ISSN: 3067-8358
Research Article
Journal of Global Perspectives on Society, Culture, and Development

Automation in Forensic Accounting

Dimitrios Karadimos[1]*, Angelidis Georgios[2] & Constantinos J Stefanou[3]

[1]School of Economics and Business Administration, Department of Accounting and Information Systems, International Hellenic University, 574 00, Thessaloniki, Greece

[2]School of Economics, Faculty of Economic and Political Sciences, Aristotle University of Thessaloniki, 541 24 Thessaloniki, Greece

[3]School of Economics and Business Administration, Department of Accounting and Information Systems, International Hellenic University, 574 00, Thessaloniki, Greece

***Corresponding author:** Dimitrios Karadimos, School of Economics and Business Administration, Department of Accounting and Information Systems, International Hellenic University, 574 00, Thessaloniki, Greece.

Submitted: 27 January 2026 **Accepted:** 03 February 2026 **Published:** 10 February 2026

Citation: *Karadimos, D., Angelidis, G., Stefanou, C. J. (2026). Automation in Forensic Accounting. J of Glob Perspect Soc Cult Dev, 2(1), 01-09.*

Abstract

This article reviews the evolution of forensic accounting in the digital age, highlighting the central role of information technology (IT) and artificial intelligence (AI) in reshaping traditional practices. Forensic accounting uses IT to improve attention to detail, validate its work, and enhance analytical investigations. We trace the evolution of the discipline, highlighting the adoption of advanced data analytics, blockchain, and machine learning, alongside tools such as digital forensics and cybersecurity, which are expanding the scope and efficiency of financial investigations. Automation is emerging as a driving force, with data mining techniques and AI not only uncovering hidden patterns but also enabling rapid responses to suspicious incidents. As the landscape evolves, challenges and ethical considerations are examined, particularly in automated communications analysis and Internet of Things (IoT) forensics. Finally, this article explores the transformative impact of blockchain on accounting professionals, highlighting the need for continuous skills development to navigate the dynamic fusion of technology and forensic accounting, ensuring practitioners remain adept in the face of ongoing technological advances.

Keywords: Automation, Forensic Accounting, Finance, Fraud, Artificial Intelligence.

Introduction

In the relentless pursuit of precision, validation, and enhanced analytical investigations, forensic accounting seamlessly integrates information technology (IT) tools, showcasing the adoption of advanced data analytics, blockchain, machine learning, and cybersecurity. Automation is emerging as a driving force, with data mining techniques and artificial intelligence (AI) not only revealing hidden patterns but also accelerating responses to suspicious incidents. The landscape expands further with discussions of challenges and ethical considerations, particularly in automated communications analysis and Internet of Things (IoT) forensics. The transformative impact of blockchain on accounting professionals takes center stage, highlighting the need for continuous skills development amid ongoing technological advances. This article serves as a comprehensive guide to the dynamic convergence of technology and forensic accounting, illuminating the path for practitioners to navigate and thrive in this ever-evolving digital terrain. In what follows, we set out the basic definitions and key concepts that are necessary for an understanding of the contextual framework within which forensic accounting operates.

According to [5], forensic accounting is defined as "the application of financial skills, and an investigative mentality to unresolved issues, conducted within the context of rules of evidence. As an emerging discipline, it encompasses financial expertise, fraud knowledge, and a sound knowledge and understanding of business reality and the working of the legal system."

Professionals in a wide range of fields have testified to the transformative impact of IT on their work processes, citing notable improvements in attention to detail and in the depth of achievement of their goals. Viewed as an indispensable tool, IT plays a pivotal role in facilitating a meticulous approach to tasks, enabling professionals to delve deeper into the intricacies of their projects. Moreover, these professionals see IT not just as a facilitator, but as a cornerstone for validating their work. The integration of advanced applications, such as archiving and planning suites, has been particularly instrumental in enhancing analytical investigations. These applications not only streamline workflows, but also enhance the analytical capabilities of professionals, allowing for more sophisticated and comprehensive investigations. As a result, IT is a driving force in raising professional standards, enabling individuals to achieve greater precision and efficiency in their endeavors, as highlighted in [3].

Initial findings on the integration of AI into audit practices show a significant increase in operational efficiency, which translates into a reduction in the amount of manpower required for certain tasks compared to traditional methods. At the same time, there is a notable increase in the overall quality of the service provided. This efficiency gain is particularly significant in the context of labour costs, where the application of AI technologies allows for a more streamlined allocation of resources, leading to a potential reduction in labour costs. Consequently, these advances in operational efficiency and resource optimisation are inextricably linked to the financial implications for audit firms, as the reduction in manpower costs has a direct impact on the fee structure of these firms. The positive spill-over effect of AI implementation on the quality and effectiveness of control mechanisms is evident, as described in [8]. This synergy between AI, operational efficiency, and financial considerations underscores the multiple benefits that can be derived from the prudent use of AI technologies in auditing.

The use of AI, particularly in fraud detection, risk management, credit decisions, algorithmic transactions and the implementation of chatbots, serves as a key strategy for improving the efficiency of business processes. The application of AI in fraud detection allows for the rapid and accurate identification of anomalies, thereby strengthening the security of financial transactions. In risk management, AI algorithms analyse vast amounts of data in real time, enabling more proactive identification and mitigation of potential risks. Credit decisions benefit from AI’s predictive analytics, enabling more nuanced assessments and faster responses. AI-powered algorithmic transactions streamline and automate complex financial processes, optimising efficiency and reducing errors. In addition, the integration of chatbots into customer interactions enhances the user experience, providing instant and personalised services. Beyond operational efficiency, the strategic use of AI contributes to broader goals, such as financial inclusion, by making modern financial services more accessible and tailored to diverse user needs. In essence, AI is emerging as a transformative force that not only optimises specific business functions, but also aligns with overarching goals of inclusivity and efficiency, as outlined in [18].

The integration of IT has been shown to significantly reduce the time required to perform various business functions. By facilitating the seamless exchange and dissemination of information, IT not only speeds up internal processes, but also enables organisations to share critical data with the wider public. This enhanced connectivity not only promotes transparency but also uncovers new investment opportunities, laying the groundwork for improved investment operations. The quality of investment operations improves significantly as technology refines and optimises various facets of the investment process. In addition, IT contributes to the impartiality of investment decisions by enabling a more data-driven and analytical approach, thereby minimising bias in judgements. Proponents of proposed software products designed to automate business processes stand to benefit significantly, particularly when evaluating criteria such as "opportunity, price, availability" as outlined in [22]. In essence, the strategic incorporation of IT not only streamlines business operations, but also has positive spill-over effects, improving investment practices and decision making while promoting efficiency and equity.

The following section examines the evolutionary trajectory of forensic accounting, emphasising its skilful adaptation to the digital age. Section 3 explores automation tools and techniques, highlighting the transformative impact of technology on conventional forensic accounting practices. Section 4 focuses meticulously on digital forensics and e-discovery, while Section 5 critically examines the field of fraud detection and prevention. Section 6 assesses the discourse on compliance and regulatory automation. Section 7 comprehensively addresses the intricate areas of cybersecurity and data protection within the scope of forensic accounting. Section 8 discusses the challenges and ethical considerations inherent in the field. Finally, Section 9 outlines future trends and provides the conclusions of the study.

Evolution of Forensic Accounting: Adapting to the Digital Age

Forensic Accounting has developed its methods to be more efficient. Forensic accounting professionals save a lot of working time by using financial computer programs. The amount of software and IT has expanded very rapidly in recent years. Auditors have adapted technology in order to keep up with the development of methods of committing criminal financial acts [7]. Over time the models were based on economic data and targeted accounting irregularities. However, prediction models based on behavioural characteristics have become increasingly common as well as models that incorporate both psychological and quantitative analysis as usual have taken precedence over models based on financial data alone [15].

The forensic accounting landscape has undergone a profound transformation, driven by significant technological advances [3]. Key developments in advanced data analytics and forensic software, including tools such as data mining and predictive analytics, have enabled practitioners to detect financial irregularities. By sifting through large data sets and identifying patterns, these technologies enhance the ability to uncover fraudulent activity. Blockchain technology, with its immutable ledger and smart contracts, plays a pivotal role in ensuring transparency and accountability in financial transactions, fostering trust and integrity [28]. AI and machine learning algorithms contribute to the field by aiding in pattern recognition and analysing unstructured data through natural language processing [19]. Digital forensic tools enable the extraction and analysis of electronic evidence from a wide range of devices. Cloud computing facilitates remote access and collaboration, fostering seamless teamwork among geographically dispersed forensic teams [23]. In addition, cybersecurity tools, advanced visualisation software, geospatial analysis and mobile technology have become indispensable components of modern forensic accounting practices [11].

Regulatory technology is emerging as a critical element to ensure compliance with relevant laws and regulations, while virtual reality and augmented reality technologies are valuable tools for crime scene reconstruction, providing a nuanced perspective [26]. These technological advances have not only increased the efficiency and accuracy of forensic accounting, but have also significantly expanded its scope. By emphasising the importance of continually refining skills in the effective use of these tools, these advances underscore the evolving nature of the discipline and position forensic accounting professionals to navigate complex financial landscapes with enhanced skills [25].

Automation Tools and Techniques

In the forensic accounting, the integration of data mining techniques has become an indispensable tool for uncovering hidden patterns and predicting future trends and behaviours. The multiple benefits of these techniques include increased revenues, reduced costs, and increased market responsiveness and information. The power of data mining lies in its ability to extract actionable insights from vast amounts of data, providing market participants with the tools they need to make informed decisions and capitalise on emerging opportunities. The synergy between research and practice is evident in the extensive work devoted to the study of data mining, as highlighted in [31].

However, it is crucial to recognise that not all data mining approaches are universally applicable. As pointed out in [21], conditional data mining approaches may not be effectively applied in the context of Anomaly Detection Systems (ADS). This finding highlights the need to tailor data mining methods to the specific needs and nuances of forensic accounting. Such customisation ensures that the techniques employed are well aligned with the intricacies of anomaly detection, a critical consideration in this dynamic and high-stakes domain. This sophisticated approach ultimately increases the reliability and effectiveness of data mining applications in financial markets. Anomaly detection algorithms aim to identify deviations from the norm. Let represent financial transactions as a vector X with various features such as transaction amount, frequency, etc. A simple mathematical formulation for anomaly detection could be based on a Gaussian distribution. Given a dataset $\{x^{(1)},\ x^{(2)}, \ldots , x^{(m)}\}$, where $x^{(i)}$is a feature vector for the i-th transaction, you estimate the mean (μ) and covariance matrix (Σ) of the features. The probability of a new transaction x being normal could be calculated using the multivariate Gaussian distribution [12]

$$P(x) = \frac{1}{2\pi^{\frac{n}{2}}\,|\Sigma|^{\frac{1}{2}}}\, exp\left(-\frac{1}{2}\,(x-\mu)^T\Sigma^{-1}(x-\mu)\right)$$

If P(x) is below a certain threshold, the transaction may be flagged as potentially fraudulent.

The integration of AI into forensic accounting harnesses the vast reservoirs of data generated by companies, not only providing predictive insights but also facilitating rapid responses to potentially suspicious incidents. The role of AI in this context is multifaceted, driven by its exceptional pattern recognition capabilities and the profound impact of deep learning, a key facet of AI that takes its analytical capabilities to a higher level, as explained in [4]. By effectively processing and interpreting large amounts of data, AI systems are able to detect subtle patterns and anomalies that may elude traditional methods of analysis. This increased level of pattern recognition enables to proactively identify and address potential risks, facilitating not only prediction but also rapid and informed action. The integration of deep learning adds a layer of complexity, enabling AI systems to continuously refine their understanding and adapt to evolving patterns, further enhancing their ability to detect and respond to suspicious incidents with speed and precision. In essence, AI serves as a formidable ally in forensic accounting, using data not only to predict trends, but also to strengthen the industry's resilience to emerging threats. AI systems in fraud detection are commonly based on decision trees and ensemble methods like Random Forests [2]. Decision trees classify data based on a series of if-else conditions. In the context of fraud detection, a decision tree might evaluate features such as transaction amount, frequency, location, etc. A Random Forest is an ensemble of multiple decision trees. Each tree is trained on a subset of the data, and the final prediction is made by aggregating the results of individual trees. The mathematical formulation involves the combination of decision trees to form a robust model for classification. If T_1, T_2, … , T_n, and $\hat{yi}$ is the prediction of the i-th tree, the final prediction $\hat{y}_{\text{final}}$ of the Random Forest can be expressed as $\hat{y}_{\text{final}}$ = $MajorityVote\ (\hat{y}_{1,}\ \hat{y}_{2,} \ldots , y_{\hat{n},})$ where the Majority Vote is a function that selects the most commonly predicted class among the individual trees. This ensemble approach is effective for capturing complex relationships in the data and improving the overall accuracy of fraud detection models.

Digital Forensics and E-Discovery

A notable contribution to memory management and access monitoring has been the introduction of a method for monitoring access to mapped shared memory files [24]. This innovative approach involves a comprehensive examination of the influence of Windows memory allocation strategies on the preservation of both data and context within the memory framework. By addressing the nuances of memory access and allocation, this research not only contributes to the understanding of Windows memory dynamics, but also provides practical insights into improving file retrieval processes associated with mapped shared memory, thereby enriching the landscape of memory management strategies.

While the conventional phases within an eDiscovery process are similar to those of traditional digital forensics, there are nuanced differences in approach that distinguish the two disciplines. The eDiscovery process, similar to digital forensics, typically includes identification, preservation, collection, processing, review, analysis and production phases. However, eDiscovery often focuses on identifying and collecting Electronically Stored Information (ESI) relevant to litigation, rather than conducting a full forensic investigation. The nuances in approach stem from the legal context of eDiscovery, where the goal is to comply with legal requirements and produce relevant evidence for litigation. While these differences offer certain advantages, such as a focus on legal relevance, they also underscore the need for additional effort. Ensuring the production of forensically sound evidence in a criminal case requires meticulous attention to detail, as legal standards demand a high level of accuracy and completeness in the handling of digital evidence. Therefore, practitioners in both eDiscovery and digital forensics must navigate these nuanced distinctions in order to maintain the integrity of the evidence presented in legal proceedings [13].

Let consider an example scenario involving the eDiscovery process in forensic accounting. Suppose a company suspects embezzlement by one of its employees. The company decides to conduct a forensic accounting investigation, leveraging eDiscovery tools to uncover electronic evidence. Step 1 - Identification (eDiscovery Kick-off): The investigation team initiates the eDiscovery process, identifying potential sources of electronic evidence. This includes emails, financial databases, and communication records.

Step 2 - Preservation: To ensure the preservation of relevant electronic evidence, the team employs digital forensic tools to create forensic images of the suspect's computer, external drives, and email accounts. Cryptographic hash functions are used to verify the integrity of the collected data.

Step 3 - Collection: Electronic evidence is collected from various sources, including the suspect's computer, the company's financial servers, and email servers. Data is collected in a forensically sound manner to maintain its admissibility in legal proceedings.

Step 4 - Processing: Collected data undergoes processing using eDiscovery software. This involves filtering and organizing the data to eliminate duplicates, irrelevant files, and non-essential information. Advanced analytics may be applied to identify patterns related to financial transactions and communication.

Step 5 - Review: Forensic accountants and investigators review the processed data, focusing on financial transactions, email communications, and any suspicious activities. Keyword searches and document categorization tools are employed to streamline the review process.

Step 6 - Analysis: Advanced analytics tools are used to analyze financial transactions, looking for anomalies, unusual patterns, or hidden relationships between transactions. Data visualization techniques may be applied to represent financial flows and highlight irregularities.

Step 7 - Production: Relevant electronic evidence, such as incriminating emails or financial transaction records, is produced for legal proceedings. Redaction tools are applied to protect sensitive information that is not relevant to the investigation. In this example, eDiscovery tools facilitate the efficient identification, collection, and analysis of electronic evidence related to financial transactions and communication, aiding forensic accountants in uncovering evidence of embezzlement. The process ensures that electronic evidence is handled in a defensible and legally admissible manner.

Fraud Detection and Prevention

The adaptability and responsiveness of computational methods, particularly neural networks and support vector machines, play a key role in the ongoing battle against fraudsters' ever-evolving techniques. These sophisticated tools demonstrate a remarkable ability to train and respond effectively to new fraud methods, providing a dynamic line of defence for cybersecurity efforts. The utility of neural networks and Support Vector Machines (SVM) lies in their ability to learn and adapt to new techniques, enabling them to stay ahead of fraudsters' tactics in the ever-evolving cyber threat landscape. Despite the progress made in the use of these computational methods, it is crucial to recognise that certain facets of intelligent fraud detection have yet to be thoroughly explored in research, as pointed out by [30]. This recognition underscores the need for continued research and innovation in the field of fraud detection, and urges researchers and practitioners to venture into uncharted territory and explore novel approaches to strengthen the resilience of systems against emerging cybersecurity threats.

SVM aims to find a hyperplane that separates the data into different classes. For a binary classification problem, the linear SVM formulation could be as follows. Let $\{(x^{(1)}, y^{(1)}), (x^{(2)}, y^{(2)}), \dots, (x^{(m)}, y^{(m)})\}$ is a set of labeled data points , where $x^{(i)}$ is the feature vector of the i-th example, and $y^{(i)}$ is its corresponding label (-1 for negative class, +1 for positive class). The linear SVM formulation seeks to find a hyperplane characterized by a weight vector w and a bias term b such that the data points are well-separated:

$$min_{w,b}\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{m} max\left(0,1-y^{(i)}\left(w^Tx^{(i)}+b\right)\right)$$

where $\frac{1}{2}\|w\|^2$ is the regularization term that penalizes large values of the weight vector w, preventing overfitting,

$$C\sum_{i=1}^{m} max\left(0,1-y^{(i)}\left(w^Tx^{(i)}+b\right)\right)$$

represents the hinge loss, which measures the degree of misclassification and the goal is to minimize this term to ensure that data points are on the correct side of the decision boundary, C is the regularization parameter. It controls the trade-off between achieving a low training error and a simple decision boundary. A smaller C emphasizes a simpler decision boundary, while a larger C allows for a more complex boundary.

The formulation above assumes that the data is perfectly separable by a hyperplane. However, in real-world scenarios, data may not be linearly separable. In such cases, a soft-margin SVM allows for some misclassification. The objective function for a soft-margin SVM could be

$$min_{w,b,\xi}\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{m}\xi_i$$

subject to $y^{(i)}\left(w^Tx^{(i)}+b\right) \geq 1-\ \xi_i$ for all i, and $\xi_i \geq 0$.

Here, ξ_i are slack variables that allow for some points to fall inside the margin or even on the wrong side of the decision boundary. The term $^1\|w\|^2$ is still the regularization term, and C is the regularization 2 parameter as before. The choice of C influences the trade-off between a larger margin and allowing some misclassification. A smaller C increases the margin but allows for more misclassification, while a larger C reduces the margin but enforces stricter adherence to the correct classification.

Generative models have received considerable attention in the contemporary literature, especially in the field of unsupervised methods, as evidenced by numerous references. These models, such as Generative Adversarial Networks (GANs) and various AutoEncoder (AE) networks, have proven to be powerful tools with diverse applications, particularly in the areas of credit card and insurance fraud detection and anti- money laundering efforts. The unique strength of generative models lies in their ability to identify and understand larger and more complex features from raw data by delving into the hidden dimensions of a training set. By exploiting the hidden space within data sets, generative models contribute to a more nuanced understanding of patterns and structures, increasing their effectiveness in identifying fraudulent activity. As the financial crime landscape continues to evolve, the exploration and refinement of generative models is a central endeavour, demonstrating their potential to enhance the efficiency and accuracy of fraud detection systems. The application of GANs and AE networks highlighted in [14] demonstrates the versatility of generative models in addressing complex financial security challenges. AE are a type of neural network [6] used for unsupervised learning, particularly in the context of dimensionality reduction and feature learning. In fraud detection scenarios, AE can be employed to learn a compact representation of normal financial transactions, and anomalies or fraudulent activities can be detected by identifying deviations from this learned representation. The AE development involves encoding the input data into a lower-dimensional representation and then decoding it back to the original data. The anomaly detection is often based on the reconstruction error. Let X be the input data, Z be the encoded representation, and $\hat{X}$ be the reconstructed output. The goal is to minimize the difference between the input and the reconstructed output.

$$Z = f_{encode}(X;\ \theta_{encode})$$

where fencode is the encoder function parameterized by θ_{encode}, which represents the weights and biases of the encoder.

$$\hat{X} = f_{decode}(Z;\ \theta_{decode})$$

Similarly, f_{decode} is the decoder function parameterized by θ_{decode}.

The objective is to minimize the reconstruction loss, typically measured as the mean squared error (MSE) between the input X and the reconstructed output $\hat{X}$. Hence, the Objective Function is

$$J(X,\hat{X}) = \left\|X - \hat{X}\right\|^2$$

The training involves adjusting the weights and biases of both the encoder and decoder to minimize the reconstruction loss: $min_{\theta encode},\ \theta decode\ J(X,\ \hat{X})$

After training the AE on normal (non-fraudulent) financial transaction data, anomalies or potentially fraudulent activities can be detected based on the reconstruction error. Transactions that deviate significantly from the normal behavior are considered as potential anomalies. The threshold for identifying anomalies is often determined based on statistical measures such as standard deviation.

$$Anomaly\ Score\ (X) = \left\|X - \hat{X}\right\|^2$$

Transactions with higher anomaly scores are more likely to be considered as potential fraudulent activities.

Compliance and Regulatory Automation

Event monitoring technology represents a revolutionary approach to monitoring distributed and heterogeneous IT systems by providing a seamlessly connected framework without the need to integrate disparate systems and components. This innovative methodology recognizes the diverse and complex nature of today's IT infrastructures and provides a solution that streamlines monitoring processes with minimal disruption. The importance of event monitoring goes beyond operational efficiency, as it is emerging as a key player in the effective implementation, continuous monitoring and rigorous enforcement of regulatory requirements, as emphasised in [10]. By harnessing the power of event monitoring, organisations can not only improve their system oversight, but also ensure compliance with regulatory standards. This not only strengthens the security and reliability of IT systems, but also the governance frameworks that are essential for maintaining integrity and accountability in the rapidly evolving technology and compliance landscape.

Event monitoring technology for fraud detection in financial statements involves tracking and analyzing various events or activities related to financial transactions. Let E represent the event data, where each event e_i contains information about a specific financial transaction or activity. A generalized methodology of Event Monitoring could involve the following steps: a) Identify the relevant events to monitor (e.g.,transaction amount, frequency, user logins, account access), b) Extract features X_i from each event e_i, capturing important information for fraud detection, c) Define thresholds for each feature based on historical data or expected norms, d) Flag events as potentially fraudulent if they exceed certain thresholds

$$Anomaly\ Indicator(e_i) = \begin{cases} 1 & \text{if } X_i > \text{Threshold}_i \\ 0 & \text{otherwise} \end{cases}$$

e) Aggregate anomaly indicators across multiple events to obtain an overall fraud score for a specific time period or user

$$Overall\ Fraud\ Score = \textstyle\sum_{i=1}^{n} Anomaly\ Indicator\ (e_i),$$

where *n* is the total number of events.

Data analytics platforms represent a transformative leap in information processing, providing a powerful means of accelerating and streamlining the evaluation of vast amounts of data. The inherent ability of these platforms to quickly analyse vast amounts of data not only reduces the burden on government agencies, but also significantly reduces the time and effort traditionally required to produce comprehensive reports. This acceleration of data processing and analysis is a game changer, allowing agencies the luxury of spending more time on the critical aspects of in-depth analysis and decision making. As highlighted in [1], the efficiency gains realised through data analytics platforms have far-reaching implications, enabling agencies to respond to complex challenges with agility, make data-driven decisions in a timely manner, and ultimately improve their overall operational effectiveness. In a landscape where the pace of data generation continues to escalate, the adoption of such platforms is paramount for organisations seeking to stay ahead in the dynamic and data-centric environments in which they operate.

Cybersecurity and Data Protection in Forensic Accounting

Academic research has delved deeply into the multifaceted area of cybersecurity within the field of accounting, scrutinising various crucial aspects. Investigations have included the study of access controls, encryption techniques, network monitoring systems, and incident response strategies, all of which collectively contribute to a comprehensive understanding of cybersecurity methodologies applicable to accounting practices, as articulated in [16].

The focus on access controls highlights how organisations can fortify their digital perimeter by regulating and securing entry points to sensitive financial data. Encryption techniques are explored to protect the confidentiality and integrity of financial information, ensuring that even in the event of unauthorised access, the data remains unintelligible and secure. Network monitoring systems are examined for their role in proactively identifying and mitigating potential cybersecurity threats, providing a critical layer of defence against malicious activity. In addition, incident response strategies are being investigated to understand how organisations can effectively and efficiently respond to security incidents, minimise the impact and quickly restore normal operations. The synthesis of these research efforts enhances the knowledge base of cybersecurity methodologies, providing valuable insights into their application and effectiveness in the specific context of accounting practices.

The dissemination of cybersecurity threat information serves a critical purpose in the field of cybersecurity. This proactive sharing of information is designed to raise awareness among stakeholders by providing up- to-date insight into the latest threats and vulnerabilities. The aim is not only to inform, but also to catalyse the rapid implementation of corrective action. By keeping abreast of the evolving threat landscape, stakeholders can better understand the risks they face and take proactive steps to strengthen their defences. However, the importance of Cyber Threat Intelligence (CTI) goes beyond mere awareness. As highlighted in [29], CTI plays a key role in supporting tactical decision making by stakeholders. It provides them with actionable insights that enable informed responses to potential threats and vulnerabilities. This strategic integration of threat intelligence into decision-making processes enhances the organization's ability to pre- emptively address cyber threats, thereby strengthening its overall cybersecurity posture and resilience. In essence, the purpose of sharing threat intelligence is not just to inform, but to equip stakeholders with the knowledge and tools they need to make timely and effective decisions in the face of evolving cybersecurity challenges.

Challenges and Ethical Considerations

Historically, the examination of ethical concerns surrounding automated communication analysis has fallen predominantly into two categories: the socio-ethical perspective and technical feasibility. However, there is a notable gap in the exploration of the complex techno-ethical tensions and dilemmas that arise at the challenging intersection of socio-technical feasibility. There is a considerable lack of research that addresses the complex interplay between technological capabilities and ethical considerations, particularly in relation to the limitations and implications of assumed solutions. In contrast to conventional approaches, recent developments have begun to emphasise more dynamic, real-time and interactive methodologies. This shift in focus offers the potential to mitigate hidden biases embedded in fully automated systems, particularly those trained on biased historical crime data, and to address challenges arising from messy or inadequate large datasets [9]. By recognising and addressing these issues, researchers and practitioners are paving the way for more ethical and socially responsible automated communications analysis, and ushering in a new era of transparency, fairness and accountability in the use of advanced technologies in this area.

The challenges of IoT forensics highlight critical gaps in cybersecurity measures. As the proliferation of IoT devices continues, the complexities associated with securing these interconnected systems are becoming increasingly apparent. However, researchers and forensic professionals are actively engaged in addressing these challenges and are devoting significant efforts to developing tools and solutions that ensure the valid collection and preservation of digital evidence within the IoT landscape. An integral part of this effort is working with device manufacturers, who play a critical role in establishing secure and legal procedures for extracting data from their products. This proactive approach is driven by the recognition that in the event of a security incident, these manufacturers and their devices may become the subject of an investigation. By recognising the need for specific and legally compliant methods of data extraction, device manufacturers are contributing to the establishment of robust forensic practices. This collaborative effort reflects a commitment to improving cybersecurity measures within the IoT ecosystem, mitigating risk and ensuring the integrity of digital evidence, thereby fostering a more secure and resilient IoT landscape [27].

The complex legal challenges associated with digital forensics are a direct reflection of the broader issues surrounding information security and preservation. In the digital age, computer systems wield considerable influence, shaping both positive and negative aspects of our lives. As a discipline, digital forensics addresses the dual role of these systems as both a tool for detecting wrongdoing and a means of protecting the integrity of digital information. The convergence of privacy and security risks in this context goes beyond the mere intrusion into the private facets of individuals' lives. It also encompasses the potential consequences of drawing erroneous or inadequately supported conclusions based on flawed analysis. As underlined in [20], these risks highlight the delicate balance that must be struck between the imperative to investigate and maintain security and the equally crucial need to respect privacy rights. The legal intricacies faced by digital forensics practitioners underscore the need for comprehensive frameworks that not only enable investigations, but also protect against the potential pitfalls of misinterpretation and inadequate analysis at the complex intersection of technology, law, and privacy.

Future Trends and Implications

The emergence of blockchain technology has brought about a transformative change in the accounting landscape, creating a demand for new professionals with the skills to navigate this novel blockchain environment. As blockchain implementations gain traction across industries, there is a need for accounting professionals with a nuanced understanding of the intricacies of this decentralised and distributed ledger technology. The integration of blockchain not only changes the traditional dynamics of accounting, but also prompts a reassessment of the roles and responsibilities of accounting professionals. In particular, the role of auditors is expected to change significantly. While internal audit functions are likely to continue, their focus may change or be carried out in a different way from traditional approaches. The inherent transparency and immutability characteristics of blockchain may reshape the audit process, potentially streamline audit procedures and improve the overall efficiency and accuracy of financial assessments. In essence, the rise of blockchain technology heralds a paradigm shift in the accounting profession, requiring a workforce that can skillfully navigate and leverage the capabilities of this innovative technology [17].

The proposed research into the impact of technological and regulatory changes on accounting firms and practitioners recognises the dynamic landscape in which the accounting industry operates. Technological advances and regulatory changes have the potential to significantly impact traditional practices and roles within the accountancy profession. While these changes can bring positive change, it’s important to recognise that innovation often has a dual nature. On the one hand, innovation can lead to the creation of new opportunities, streamlined processes and improved efficiencies, thereby fostering growth and development within the accounting sector. On the other hand, there is an inherent risk of job displacement as certain roles become automated or obsolete due to technological advances. The delicate balance between job creation and destruction within the accounting profession is a critical facet of the research. Understanding and navigating the distinction of these impacts is crucial for accounting firms and practitioners to proactively adapt to the evolving landscape, harnessing innovation to their advantage while mitigating potential challenges associated with job displacement. The research of [17] serves as a critical step in formulating strategies to ensure the resilience and sustainability of the accounting profession in the face of ongoing technological and regulatory change.

The accounting landscape has been transformed in recent years with the introduction of financial robots by the big accounting firms. These advanced technologies demonstrate the ability to autonomously scan data, import invoices and produce comprehensive financial reports. This marks a significant leap in accounting automation, suggesting that these financial robots are ready to take on the roles traditionally performed by basic accounting clerks. The automation of routine accounting tasks streamlines processes, reduces the need for manual intervention and speeds up the generation of financial information. A notable outcome of this development is that business managers, regardless of their accounting expertise, can now use these financial robots to access and interpret basic accounting information. This accessibility enables business leaders to make informed decisions based on accurate and timely financial data without the need for a deep understanding of accounting principles. The emergence of financial robots from major accounting firms reflects a broader trend of using technology to improve efficiency and democratise access to financial insight within the business sphere [32].

Reorganizing accounting processes, reducing errors and distortions of accounting information, improving accounting efficiency, and promoting the transformation of accounting structures are the major changes in accounting that have been made by integrating emerging technologies such as Big Data, Machine Learning (ML), AI, and blockchain into the accounting field [32].

While new technologies have the potential to be transformative and have a significant impact on the work of accountants, their development alone is not sufficient without the concomitant development of new standards. For these technological advances to be used effectively, there must be a concurrent effort to create standards that facilitate the understanding of new data and methodologies. Meeting these challenges requires a proactive approach by professional accountants, involving the development of a diverse set of skills and credentials tailored to future careers in accountancy. This strategic preparation will enable accountants not only to navigate the changes ahead, but also to anticipate potential problems. It will also enable them to seize the opportunities presented by the evolving accounting landscape and ensure that they remain adaptable and innovative in their practice. The symbiotic relationship between technological evolution, standardisation and skills development is critical for the accounting profession to successfully navigate the complexities of the modern era, as highlighted in [17].

Conclusion

This review article explores the dynamic intersection of forensic accounting and evolving technologies. Initially defining forensic accounting as the application of financial skills and an investigative mindset, it highlights the integral role of IT and AI in enhancing the attention to detail and validation of forensic accounting work. The integration of AI into audits has been shown to increase efficiency and improve quality of service, particularly by reducing manpower requirements. Advanced technologies such as data analytics, blockchain, AI, and ML have had a significant impact on forensic accounting, broadening its scope and increasing efficiency. Automation tools, including data mining and AI, are widely used to uncover hidden patterns and predict financial trends. The study delves into digital forensics, fraud detection, compliance, and cybersecurity, highlighting their central role in modern forensic accounting. It also addresses challenges and ethical considerations, including the complex technical-ethical tensions in automated communications analysis and IoT forensics. The review concludes with a forward-looking perspective on the future trends and implications of emerging technologies, such as blockchain, in reshaping the roles of accounting professionals and the potential transformative impact on accounting research.

The future of forensic accounting lies at the intersection of technology and financial investigation. As blockchain technology gains prominence, accounting professionals will need to acquire new skills to navigate the evolving landscape. The role of auditors is expected to change, highlighting the need for a realignment of the focus of internal audit. Further research is needed into the impact of technological and regulatory changes on accounting firms and practitioners, acknowledging both positive innovations and the potential job changes they may bring.

The rise of financial robots from major accounting firms suggests a paradigm shift in automating routine tasks, enabling business managers with limited accounting knowledge to make informed decisions. The integration of emerging technologies such as big data, ML, AI, and blockchain into the accounting process has been identified as a major trend, requiring simultaneous efforts to establish new standards for data understanding and working methods. Forensic accounting professionals are advised to develop a diverse set of skills to adapt to change, anticipate problems, and capitalize on potential opportunities in this rapidly changing accounting landscape.

Data Availability Statement

"The data presented in this study are available as stated and involved in the references".

Conflicts of Interest

"The authors declare no conflict of interest".

References

1. Ahluwalia, K., Abernathy, M. J., Beierle, J., Cauchon, N. S., Cronin, D., Gaiki, S., Xue, G. (2022). The future of CMC regulatory submissions: Streamlining activities using structured content and data management. Journal of Pharmaceutical Sciences, 111(5), 1232-1244.
2. Altman, N., Krzywinski, M. (2017). Ensemble methods: Bagging and random forests. Nature Methods, 14(10), 933-935.
3. Asuquo, A. I. (2012). Empirical analysis of the impact of information technology on forensic accounting practice in Cross River State–Nigeria. International Journal of Scientific and Technology Research, 1(7), 25-33.
4. Aziz, L. A. R., Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.
5. Bologna, G. J., Lindquist, R. J. (1995). Fraud auditing and forensic accounting: New tools and techniques (2nd ed.). John Wiley & Sons.
6. Choi, H., Kim, M., Lee, G., Kim, W. (2019). Unsupervised learning approach for network intrusion detection system using autoencoders. The Journal of Supercomputing, 75(12), 5597-5621.
7. Dreyer, K. (2014). A history of forensic accounting (Honors Projects No. 296). Grand Valley State University. https://scholarworks.gvsu.edu/honorsprojects/296
8. Fedyk, A., Hodson, J., Khimich, N., Fedyk, T. (2022). Is artificial intelligence improving the audit process? Review of Accounting Studies, 27(3), 938-985.
9. Fischer, M. T., Hirsbrunner, S. D., Jentner, W., Miller, M., Keim, D. A., & Helm, P. (2022). Promoting ethical awareness in communication analysis: Investigating potentials and limits of visual analytics for intelligence applications. In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, 21-24.
10. Giblin, C., Müller, S., & Pfitzmann, B. (2006). From regulatory policies to event monitoring rules: Towards model-driven compliance automation (IBM Research Report RZ-3662). IBM Research Zurich. https://dominoweb.draco.res.ibm.com/reports/rz3662.pdf
11. González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.
12. Goodman, N. R. (1963). Statistical analysis based on a certain multivariate complex Gaussian distribution (an introduction). The Annals of Mathematical Statistics, 34(1), 152-177.
13. Grossman, M. R., Cormack, G. V. (2011). Technology-assisted review in e-discovery can be more effective and more efficient than exhaustive manual review. Richmond Journal of Law & Technology, 17(3), 11.
14. Grossman, M. R., Cormack, G. V. (2011). Technology-assisted review in e-discovery can be more effective and more efficient than exhaustive manual review. Richmond Journal of Law & Technology, 17(3), 11.
15. Honigsberg, C. (2020). Forensic accounting. Annual Review of Law and Social Science, 16, 147-164.
16. Kafi, M. A., Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. American Journal of Trade and Policy, 10(1), 15-26.
17. Kroon, N., do Céu Alves, M., Martins, I. (2021). The impacts of emerging technologies on accountants' role and skills: Connecting to open innovation—a systematic literature review. Journal of Open Innovation: Technology, Market, and Complexity, 7(3), 163.
18. Kunwar, M. (2019, August). Artificial intelligence in finance: Understanding how automation and machine learning is transforming the financial industry (Master's thesis, Centria University of Applied Sciences, Finland). Theseus. https://www.theseus.fi/bitstream/handle/10024/227560/Manju%20Kunwar%20Thesis.pdf?sequence=2
19. Lavanya, P. M., Sasikala, E. (2021). Deep learning techniques on text classification using natural language processing (NLP) in social healthcare network: A comprehensive survey. In 2021 3rd International Conference on Signal Processing and Communication (ICSPC) 603-609.
20. Losavio, M. M., Chow, K. P., Koltay, A., James, J. (2018). The Internet of Things and the smart city: Legal challenges with digital forensics, privacy, and security. Security and Privacy, 1(3), e23.
21. Phua, C., Lee, V., Smith, K., Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv. https://doi.org/10.48550/arXiv.1009.6119
22. Pronoza, P., Chernyshov, V., Ye, M., Aleksieienko, I. (2023). Optimization of business processes in investment using automation technology, financial calculations, and risk assessment methods. Eastern-European Journal of Enterprise Technologies, 122(13).
23. Quick, D., Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11(4), 273-294.
24. Raghavan, S. (2013). Digital forensic research: Current state of the art. CSI Transactions on ICT, 1, 91-114. https://doi.org/10.1007/s40012-012-0008-7
25. Singleton, T. W., Singleton, A. J. (2010). Fraud auditing and forensic accounting. John Wiley & Sons.
26. Slater, M., Gonzalez-Liencres, C., Haggard, P., Vinkers, C., Gregory-Clarke, R., Jelley, S., Silver, J. (2020). The ethics of realism in virtual and augmented reality. Frontiers in Virtual Reality, 1, 1.
27. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, 22(2),

1191-1221.

28. Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Rahman, M. H. (2021). Blockchain and artificial intelligence technology in e-health. Environmental Science and Pollution Research, 28, 52810-52831.
29. Wagner, T. D., Mahbub, K., Palomar, E., Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.
30. West, J., Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47-66.
31. Zhang, D., Zhou, L. (2004). Discovering golden nuggets: Data mining in financial application. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 34(4), 513-522.
32. Zhang, Y., Xiong, F., Xie, Y., Fan, X., Gu, H. (2020). The impact of artificial intelligence and blockchain on the accounting profession. IEEE Access, 8, 110461-110477.