kit: An open-source toolkit for disk imaging, file system analysis, and data recovery.

A forensic accountant can employ various tools to detect fraud in healthcare as follows [23, 24]:

- Case management software: Helping an accountant to manage documentation and cases.
- Forensic imaging tools: Helping an accountant examine digital evidence (e.g., documents, emails, and financial transactions).
- Data analysis software: Helps analyze a large amount of data, identify patterns, and detect fraud.
- Digital ledger examination software: Helping analyze digital ledgers.
- Auditing and compliance tools: Helping perform audits and guarantee compliance.

6. CONCLUSION

Forensic accounting helps prevent fraud in financial reporting. Aligning cyber forensics and accounting investigations provides advantages and is useful for the investigation of financial fraud and other cybercrimes. Data mining can be used to help with financial accounting fraud detection. BI facilitates forensic accounting. The integration of big data into forensic accounting reshapes the fraud detection process. Big data and big data analytics enable significant dispositional affordances and relational affordances.

Forensic accounting can help with litigation, discover damage, and defend against healthcare fraud. Significant considerations for healthcare cyber forensics lie in 1) data sensitivity (sensitive patient data, careful handling, and encryption of data, etc.) and 2) compliance with regulations (adherence to strict data privacy regulations like HIPAA during a cyber forensic investigation).It is suggested that forensic accountants and cyber forensic experts should collaborate more effectively. Specific suggestions are: 1) strategic and methodological integration (e.g., creating integrated and joint protocols, establishing multidisciplinary teams, etc.), 2) advanced technologies and tools (such as integrated technology platforms, performing advanced data analytics, and using real-time monitoring systems), and 3) communication and training, such as establishing secure and ongoing lines of communication (e.g., encrypted platforms) and cross-disciplinary training.Future research work is evidentiary standards, admissibility issues, chain-of-custody challenges, and ethical considerations related to digital evidence handling, privacy, consent, and cross-border data issues.

ACKNOWLEDGEMENTS

The authors would like to express their thanks to Technology and Healthcare Solutions, USA, for its help and support.

DECLARATION OF THE USE OF AI TOOLS

The authors declare that they did not use AI tools inwriting this paper.

CONFLICT OF INTEREST

The authors would like to announce that there is no conflict of interest.

ETHICS

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

REFERENCES

[1] Honigsberg C. Forensic accounting. Annual Review of Law and Social Science 2020; 16(1): 147-164. https://doi.org/10.1146/annurev-lawsocsci-020320-022159

[2] Rechtman YM. The Past, Present, and Future of Forensic Accounting. CPA Journal 2020; 90(3): 10-12.

[3] Negangard EM, Fay RG. Electronic discovery (eDiscovery): Performing the early stages of the Enron investigation. Issues in Accounting Education 2020; 35(1): 43-58. https://doi.org/10.2308/issues-16-064

[4] Özcan A. The use of Beneish model in forensic accounting: evidence from Turkey. Journal of Applied Economics and Business Research 2018; 8(1): 57-67.

[5] Rufus RJ. The 3 W's of engaging a forensic accountant: Why, when, and who. American Journal of Family Law 2018; 32(3): 108-114.

[6] Wiesenfeld J. COVID-19 challenges to forensic accounting. Journal of Accountancy 2020: 1-3.

[7] Grove H, Clouse M. Financial and non-financial fraud risk assessment. Journal of Forensic and Investigative Accounting 2020; 12(3): 422-441.

[8] Comunale CL, Caprariello P, Taylor EZ, Gara S, Sexton TR. The Value of a Contentious Auditor. Journal of Forensic and Investigative Accounting 2024; 16(3): 336-348.

[9] Bou Reslan F, Jabbour Al Maalouf N. Assessing the transformative impact of AI adoption on efficiency, fraud detection, and skill dynamics in accounting practices. Journal of Risk and Financial Management 2024; 17(12): 577. https://doi.org/10.3390/jrfm17120577

[10] Tekavčič M, Damijan S. Forensic Accounting vs Fraud examination: Roles, Importance and Differences. Journal of Forensic Accounting Profession 2021; 1(2): 29-47. https://doi.org/10.2478/jfap-2021-0007

[11] Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials 2020; 22(2): 1191-221. https://doi.org/10.1109/COMST.2019.2962586

[12] Fernando V. Cyber forensics tools: A review on mechanism and emerging challenges. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2021 (pp. 1-7). IEEE. https://doi.org/10.1109/NTMS49979.2021.9432641

[13] Smith KT, Smith LM. Examining documentation tools for audit and forensic accounting investigations. Journal of Risk and Financial Management 2024; 17(11): 491. https://doi.org/10.3390/jrfm17110491

[14] Clavería Navarrete A, Carrasco Gallego A. Forensic accounting tools for fraud deterrence: a qualitative approach. Journal of Financial Crime 2023; 30(3): 840-854. https://doi.org/10.1108/JFC-03-2022-0068

[15] Sharma A, Panigrahi PK. A review of financial accounting fraud detection based on data mining techniques. arXiv preprint arXiv: 1309.3944 2013.

[16] Wong S, Venkatraman S. Financial accounting fraud detection using business intelligence. Asian Economic and Financial Review 2015; 5(11): 1187. https://doi.org/10.18488/journal.aefr/2015.5.11/102.11.1187.1207

[17] Gabrielli G, Magri C, Medioli A, Marchini PL. The power of big data affordances to reshape anti-fraud strategies. Technological Forecasting and Social Change 2024; 205: 123507. https://doi.org/10.1016/j.techfore.2024.123507

[18] Kaur B, Sood K, Grima S. A systematic review on forensic accounting and its contribution towards fraud detection and prevention. Journal of Financial Regulation and Compliance 2023; 31(1): 60-95. https://doi.org/10.1108/JFRC-02-2022-0015

[19] Atlam HF, Ekuri N, Azad MA, Lallie HS. Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. Electronics 2024; 13(17): 3568. https://doi.org/10.3390/electronics13173568

[20] D'Anna T, Puntarello M, Cannella G, Scalzo G, Buscemi R, Zerbo S, Argo A. The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data. In Healthcare 2023 (Vol. 11, No. 5, p. 634). MDPI. https://doi.org/10.3390/healthcare11050634

[21] Klasén L, Fock N, Forchheimer R. The invisible evidence: Digital forensics as key to solving crimes in the digital age. Forensic Science International 2024; 362: 112133. https://doi.org/10.1016/j.forsciint.2024.112133

[22] Lovanshi M, Bansal P. Comparative study of digital forensic tools. In Data, Engineering and Applications: Volume 2 2019 (pp. 195-204). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-13-6351-1_15

[23] Sachdeva S, Raina BL, Sharma A. Analysis of digital forensic tools. Journal of Computational and Theoretical Nanoscience 2020; 17(6): 2459-2467. https://doi.org/10.1166/jctn.2020.8916

[24] Wu T, Breitinger F, O'Shaughnessy S. Digital forensic tools: Recent advances and enhancing the status quo. Forensic Science International: Digital Investigation 2020; 34: 300999. https://doi.org/10.1016/j.fsidi.2020.300999

Received on 05-12-2025 Accepted on 06-01-2026 Published on 23-01-2026

https://doi.org/10.65879/3070-5789.2026.02.01