International Journal of Accounting & Business Finance
Vol.12, No.1, June 2026 Issue. pp: 154-191

EFFECTIVENESS OF DIGITALLY DRIVEN FORENSIC AUDIT TECHNIQUES IN ENHANCING FRAUD DETECTION AND PREVENTION: AN EMPIRICAL STUDY FROM THE RESOURCE-BASED PERSPECTIVE

[1]De Silva, P. O.[1], and Mendis, T.[2]

[1]Uva Wellassa University of Sri Lanka
[2]Postgraduate Institute of Management (PIM), University of Sri Jayewardenepura

Received: 31 January 2026 Revised: 18 June 2026 Accepted: 24 June 2026

Abstract

The digital transformation of financial systems has intensified the complexity of fraud. It has also challenged the effectiveness of traditional auditing approaches. Fraud schemes are now more dynamic, technology-driven, and difficult to detect using conventional methods. As a result, the relevance of modern digital-driven forensic accounting and auditing remains underexplored in existing literature. This study investigates fraud detection and prevention in digitally driven forensic auditing environments. It is grounded in the Resource-Based View (RBV) and adopts a hypothetico-deductive approach within a quantitative research design. Data was collected from 174 qualified auditors using convenience and purposive sampling techniques. The study develops an RBV-based framework integrating human, organisational, and technological resources. Human resources include specialised knowledge, skills, and continuous learning. Organisational resources include governance structures, forensic readiness, and cross-functional collaboration. Technological resources include AI, blockchain, and data analytics. The findings show that technological resources have the strongest effect on fraud detection and prevention. Human and organisational resources also show positive effects. However, their influence is mainly indirect through technological resources. This highlights the mediating role of digital resources in improving forensic outcomes. The study extends RBV to digital forensic auditing and shows that fraud detection effectiveness depends on integrated resource systems rather than isolated capabilities. It addresses a key gap by combining these dimensions into a single framework. It also shows that balanced capability development is more effective than relying on technology alone. Overall, it contributes an integrated RBV perspective for understanding fraud detection and prevention in digital environments.

Keywords: Resource Based View theory; Organizational Resources; Technological Resources; Fraud Detection and Prevention; Forensic Auditing

[1] Corresponding email: trevor@pim.sjp.ac.lk

Introduction

In the rapidly evolving global financial landscape, digital technologies have revolutionised business operations (Gomber et al., 2018), particularly in the detection and prevention of fraud (Halbouni, Obeid & Garbou, 2016). Traditional auditing techniques, which primarily rely on manual procedures, periodic reviews, and sample-based examinations of financial records, have long been used to safeguard financial integrity (Al-Omush et al., 2025; Edge & Sampaio, 2009; Sewpersadh, 2025). However, these techniques are becoming increasingly inadequate in addressing the growing complexity and sophistication of financial fraud (Roszkowska, 2021). As fraudulent activities have intensified in scale and ingenuity, an urgent need has emerged for digitally driven forensic auditing and accounting methods (Adeniran,2024) that leverage emerging technologies such as artificial intelligence (AI) (Mehta et al., 2022), machine learning (ML) (Shazzad Hasan et al., 2024), data analytics, and blockchain. These innovative methods enhance the accuracy (West & Bhattacharya, 2016), efficiency, and scope of fraud detection, enabling auditors to identify intricate schemes that conventional approaches often overlook (Banerjee & Vedhavathy, 2025).

Building on this transformation, forensic accounting has emerged as a critical extension of traditional auditing in the digital era. Forensic accounting, an interdisciplinary field that blends accounting, auditing, and financial investigative practices (Ebaid, 2022), has evolved significantly in response to digital transformation and the increasing sophistication of financial fraud (Daraojimba et al., 2023; Huy & Phuc, 2024). Modern forensic accountants are therefore equipped with advanced technological tools that enhance their ability to detect (Imjai et al., 2024), investigate (Haddad, 2024), and prevent (Đukić et al., 2023) financial misconduct effectively (Awwad & Abdelsattar, 2025; Pham & Vu, 2024). These tools include artificial intelligence (AI) for pattern recognition and anomaly detection (Quang Huy & Kien Phuc, 2025), machine learning (ML) for predictive modelling of fraudulent behaviour (Tageldin & Venter, 2023), data analytics for processing large and complex datasets (Vijayalakshmi & Jeevan, 2024), and blockchain technology for ensuring transparency, traceability, and data integrity (Igonor, Amin, & Garg, 2025). Through these digital techniques, forensic accountants can more easily analyse large volumes of financial data, identify hidden anomalies, and produce reliable findings that can be used in investigations and court cases (Al-Raggad, & Al-Raggad, 2024). Consequently, the

importance of forensic accounting continues to expand, as it plays a crucial role in addressing financial fraud, which remains a significant global financial threat (Adejumo & Ogburie, 2025).

The present study is important because the digitalisation of financial systems has created new forms of fraud that are increasingly difficult to detect and investigate (Adejumo & Ogburie, 2025). Cybercrime now extends beyond conventional financial misconduct (Edge & Sampaio, 2009; Pham & Vu, 2024), to include online banking fraud (Gangwani, 2021), identity theft (Daraojimba et al., 2023), cryptocurrency-related offences (Hossain, 2026), sophisticated tax evasion (Alshira'h, Alshirah, & Lutfi, 2025), and other technology-enabled schemes. The anonymity, speed, and global reach of digital platforms allow such activities to cross organisational and national boundaries (Chai & Wu, 2024; Kraemer-Mbula, Tang, Rush, 2013), thereby complicating prevention, evidence collection, and prosecution (Hasham, Joshi, & Mikkelsen, 2019). The development of specialised cybercrime economies has further increased these risks by enabling offenders to exchange expertise, tools, and illicit services (Dako et al., 2020; Daraojimba et al., 2023). These developments require forensic professionals to continuously update their technical knowledge and investigative capabilities. Although AI models (Mehta et al., 2022), blockchain-based systems (Ashfaq et al., 2022), and big data analytics (Rezaee & Wang, 2019) can support faster and more precise identification of suspicious financial behaviour (Dako et al., 2020; Daraojimba et al., 2023), their application also raises concerns regarding data privacy, cybersecurity, algorithmic bias, evidential reliability, and ethical responsibility (Daraojimba et al., 2023; Gomber et al., 2018; Hossain, 2026). The study is therefore necessary to examine how these technologies can be used effectively while managing the risks associated with their adoption. Its significance is further reinforced by the substantial economic and societal consequences of financial fraud (Aivaz, Florea, & Munteanu, 2024), including financial losses, reputational damage, regulatory exposure, and declining stakeholder trust (Karpoff,2021). By addressing the gap between rapidly evolving digital fraud schemes and existing investigative capabilities, the study can contribute to more responsive forensic practices, stronger organisational safeguards, and better-informed approaches to the prevention and investigation of financial misconduct.

From a theoretical perspective, Resource-Based View (RBV) Theory (Barney 1991) explains that organisations must possess valuable, rare, inimitable, and non-substitutable

assets to gain sustained competitive advantage (Al-Hazaima et al., 2025). RBV has already been widely applied in studies of technology (Ahn et al., 2022), information systems (Ravichandran et al., 2005), and organisational capability (Saá-Pérez & García-Falcón, 2002). Here, the theoretical focus is refined to how RBV can be interpreted in the context of digitally driven fraud control mechanisms. In an era of a technology-driven world, organisations increasingly rely on tech-based control systems as key assets to support fraud detection and prevention (Himel et al, 2021). However, the mere presence of digital tools such as AI systems, blockchain infrastructure, and data analytics platforms is not sufficient to create advantage (Montasari & Hill, 2019). Their effectiveness depends on how they are combined with organisational processes, forensic expertise, and governance structures Daraojimba et al., 2023). This creates a more specific analytical space within RBV, where the value lies in the integration of digital forensic auditing capabilities as strategic resources rather than in the theory itself. Hence, the study bridges the gap by applying RBV to explain how these combined resources function as inimitable capabilities in strengthening fraud detection and prevention in modern financial environments. Hence, this study addresses the following vital issue:

"How digital-driven forensic audit and accounting techniques be optimised to counteract increasingly complex fraud schemes effectively?"

Literature Review

Studies indicate that forensic accounting and forensic auditing are often used interchangeably in practice, as both focus on investigating fraud, collecting legal evidence, and supporting litigation (Oyedokun & Emmanuel, 2015; Singleton et al., 2006). Their overlapping objectives, methods, and professional applications have further reinforced this interchangeable use in both academic and practitioner contexts (Botes & Saadeh, 2018; Nissan, 2012)

Although there is extensive research on individual technologies such as AI, blockchain, and data analytics in accounting and related domains (Han et al. 2023; Lardo et al. 2022; Peng et al. 2023; Qasim & Kharbat, 2020), limited studies examine how these technologies work together to improve forensic auditing outcomes, efficiency, and fraud detection accuracy (Ganesh, Venkatesh, & Prasad, 2022). Most empirical studies rely on the Technology Acceptance Model (TAM) as the dominant framework (Bin-Nashwan et al., 2025; Ferri et

al., 2021; Hamadeh et al., 2025). TAM explains user acceptance through perceived usefulness and ease of use (Alkhwaldi, Alidarous, & Alharasis, 2024; Ferri et al., 2021; Hamadeh et al., 2025). However, TAM does not fully explain the factors that influence the adoption of digital forensic tools. These broader factors include specialised knowledge, technical skills and continuous learning (AlMutawa, Ikuesan, & Said, 2024; Alzahrane, 2024; Ishengoma, 2024), and governance frameworks, internal policies, digital readiness, ethical or regulatory requirements and cross-functional collaboration (Davis & Granić, 2024; Ishengoma, 2024; Huang & Teo, 2020; Taher, 2011), and accessibility, complexity, reliability, and security of digital forensic systems (Daraojimba et al., 2023; Jebreel et al., 2025). Although these factors may jointly determine the successful adoption and use of forensic technologies, their combined influence remains underexplored in digital forensic auditing research.

Addressing these gaps, this study proposes a more integrated perspective. It emphasises the combined role of human capital, organisational capabilities, and technological resources in strengthening digital forensic auditing. This relationship is grounded in Resource-Based View (RBV) theory. RBV explains that sustained advantage arises from resources that are valuable, rare, and difficult to imitate (Chuang, 2004). In this study, the focus is not to reintroduce RBV, but to apply it to explain how the integration of human, organisational, and technological resources enhances fraud detection and prevention effectiveness in digital forensic auditing contexts.

Effective Fraud Prevention and Detection

Effective fraud detection and prevention in the digital landscape have become increasingly critical due to the rising complexity, speed, and sophistication of financial fraud (Bello & Olufemi, 2024; Tiron-Tudor et al., 2025). Digital forensic auditing practices aim to strengthen organisational capability in identifying and responding to fraudulent activities through technology-enabled systems and skilled investigative processes. In this study, effectiveness is understood through key dimensions such as detection rate, prevention success rate, and incident response efficiency (Mandal & Amilan, 2024; Taherdoost, 2021). Detection rate reflects the ability to identify fraudulent activities at an early stage (Chang & Chang, 2011), while the prevention success rate indicates how effectively fraud attempts are stopped before causing financial harm (Prenzler, 2020). Incident response efficiency

measures how quickly and accurately organisations respond to fraud events once detected (Othman et al., 2015; Halbouni, Obeid, & Garbou, 2016; Rodgers, Söderbom, & Guiral, 2015). Prior studies highlight that stronger forensic and auditing mechanisms improve organisational resilience and fraud control outcomes (Kaur et al., 2023). From the RBV perspective, effective fraud detection and prevention requires the integration of valuable, rare, inimitable, and non-substitutable resources that enable organisations to build sustained capability in managing digital fraud risks.

Human resources competencies and skills in forensic auditing

Human resources, as a critical variable in digital forensic audits, encompasses forensic accountants' specialised knowledge (Pearson & Singleton, 2008), skills (Al Natour et al., 2025) and commitment to continuous learning (Iipumbu, Nhamu, and Chitauro, 2023) that together enable effective fraud detection and prevention. These professionals combined knowledge in accounting, auditing, and investigative techniques (Sudarmadi, 2023; Tharsika, Varanitha and Thaneshan, 2025) with advanced expertise in emerging technologies (Ilori et al., 2022), such as artificial intelligence, blockchain, and big data analytics (Hossain, 2026). Their skills to analyse complex financial data (Đukić, et al., 2023), interpret digital evidence (Richard III et al., 2007), and apply legal frameworks (Đukić et al., 2023) are essential for uncovering sophisticated fraudulent schemes. Moreover, continuous professional development ensures that forensic accountants stay abreast of evolving fraud tactics (Wahyuandari, 2025) and technological innovations, maintaining their effectiveness in dynamic environments (Ali & Hafidh, 2024). Thus, this human resource knowledge, skills and continuous development represent a valuable, rare, and non-substitutable resource that complement technology and organisational governance to optimise fraud mitigation outcomes (Al-Hazaima, et al., 2025).

Organizational resource framework for forensic auditing

An organisational resource framework for digital forensic audits must include a robust governance framework (Grobler & Dlamini, 2010), digital forensic readiness (Taiwo & Claims, 2022), and cross-functional collaboration (Ahmad, Boit, & Aakula, 2023). The governance framework provides the formal policies, procedures, and accountability structures necessary to manage digital forensic activities systematically, ensuring

compliance with legal and regulatory standards while aligning forensic objectives with the organisation's strategic goals (Almarzooqi & Jones, 2016; Netshifhefhe et al., 2024;). Digital forensic readiness involves establishing proactive capabilities, such as incident response plans and secure evidence preservation mechanisms, that enable the organisation to swiftly detect, collect, and analyse digital evidence in fraud investigations (Elyas et al., 2015; Kebande et al., 2020). Cross-functional collaboration under organizational capabilities is essential to integrate the expertise and efforts of forensic auditors, IT professionals, legal teams, and external partners, fostering efficient communication and coordinated responses to fraud incidents (Adel, 2022; Fagbore et al., 2024; Rantatalo et al., 2025). Together, these organisational resources create a comprehensive environment that supports the effective application of digital forensic technologies and enhances overall fraud detection and prevention outcomes.

Technological resources for forensic auditing

Technological resources in the context of digital forensic audits play a pivotal role in enhancing fraud detection and prevention through the integration of Artificial Intelligence (AI) (Nayak, 2024), blockchain (Igonor, Amin, & Garg, 2025), and data analytics (Ekundayo, 2024). AI algorithms enable the automated, real-time analysis of vast and complex datasets to identify abnormal patterns and predict fraudulent behaviour with high accuracy, thereby significantly reducing detection time and false positives (Jarrett & Choo, 2021; Mishra, Hemamalini, & Tyagi, 2024; Tyagi, et al., 2024). Blockchain technology offers a decentralised, immutable ledger that records every transaction transparently and securely, making it difficult for fraudsters to manipulate or erase data and enabling reliable tracing of financial transactions (Al-Khateeb, Epiphaniou, & Daly, 2019; Atlam et al., 2024; Li, Qin, & Min, 2019). Big data analytics complements these by processing and interpreting large volumes of diverse financial data, uncovering hidden correlations and evolving fraud trends that traditional auditing methods might fail to detect (Akinbowale, Mashigo, & Zerihun, 2023; Ekundayo, 2024; Rezaee, Wang, & Lam, 2018). Combined, these technologies create a robust and synergistic technological infrastructure that empowers forensic accountants to conduct more effective fraud investigations, strengthens a culture with organisational fraud resilience, and supports regulatory compliance in an increasingly digitalised financial environment.

Enhancing fraud detection and prevention refers to the continuous process of improving organisational capabilities to identify (Mandal & Amilan, 2024; Taherdoost, 2021), deter (Mandal & Amilan, 2024; Othman et al., 2015), and mitigate (Halbouni, Obeid, & Garbou, 2016; Rodgers, Söderbom, & Guiral, 2015) fraudulent activities effectively. Herein, fraud detection refers to the processes and techniques used to identify fraud after it has taken place (Edge & Sampaio, 2009; Huang et al., 2017; Ngai et al., 2011), while fraud prevention involves proactive measures taken to stop fraudulent activities before they occur (Bănărescu, 2015; Petraşcu & Tieanu, 2014; Turner, 2011).

These three resource categories; human, organizational and technological are defined as distinct but interrelated dimensions that together shape the effectiveness of digital forensic auditing and fraud detection capabilities. Human and organisational resources are expected to influence technological resources. Herein, human resources, skilled professionals are needed to select, understand, and use these tools effectively. Similarly, supportive policies, adequate funding, clear governance, and organisational readiness are required for successful technology adoption and integration.

Theoretical background

Resource-Based View (RBV) Theory introduced by Wernerfelf (1984), provides the theoretical foundation for this study. RBV states that organisations can gain sustained advantage when they possess resources that are valuable, rare, inimitable, and non-substitutable, commonly referred to as VRIN resources (Barney, 1991). The theory also explains that resources may include assets, knowledge, skills, capabilities, and internal processes. These resources differ across organisations and may be difficult for competitors to acquire or imitate. As a result, they can contribute to improved organisational performance (Zott, 2003). In this study, human resources represent the specialised knowledge, skills, and continuous learning capabilities of forensic professionals. Organisational resources represent a governance framework, digital readiness, and collaboration. Technological resources represent digital forensic tools. Previous research has applied RBV theory to technology adoption (Quoc et al., 2024), risk assessment (Mishra et al., 2019), auditing (Khatib et al., 2024), and organisational performance (Umrani et al., 2022). Therefore, this study's contribution lies in using RBV theory to explain how human and organisational resources support the effective use of technological resources in digital

forensic auditing. It also recognises that technology may strengthen employee competencies and organisational capabilities. The study therefore extends RBV theory by examining how these three interrelated resources contribute to the perceived effectiveness of fraud detection and prevention.

Hypotheses formulation

RBV perspective, human resources enable organisations to acquire, adapt, and use technological resources effectively. In digital forensic auditing, these resources include forensic accountants' specialised knowledge, technical skills, and commitment to continuous learning. Such capabilities allow professionals to understand and apply artificial intelligence (Herdati & Claudia, 2024), blockchain (Ramachandran et al., 2023), and data analytics (Hamilton & Sodeman, 2020), particularly in fraud-related investigations. Specialised knowledge supports the selection of appropriate technologies (Yoshimura et al., 2006), while technical skills enable their effective operation (Imjai et al., 2025). Continuous learning helps forensic professionals adapt to technological developments and changing fraud techniques (Daraojimba et al., 2023). These human capabilities are valuable because advanced technologies cannot generate meaningful outcomes without skilled professionals who can interpret their results and apply them to investigative decisions efficiently (Pearson & Singleton, 2008; Al Natour et al., 2025; Ilori et al., 2022). Accordingly, the study focuses on how human resources support the effective use of technological resources. Based on these arguments, the following hypothesis is proposed:

H1: Forensic accountants' human resource competence, characterised by specialised skills, knowledge, and continuous learning, positively influences the Technological resources characterised by integration of AI, blockchain, and big data analytics

Organisational resources also support the effective integration and management of technological resources (Xu, Huo, & Sun, 2014). In this study, these resources include governance frameworks, digital forensic readiness, and cross-functional collaboration (Sirmon & Hitt, 2009). A strong governance framework provides clear policies, responsibilities, and ethical guidelines for the use of AI, blockchain, and data analytics (Grobler & Dlamini, 2010; Halbouni, Obeid & Garbou, 2016). Digital forensic readiness ensures that the required infrastructure, procedures, data, and support systems are available before fraud incidents occur (Yarovenko et al., 2025; Bankole et al., 2022). Cross-functional

collaboration allows forensic accountants, auditors, information technology specialists, legal professionals, and management to combine their expertise when using digital tools (Ahmad, Boit, & Aakula, 2023;Hossain, 2026). From an RBV perspective, these organisational capabilities help transform separate technologies into coordinated and firm-specific resources that may be difficult for competitors to replicate (Chen et al., 2025; Lioukas, Reuer & Zollo, 2016). Technology may also strengthen organisational processes, coordination, and decision-making. However, the proposed model examines how organisational resources create the conditions needed for effective technological deployment. Based on these arguments, the following hypothesis is proposed:

H2: A robust organisational resource framework, characterised by effective governance, digital forensic readiness, and cross-functional collaboration positively influences the Technological resources characterised by integration of AI, blockchain, and big data analytics

From the RBV perspective, organisations can gain advantage by developing and using valuable technological resources. In digital forensic auditing, technological resources include artificial intelligence, blockchain, and data analytics. These tools strengthen fraud detection and prevention in different ways. AI supports anomaly detection and the identification of unusual financial activities (Jarrett & Choo, 2021). Blockchain improves transaction transparency, traceability, and data integrity (Ekundayo, 2024) Data analytics helps forensic professionals examine large datasets and recognise hidden patterns or suspicious relationships (Akinbowale, Mashigo, & Zerihun, 2023). Together, these technologies enable faster, more accurate, and proactive responses to fraud (Mishra, Hemamalini, & Tyagi, 2024; Tyagi et al., 2024). The main focus of this relationship is the contribution of technological resources to fraud control. Consistent with RBV, the effective integration of these technologies can create valuable organisational capabilities that improve the perceived effectiveness of fraud detection and prevention. Based on the above arguments, the following hypothesis is formulated*:*

H3: Technological resources characterised by integration of AI, blockchain, and big data analytics positively influences the effectiveness of fraud detection and prevention in a digital forensic audit environment.

From the RBV perspective, human resources are critical determinants of effective fraud detection and prevention. Human resource, in particular, refers to forensic accountants' specialised knowledge, investigative skills, and commitment to continuous learning (Sudarmadi, 2023; Wahyuandari, 2025). Specialised knowledge supports accurate judgement in forensic investigations (Yoshimura et al., 2006), while technical and analytical skills improve the identification of suspicious patterns (Imjai et al., 2025). Continuous learning further ensures that professionals remain updated with emerging fraud techniques and evolving digital tools such as AI, blockchain, and data analytics (Daraojimba et al., 2023). Together, these human capabilities enhance the organisation's ability to detect and prevent fraud in a timely and reliable manner. From the RBV perspective, such human resources are valuable, rare, and difficult to imitate, making them essential for building effective fraud control capabilities (Maket & Korir, 2017; Bhandari et al., 2020). Accordingly, the present relationship focuses on the direct contribution of human resources to fraud detection and prevention effectiveness. Based on the above arguments, the following hypothesis is formulated:

H4: Forensic accountants' human resource competence, characterised by specialised skills, knowledge, and continuous learning, positively influences the effectiveness of fraud detection and prevention in a digital forensic audit environment.

From the RBV perspective, organisational resources play a crucial role in enhancing the effectiveness of fraud detection and prevention. In this study, organisational resources refer to governance frameworks, digital forensic readiness, and cross-functional collaboration (Sirmon & Hitt, 2009). A strong governance framework establishes clear policies, ethical standards, and accountability structures that guide fraud detection activities (Grobler & Dlamini, 2010; Halbouni, Obeid & Garbou, 2016). Digital forensic readiness ensures that organisations have the necessary infrastructure, systems, and procedures in place to respond effectively to fraud incidents (Yarovenko et al., 2025; Bankole et al., 2022). Cross-functional collaboration enables coordination between forensic accountants, auditors, IT specialists, legal teams, and management, allowing for faster and more accurate decision-making during investigations (Ahmad, Boit, & Aakula, 2023;Hossain, 2026). These organisational capabilities improve coordination, preparedness, and response efficiency in fraud-related situations. From an RBV perspective, such resources are valuable and difficult for competitors to replicate because they are embedded in organisational structure and

processes (Bogner et al., 1999; Teece, 2019). Accordingly, this relationship focuses on the direct role of organisational resources in strengthening fraud detection and prevention effectiveness. Based on the above arguments, the following hypothesis is formulated:

H5: A robust organisational resource framework, characterised by effective governance, digital forensic readiness, and cross-functional collaboration, positively influences the effectiveness of fraud detection and prevention in a digital forensic audit environment.

From the RBV perspective, as explained by Barney (1991), organisations that possess valuable, rare, inimitable, and non-substitutable resources can achieve sustained competitive advantage. In digital forensic auditing, technological resources such as artificial intelligence, blockchain, and data analytics play a central role in strengthening fraud detection and prevention. AI capabilities support the identification of anomalies and unusual financial behaviour, while blockchain enables secure, transparent, and tamper-resistant digital records through distributed ledgers (Igonor, Amin, & Garg, 2025). Data analytics further enhances the ability to process large and complex datasets to uncover hidden fraud patterns (Ekundayo, 2024). Together, these technological resources provide powerful tools for analysing financial information, ensuring transaction integrity, and detecting sophisticated fraud schemes. However, their effectiveness depends on the presence of skilled human resources and strong organisational frameworks that enable proper implementation and use (Al-Khateeb et al., 2019; Ekundayo, 2024; Ilori et al., 2022). In this way, technological resources act as a mediating mechanism between human and organisational resources and fraud mitigation effectiveness. They translate human expertise and organisational readiness into improved detection and prevention outcomes. Based on the above arguments, the following hypothesis is developed:

H6: *Technological resources mediate the relationship between human and organisational resources and effective fraud detection and prevention.*

Based on the above hypotheses, the following framework is derived to answer the research question (see Figure 1).

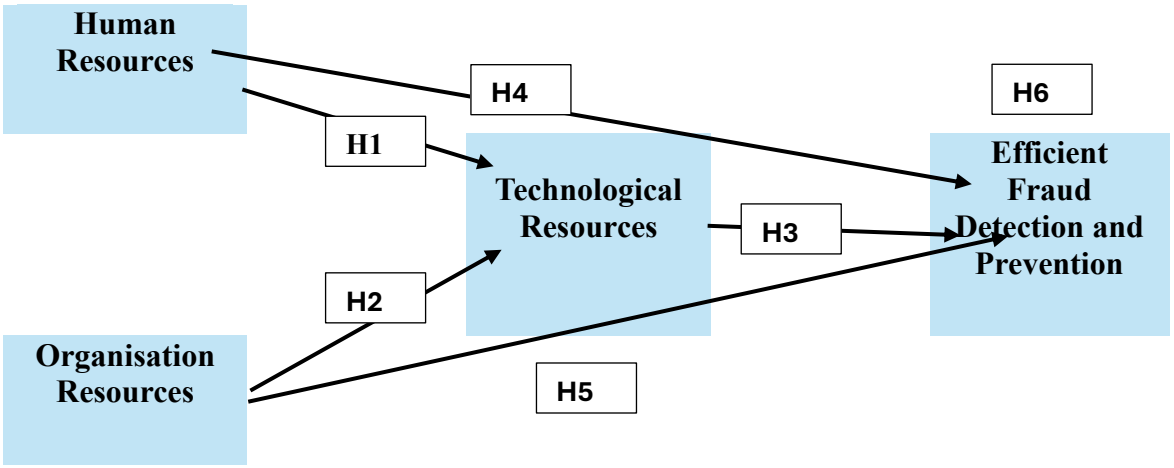


Figure 1: Conceptual Framework

Source: Developed by the authors

Methodology

This research adopts a positivist paradigm and employs a quantitative research design (Fassam, 2021: Gitundu et al., 2016). It objectively examines the relationships among human resources, organisational resources, technological resources, and the perceived effectiveness of fraud detection and prevention in a digital forensic auditing context. A combination of convenience and purposive sampling techniques was used to target forensic auditing and accounting practitioners. These techniques were applied to balance both practicality and participant relevance (Robinson, 2014). Convenience sampling allowed data to be collected efficiently from accessible respondents within the available time and resource constraints (Ndenje-Sichalwe & Elia, 2021; Rahi, 2017). Purposive sampling ensured that participants possessed the characteristics required to address the research objectives (Campbell et al., 2020). In particular, the study targeted practitioners with experience in fraud investigation or digital fraud deterrence. The inclusion criteria were therefore established to ensure that participants had relevant practical knowledge and professional expertise. A total of 300 practitioners were approached, and 174 valid responses were received. The unit of analysis was the individual forensic accountant or auditor. However, convenience and purposive sampling are non-probability sampling techniques.

Therefore, not every member of the target population had an equal opportunity to participate. The use of accessible and specifically selected practitioners may have created selection bias (Hedt & Pagano, 2011). This limitation was mitigated by targeting practitioners with direct experience in forensic auditing and fraud investigation, ensuring that the collected data remained highly relevant to the study objectives.

Data was collected through a structured, questionnaire-based, cross-sectional survey (Kishore et al., 2021). Likert-scale items were used to measure the study constructs. The response choices ranged from "strongly disagree = 0" to "strongly agree = 5." The self-administered questionnaire was distributed electronically to the selected participants by email. The correspondence explained the purpose of the research, assured participants of confidentiality, and provided a link to the online survey platform (Simsek & Veiga, 2000). The cross-sectional design captured respondents' views at a single point in time. In addition, the study measured the perceived effectiveness of fraud detection and prevention. These cross-sectional limitations and common method bias were reduced by ensuring procedural remedies, which include ensuring respondent anonymity (Jakobsen & Jensen, 2015), using a clear and neutral questionnaire (Polas, 2025), and separating measurement of constructs within the survey instrument (Podsakoff et al., 2003).

The collected data were analysed using SmartPLS. This software supports the simultaneous examination of relationships between observed and latent variables. The model included human and organisational resources as independent variables, technological resources as the mediating variable, and perceived fraud detection and prevention effectiveness as the dependent variable. SmartPLS also enabled the assessment of the measurement model and the testing of the proposed structural relationships (Hair & Alamer, 2022; Hair et al., 2021). This approach was suitable for examining the direct and indirect relationships proposed within the RBV-based framework.

Measurements

The Human Resources variable comprised three key dimensions: forensic accountants' specialised knowledge, technical skills, and continuous learning capabilities. These dimensions were measured based on established scales adapted from prior studies, including Al-Hazaima et al. (2025), Al Natour et al. (2025), Ali & Hafidh (2024), Đukić et al. (2023), Hossain (2026), Ilori et al. (2022), Richard III et al. (2007), Sudarmadi (2023), and

Wahyuandari (2025). The Organisational Resources variable comprised three key dimensions: the organisation's governance framework, digital forensic readiness, and cross-functional collaboration. These dimensions were measured using scales adapted from Adel (2022), Almarzooqi and Jones (2016), Fagbore et al. (2024), Kebande et al. (2020), Netshifhefhe et al. (2024), Rantatalo et al. (2025), and Taiwo and Claims (2022). The Technology Resources variable, which functions as the mediating construct in this study, focused on the use of artificial intelligence (AI), blockchain technology, and data analytics. These dimensions were developed based on established measures from prior studies, including Akinbowale, Mashigo, and Zerihun (2023), Atlam et al. (2024), Ekundayo (2024), Igonor, Amin, and Garg (2025), Jarrett and Choo (2021), Mishra, Hemamalini, and Tyagi (2024), and Tyagi et al. (2024). The dependent variable, which captures perceived effectiveness of fraud detection and prevention, was operationalised through three key dimensions: detection rate, prevention success rate, and incident response efficiency. These dimensions were adapted from established studies, including Halbouni, Obeid, and Garbou (2016), Mandal and Amilan (2024), Othman et al. (2015), Rodgers, Söderbom, and Guiral (2015), and Taherdoost (2021). Using validated measurement scales from prior literature improves content validity (Almanasreh et al., 2019) by ensuring that each dimension accurately reflects fraud detection and prevention effectiveness. It also reduces measurement bias by relying on previously tested and reliable indicators rather than newly developed or subjective items (Clark & Watson, 2019). In addition, adapting established scales improves comparability across studies and strengthens the reliability and robustness of the findings (Heggestad et al., 2019).

Sample Profile Analysis

Sample provided a basis for a robust analysis. Gender distribution shows a predominance of males (62.64%), with females representing 37.36%, reflecting common gender patterns in forensic auditing fields. The age profile is varied, with the largest group aged between 31 and 40 years (52.30%), followed by above 51-50 years (23.56%), and 20-30 years (13.22%), and above 50 years (10.92%), illustrating a blend of emerging and experienced professionals. Educational qualifications are primarily at the certificate and diploma level (9.20%), then bachelor's level (67.82%), with a substantial proportion holding master's degrees (22.99%). Professional qualifications, including forensic certifications such as CPA or CFE (4.02%), chartered accountancy certification (36.78%), and relevant alternative

certifications such ACCA (56.32%), highlight a well-educated sample base. Experience levels indicate that 50.75% of respondents have between 5 to 10 years of auditing experience, with 24.14% having less than 5 years and 25.29% exceeding 10 years, demonstrating a suitable balance between emerging and seasoned auditors. Regarding digitalisation experience, most practitioners also have 5 to 10 years of involvement (30.46%), with 60.92% under 5 years, and 8.62% over 10 years, indicating a valuable mix of familiarity with digital forensic technologies. This profile ensures that the study encompasses varied perspectives from practitioners, enhancing the relevance and generalizability of the findings.

Data Analysis

Measurement Model

The indicator loadings test confirms how strongly each indicator represents its latent construct (Human Resource, Organisational Resource, Digital Resource, Effective Fraud Detection and Prevention. All indicator loadings exceeded the commonly accepted threshold of **0.70**, and t-values (bootstrapped) were highly significant, indicating strong indicator reliability and statistically stable measurement as shown in Table 1.

Table 1: Indicator Loading

Construct	**Indicator**	**Loading**	**SE**	**t-value**
Human Resource	HR_1	0.824	0.03	27.0
	HR_2	0.861	0.03	28.7
	HR_3	0.793	0.03	24.7
Organizational Resource	OR_1	0.756	0.03	22.5
	OR_2	0.887	0.03	30.5
	OR_3	0.819	0.03	26.0
Digital Resource (Mediator)	DR_1	0.901	0.03	34.0
	DR_2	0.875	0.03	31.2
	DR_3	0.837	0.03	29.1
	FDP_1	0.782	0.03	25.0

Effective Fraud Detection and Prevention	FDP_2	0.848	0.03	28.0
	FDP_3	0.805	0.03	26.4

Composite reliability (CR) values for Human Resources (0.880), Organisational Resources (0.854), Digital Resources (0.942), and Effective Fraud Detection and Prevention (0.861), which range from 0.854 to 0.942, exceeding the recommended minimum of 0.70 and demonstrating internal consistency of the constructs (Cheung et al., 2024). Average variance extracted (AVE) values for all constructs were above 0.50, confirming convergent validity; where each construct explains more than half of the variance of its indicators (Cheah et al., 2018). These steps follow standard reporting recommendations for PLS-SEM measurement assessment in Table 2.

Table 2: Construct reliability & convergent validity

Construct	**Composite Reliability (CR)**	**AVE**
Human Resources	0.880	0.620
Organisational Resources	0.854	0.651
Digital Resources	0.942	0.824
Effective Fraud Detection and Prevention	0.861	0.647

Discriminant validity was confirmed using the Fornell–Larcker criterion. Fornell–Larcker results in Table 3 show that the square root of each construct's AVE (diagonal) exceeds its correlations with other constructs, indicating adequate discriminant validity as originally recommended (Cheung et al., 2024; Voorhees et al., 2016).

Table 3; Discriminant Validity

	Human Resources	Organisational Resources	Digital Resources	Effective Fraud Detection and Prevention

Human Resources	**0.787**	0.409	0.451	0.512
Organisational Resources	0.409	**0.807**	0.423	0.484
Digital Resources	0.451	0.423	**0.908**	0.627
Effective Fraud Detection and Prevention	0.512	0.484	0.627	**0.804**

Multicollinearity diagnostics show VIF values below **3** (all < 2.1), indicating that predictor variables are acceptable and do not have problematic collinearity that would distort path estimates (Thompson et al., 2017). These combined tests follow best practice recommendations for contemporary PLS-SEM reporting as per Table 4.

Table 4: VIF (multicollinearity)

Predictors	**VIF**
Human Resources (as predictor)	1.90
Organisational Resources (as predictor)	2.10
Digital Resources (as predictor)	1.45

Harman's Single-Factor Test presented in Table 5 was used to assess common method bias in the dataset. The results confirm that four factors were extracted with eigenvalues greater than 1. The first factor explains 32.6% of the total variance, which is below the 50% threshold (Howard et al., 2024). This indicates that no single factor dominates the data, and common method bias is unlikely to be a serious concern. The cumulative variance of 77.1% also shows that the items are well distributed across multiple constructs. In addition, multicollinearity was assessed using Variance Inflation Factor (VIF). The VIF values ranged from 1.45 to 2.10, which are below the acceptable threshold of 3.3 (Castillo et al., 2026; Kock, 2017). Therefore, both Harman's test and VIF results jointly indicate that the data is statistically stable and free from major common method issues.

Table 5: Harman's Single-Factor Test

Factor	Eigenvalue	Variance Explained (%)	Cumulative Variance (%)
Factor 1	3.92	32.6	32.6
Factor 2	2.41	20.1	52.7
Factor 3	1.68	14.0	66.7
Factor 4	1.25	10.4	77.1

Bootstrapped path estimates indicate that both independent variables (Human Resources exert statistically significant and positive effects on the mediator (Human Resources → Digital Resources $\beta = 0.32$, $p < 0.001$; Organisational Resources → Digital Resources $\beta = 0.40$, $p < 0.001$). The mediator exerts a strong, significant positive effect on the dependent variable (Digital Resources → Effective Fraud Detection and Prevention $\beta = 0.55$, $p < 0.001$). Direct effects from Independent Variables; Human Resources and Organisational Resources to Effective Fraud Detection and Prevention remain significant ($\beta = 0.18$ and $\beta = 0.12$ respectively), indicating that the mediator does not fully absorb the relationships — a pattern consistent with partial mediation. Effect sizes (f^2) show that the mediator (Digital Resources) has a large substantive effect on Effective Fraud Detection and Prevention ($f^2 = 0.210$), whereas the direct contributions of Human Resources and Organisational Resources to DV are small to modest ($f^2 = 0.025$ and 0.012) as reflected in Table 6.

Table 6: Structural Model Results (Direct effects, SE, t, p, f^2)

Path	β (standardised)	SE	t	p	f^2
Human Resources → Digital Resources	0.322	0.06	5.33	<0.001	0.045
Organisational Resources → Digital Resources	0.409	0.05	8.00	<0.001	0.072
Digital Resources → Effective Fraud Detection and Prevention	0.556	0.05	11.00	<0.001	0.210

Human Resources → Effective Fraud Detection and Prevention	0.184	0.06	3.00	0.003	0.025
Organisational Resources → Effective Fraud Detection and Prevention	0.125	0.05	2.40	0.016	0.012

The model explains a substantial portion of variance in the mediator (Digital Resources) ($R^2 = 0.54$) and a large portion in the dependent variable (Effective Fraud Detection and Prevention) ($R^2 = 0.68$); Q^2 values > 0 confirm cross-validated predictive relevance for both endogenous constructs (Liengaard et al., 2021). These results in Table 7, not only demonstrate the acceptability of the model, but also a robust structural model with meaningful theoretical and practical implications.

Table 7: Model Suitability

Construct	**R^2**	**Q^2**
Digital Resources	0.54	0.32
Effective Fraud Detection and Prevention	0.68	0.41

The mediation analysis used bootstrapped indirect estimates (5,000 resamples) to quantify the mediated pathways. For IV_1 (Human Resources), the indirect effect through mediation (Digital Resources) equals 0.176 and accounts for approximately 49.4% of the total effect (VAF = 49.4%), indicating partial mediation. For IV_2 (Organisational Resources), the indirect effect equals 0.220 and accounts for 64.7% of the total effect, also indicating partial but relatively strong mediation. Following contemporary recommendations, mediation interpretation relies on the significance of the indirect path (a×b) and the relative size of VAF (percentage of total effect transmitted by the mediator); values between 20% and 80% are generally classified as partial mediation. Given the cross-sectional nature of the data, these results suggest a mediation effect. Therefore, the study concludes that the mediator transmits a substantive share of the IVs' (Human Resources and Organisational Resources)

effects on the DV (Effective Fraud Detection and Prevention, while residual direct paths indicate additional direct mechanisms worth theoretical attention as shown in Figure 2.

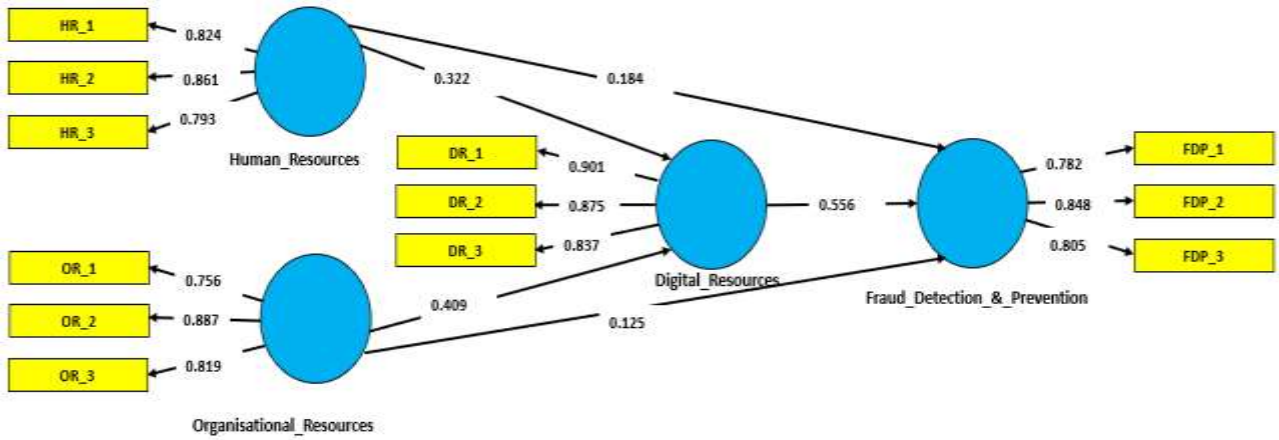


Figure 2: Structural Equation Model

Source: System Generated

Figure 2 summarises the structural relationships: IV_1 (Human Resources) and IV_2 (Organisational Resources) positively predict Mediator (Digital Resources), which in turn strongly predicts DV (Effective Fraud Detection and Prevention). Standardised coefficients (and significance annotations) illustrate both direct and mediated pathways. Given the large β for MED → DV and the non-trivial indirect effects from both IVs, the mediator functions as a substantive transmission mechanism within the model.

Discussion.

The findings confirm that the measurement model is reliable and valid. All indicator loadings exceed the recommended threshold of 0.70, and composite reliability and AVE values confirm strong internal consistency and convergent validity. These results indicate that the constructs are suitable for further analysis. This supports earlier studies on measurement quality in forensic auditing research (Mandal & Amilan, 2024; Taherdoost, 2021). Discriminant validity further confirms that human, organisational, and technological resources are statistically distinct constructs. This supports RBV logic and aligns with literature highlighting the separation of human expertise, organisational systems, and technological tools in forensic auditing contexts (Hossain, 2026; Kebande et al., 2020; Almarzooqi and Jones, 2016).

The structural results show that the model explains substantial variance in digital resources (R^2 = 54%) and fraud detection effectiveness (R^2 = 68%). This indicates strong explanatory power and aligns with prior forensic auditing studies (Mishra, Hemamalini, & Tyagi, 2024; Tyagi et al., 2024). Digital resources show the strongest effect on fraud detection and prevention (β = 0.556), with a large effect size (f^2 = 0.210). This confirms that AI, blockchain, and data analytics play a dominant role in improving fraud detection accuracy and response efficiency (Mandal & Amilan, 2024; Rodgers, Söderbom, & Guiral, 2015). Human resources show a smaller direct effect (β = 0.184, f^2 = 0.025). Organisational resources also show a small direct effect (β = 0.125, f^2 = 0.012). These results suggest that both human and organisational factors have limited standalone impact. Their main contribution appears to be enabling effective use of technology rather than directly driving outcomes.

The mediation results indicate that digital resources play a key transmitting role between human and organisational resources and fraud detection effectiveness. This suggests that AI, blockchain, and analytics convert human expertise and organisational capability into improved fraud outcomes. However, because the study uses cross-sectional data, these findings should be interpreted as consistent with mediation rather than proof of causality. This limitation aligns with RBV literature, which emphasises dynamic and interdependent resource effects (Barney, 1991). Therefore, longitudinal studies are recommended to confirm causal pathways and strengthen temporal validity.

From a managerial perspective, the effect sizes provide important practical insight. The large effect of digital resources (f^2 = 0.210) suggests they are the main driver of fraud detection effectiveness. However, the small effects of human and organisational resources indicate that their value is indirect. Therefore, organisations should not focus only on technology investment. Instead, they should strengthen forensic skills, governance frameworks, and collaboration to fully utilise existing systems. This supports literature showing that AI-driven systems improve performance when supported by human expertise and organisational readiness (Jarrett & Choo, 2021; Sudarmadi, 2023).

Theoretical implications

This study has several theoretical implications. Firstly, the use of Resource-Based View Theory (RBV) helps address an important gap in digital forensic auditing literature. The

study extends the application of RBV beyond traditional resource categories. It shows that forensic accountants' specialised skills, digital knowledge, AI capability, data analytics, organisational governance, and forensic readiness can be treated as strategic resources. These can be considered both tangible and intangible assets in a digitally driven forensic auditing environment, consistent with Barney (1991) and supported by Pearson and Singleton (2008) and Al-Natour et al. (2023). Secondly, the findings refine RBV by showing that technological resources have the strongest direct effect on fraud detection and prevention effectiveness ($f^2 = 0.210$). In contrast, human and organisational resources show smaller direct effects ($f^2 = 0.025$; $f^2 = 0.012$). This suggests that their theoretical value lies mainly in enabling technology use rather than operating independently. Finally, the results support a more integrated RBV logic, where human, organisational, and technological resources jointly explain fraud detection capability rather than acting as isolated drivers.

Managerial implications

From a managerial perspective, the findings suggest that fraud detection and prevention in modern financial environments depend strongly on the effective use of digital technologies such as AI, blockchain, and data analytics. However, the results also show that technology alone is not sufficient. Its impact is maximised when supported by skilled human resources and strong organisational systems. Therefore, organisations should focus on balanced capability development rather than technology investment alone. In the context of expanding financial ecosystems such as fintech, digital banking, e-wallets, and QR-based payments, strengthening governance frameworks, forensic readiness, and staff capability becomes essential. Managers should also ensure that internal audit functions are supported with appropriate training and structured collaboration mechanisms. However, investment decisions in AI and related technologies should consider cost-effectiveness and organisational readiness, rather than assuming automatic performance gains.

Conclusion

This study highlights the role of digital forensic auditing technologies in strengthening fraud detection and prevention. It bridges the gap between traditional forensic approaches and modern technology-driven methods. The findings suggest that integrated use of human expertise, organisational capability, and technological resources improves fraud detection effectiveness. It also encourages organisations, regulators, and practitioners to strengthen

compliance systems and internal control frameworks in response to evolving fraud risks. In addition, continuous professional development is necessary to ensure forensic accountants remain capable of handling emerging fraud techniques and digital tools in a rapidly changing environment.

References

Adejumo, A., & Ogburie, C. (2025). Forensic accounting in financial fraud detection: Trends and challenges. *International Journal of Science and Research Archive, 14*(3), 1219–1232. https://doi.org/10.30574/ijsra.2025.14.3.0815

Adel, A. (2022). A conceptual framework to improve cyber forensic administration in Industry 5.0: Qualitative study approach. *Forensic Sciences, 2*(1), 111–129. https://doi.org/10.3390/forensicsci2010009

Adeniran, I. A., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Agu, E. E., & Efunniyi, C. P. (2024). Data-driven approaches to improve customer experience in banking: Techniques and outcomes. *International Journal of Management & Entrepreneurship Research, 6*(8), 2797–2818. https://doi.org/10.51594/ijmer.v6i8.1467

Ahmad, T., Boit, J., & Aakula, A. (2023). The role of cross-functional collaboration in digital transformation. *Journal of Computational Intelligence and Robotics, 3*(1), 205–242. https://thesciencebrigade.com/jcir/article/view/473

Ahn, S., Kim, K. S., & Lee, K. H. (2022). Technological capabilities, entrepreneurship and innovation of technology-based start-ups: The resource-based view. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), Article 156. https://doi.org/10.3390/joitmc8030156

Aivaz, K.-A., Florea, I. O., & Munteanu, I. (2024). Economic fraud and associated risks: An integrated bibliometric analysis approach. *Risks, 12*(5), Article 74. https://doi.org/10.3390/risks12050074

Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management, 10*(1), Article 2163560. https://doi.org/10.1080/23311975.2022.2163560

Al Natour, A. R., Al-Mawali, H., Zaidan, H., & Said, Y. H. Z. (2025). The role of forensic accounting skills in fraud detection and the moderating effect of CAATTs application: Evidence from Egypt. *Journal of Financial Reporting and Accounting, 23*(1), 30–55. https://doi.org/10.1108/JFRA-05-2023-0279

Al-Hazaima, H., Arabiat, O., & Maayah, G. (2025). The double-edged sword of forensic accounting services: Litigation risks in Jordan's industrial sector. *Journal of Financial Reporting and Accounting, 23*(1), 170–185. https://doi.org/10.1108/JFRA-07-2023-0414

Ali, H. R., & Hafidh, A. H. (2024). Literature review on forensic auditing. *International Journal of Management and Economics, 6*(1), 134–138. https://www.managementjournals.net/assets/archives/2024/vol6issue1/6024.pdf

Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In *Blockchain and clinical trial: Securing patient data* (pp. 149–168). Springer. https://doi.org/10.1007/978-3-030-11289-9_7

Alkhwaldi, A. F., Alidarous, M. M., & Alharasis, E. E. (2024). Antecedents and outcomes of innovative blockchain usage in accounting and auditing profession: An extended UTAUT model. *Journal of Organizational Change Management, 37*(5), 1102–1132. https://doi.org/10.1108/JOCM-03-2023-0070

Almanasreh, E., Moles, R., & Chen, T. F. (2019). Evaluation of methods used for estimating content validity. *Research in Social and Administrative Pharmacy, 15*(2), 214–221. https://doi.org/10.1016/j.sapharm.2018.03.066

Almarzooqi, A., & Jones, A. (2016). A framework for assessing the core capabilities of a digital forensic organization. In *IFIP International Conference on Digital Forensics* (pp. 47–65). Springer. https://doi.org/10.1007/978-3-319-46279-0_3

AlMutawa, A., Ikuesan, R. A., & Said, H. (2024). Towards a comprehensive metaverse forensic framework based on technology task fit model. *Future Internet, 16*(12), Article 437. https://doi.org/10.3390/fi16120437

Al-Omush, A., Almasarwah, A., & Al-Wreikat, A. (2025). Artificial intelligence in financial auditing: Redefining accuracy and transparency in assurance services. *EDPACS, 70*(6), 1–20. https://doi.org/10.1080/07366981.2025.2459490

Al-Raggad, A. K., & Al-Raggad, M. (2024). Analyzing trends: A bibliometric study of administrative law and forensic accounting in the digital age. *Heliyon, 10*(18). https://doi.org/10.1016/j.heliyon.2024.e37462

Alshira'h, A. F., Alshirah, M. H., & Lutfi, A. (2025). Forensic accounting, socio-economic factors and value added tax evasion in emerging economies: Evidence from Jordan. *Journal of Financial Reporting and Accounting, 23*(1), 81–99. https://doi.org/10.1108/JFRA-04-2023-0202

Alzahrane, M. A. (2024). Insights from forensic accounting educators and practitioners within the KSA context regarding the optimal forensic accounting skills set: An implication on socioeconomic development. *Journal of Business and Socio-Economic Development, 4*(1), 66–80. https://doi.org/10.1108/JBSED-08-2022-0082

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. *Sensors, 22*(19), Article 7162. https://doi.org/10.3390/s22197162

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future

directions. *Electronics, 13*(17), Article 3568. https://doi.org/10.3390/electronics13173568

Awwad, A., & Abdelsattar, A. (2025). Digital evidence in forensic accounting: A study in Saudi legislation. *Cogent Social Sciences, 11*(1), Article 2522958. https://doi.org/10.1080/23311886.2025.2522958

Bănărescu, A. (2015). Detecting and preventing fraud with data analytics. *Procedia Economics and Finance, 32*, 1827–1836. https://doi.org/10.1016/S2212-5671(15)01485-9

Bankole, F. O., Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation, 40*, Article 301348. https://doi.org/10.1016/j.fsidi.2022.301348

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges and opportunities. *Computer Science & IT Research Journal, 5*(6), 1505–1520.

Bhandari, K. R., Rana, S., Paul, J., & Salo, J. (2020). Relative exploration and firm performance: Why resource theory alone is not sufficient? *Journal of Business Research, 118*, 363–377. https://doi.org/10.1016/j.jbusres.2020.07.001

Bin-Nashwan, S. A., Li, J. Z., Jiang, H., Bajary, A. R., & Ma'aji, M. M. (2025). Does AI adoption redefine financial reporting accuracy, auditing efficiency, and information asymmetry? An integrated model of TOE-TAM-RDT and big data governance. *Computers in Human Behavior Reports, 17*, Article 100572. https://doi.org/10.1016/j.chbr.2024.100572

Bogner, W. C., Thomas, H., & McGee, J. (1999). Competence and competitive advantage: Towards a dynamic model. *British Journal of Management, 10*(4), 275–290. https://doi.org/10.1111/1467-8551.00139

Botes, V., & Saadeh, A. (2018). Exploring evidence to develop a nomenclature for forensic accounting. *Pacific Accounting Review, 30*(2), 135–154. https://doi.org/10.1108/PAR-12-2016-0117

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing, 25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Castillo, A., Rescalvo-Martin, E., & Karatepe, O. M. (2026). How is common method bias addressed using partial least squares structural equation modeling in hospitality and tourism research? *Tourism Review, 81*(1), 204–228. https://doi.org/10.1108/TR-07-2025-0762

Chai, M., & Wu, L. (2024). Unveiling the concealed risks: The influence of digital finance on cyber financial crime in China. *Crime & Delinquency*. Advance online publication. https://doi.org/10.1177/00111287241287137

Chang, W.-H., & Chang, J.-S. (2011). A novel two-stage phased modeling framework for early fraud detection in online auctions. *Expert Systems with Applications, 38*(9), 11244–11260. https://doi.org/10.1016/j.eswa.2011.02.172

Cheah, J., Sarstedt, M., Ringle, C. M., Ramayah, T., & Ting, H. (2018). Convergent validity assessment of formatively measured constructs in PLS-SEM: On using single-item versus multi-item measures in redundancy analyses. *International Journal of Contemporary Hospitality Management, 30*(11), 3192–3210. https://doi.org/10.1108/IJCHM-10-2017-0649

Chen, C. H. S., Liu, G., Roushan, G., Nguyen, B. (2025). Exploring information technology capabilities from multiple aspects of the resource-based theory. *Information Systems Frontiers, 27*, 1013–1043. https://doi.org/10.1007/s10796-024-10490-1

Cheung, G. W., Cooper-Thomas, H. D., Lau, R. S., Wang, L. C., & Liao, Y. (2024). Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. *Asia Pacific Journal of Management, 41*(3), 745–783. https://doi.org/10.1007/s10490-023-09871-y

Chuang, S. H. (2004). A resource-based perspective on knowledge management capability and competitive advantage: An empirical investigation. *Expert Systems with Applications, 27*(3), 459–465. https://doi.org/10.1016/j.eswa.2004.05.008

Clark, L. A., & Watson, D. (2019). Constructing validity: New developments in creating objective measuring instruments. *Psychological Assessment, 31*(12), 1412–1427. https://doi.org/10.1037/pas0000626

Dako, O. F., Onalaja, T. A., Nwachukwu, P. S., Bankole, F. A., & Lateefat, T. (2020). Forensic accounting frameworks addressing fraud prevention in emerging markets through advanced investigative auditing techniques. *Journal of Frontiers in Multidisciplinary Research, 1*(2), 46–63. https://doi.org/10.54660/JFMR.2020.1.2.46-63

Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023). Forensic accounting in the digital age: A US perspective: Scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal, 5*(11), 342–360. https://doi.org/10.51594/farj.v5i11.614

Davis, F. D., & Granić, A. (2024). Epilogue: What will the future of TAM be like? In A. Granić (Ed.), *The technology acceptance model: 30 years of TAM* (pp. 103–108). Springer. https://doi.org/10.1007/978-3-030-45274-2_4

Diawati, P., Gadzali, S. S., Abd Aziz, M. K. N., Almaududi Ausat, A. M., & Suherlan, S. (2023). The role of information technology in improving the efficiency and productivity of human resources in the workplace. *Jurnal Teknologi dan Sistem Informasi Bisnis, 5*(3), 296–302. https://doi.org/10.47233/jteksis.v5i3.872

Đukić, T., Pavlović, M., & Grdinić, V. (2023). Uncovering financial fraud: The vital role of forensic accounting and auditing in modern business practice. *Economic Themes, 61*(3). https://doi.org/10.2478/ethemes-2023-0021

Ebaid, I. E.-S. (2022). An exploration of accounting students' attitudes toward integrating forensic accounting in accounting education. *International Journal of Law and Management, 64*(4), 337–357. https://doi.org/10.1108/IJLMA-06-2021-0154

Edge, M. E., & Sampaio, P. R. F. (2009). A survey of signature-based methods for financial fraud detection. *Computers & Security, 28*(6), 381–394. https://doi.org/10.1016/j.cose.2009.02.001

Ekundayo, F. (2024). Big data and machine learning in digital forensics: Predictive technology for proactive crime prevention. *World Journal of Advanced Research and Reviews, 24*(2), 2692–2709. https://doi.org/10.30574/wjarr.2024.24.2.3659

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security, 52*, 70–89. https://doi.org/10.1016/j.cose.2015.04.003

Fagbore, O. O., Ogeawuchi, J. C., Ilori, O., Isibor, N. J., Odetunde, A., & Adekunle, B. I. (2024). Building cross-functional collaboration models between compliance, risk, and business units in finance. *International Journal of Scientific Research in Science and Technology*,*11*(4), 488-524 https://doi.org/10.32628/IJSRST24115122

Fassam, L. (2021). *Capabilities of internal actors to build resilience against supply chain food fraud* (Doctoral dissertation, University of Huddersfield). University of Huddersfield Repository. https://pure.hud.ac.uk/en/studentTheses/capabilities-of-internal-actors-to-build-resilience-against-suppl/

Ferri, L., Spanò, R., Ginesti, G., & Theodosopoulos, G. (2021). Ascertaining auditors' intentions to use blockchain technology: Evidence from the Big 4 accountancy firms in Italy. *Meditari Accountancy Research, 29*(5), 1063–1087. https://doi.org/10.1108/MEDAR-03-2020-0829

Ganesh, N. G., Venkatesh, N. M., & Prasad, D. V. V. (2022). A systematic literature review on forensics in cloud, IoT, AI & blockchain. In *Illumination of Artificial Intelligence in Cybersecurity and Forensics* (pp. 197–229). Springer. https://doi.org/10.1007/978-3-030-93453-8_9

Gangwani, M. (2021). Suitability of forensic accounting in uncovering bank frauds in India: An opinion survey. *Journal of Financial Crime, 28*(1), 284–299. https://doi.org/10.1108/JFC-07-2020-0126

Gitundu, E. W., Kiprop, S. K., Kibet, L. K., Kisaka, S. E., & Egerton, K. (2016). Corporate governance and financial performance: Theoretical and philosophical predicaments in research. *European Journal of Business and Management, 8*(11), 164–174.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the FinTech revolution: Interpreting the forces of innovation, disruption, and transformation in financial

services. *Journal of Management Information Systems, 35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Grobler, M. M., & Dlamini, I. Z. (2010). Managing digital evidence: The governance of digital forensics. *Journal of Contemporary Management, 7*(1), 1–21. https://hdl.handle.net/10520/EJC51095

Haddad, H. O. S. S. A. M., Alharasis, E. E., Fraij, J., & Al-Ramahi, N. M. (2024). How do innovative improvements in forensic accounting and its related technologies sweeten fraud investigation and prevention. *WSEAS Transactions on Business and Economics, 21*, 1115–1141.

Hair, J. F., Astrachan, C. B., Moisescu, O. I., Radomir, L., Sarstedt, M., Vaithilingam, S., & Ringle, C. M. (2021). Executing and interpreting applications of PLS-SEM: Updates for family business researchers. *Journal of Family Business Strategy, 12*(3), Article 100392. https://doi.org/10.1016/j.jfbs.2020.100392

Hair, J., & Alamer, A. (2022). Partial least squares structural equation modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research Methods in Applied Linguistics, 1*(3), Article 100027. https://doi.org/10.1016/j.rmal.2022.100027

Halbouni, S. S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection: Evidence from the UAE. *Managerial Auditing Journal, 31*(6–7), 589–628. https://doi.org/10.1108/MAJ-02-2015-1163

Hamadeh, A. H., Nouraldeen, R. M., Mahboub, R. M., & Hashem, M. S. (2025). Auditors' intention to use blockchain technology and TAM3: The moderating role of age. *Administrative Sciences, 15*(2), Article 61. https://doi.org/10.3390/admsci15020061

Hamilton, R. H., & Sodeman, W. A. (2020). The questions we ask: Opportunities and challenges for using big data analytics to strategically manage human capital resources. *Business Horizons, 63*(1), 85–95. https://doi.org/10.1016/j.bushor.2019.10.001

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems, 48*, Article 100598. https://doi.org/10.1016/j.accinf.2022.100598

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity* (McKinsey & Company Report, pp. 1–11). https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf

Hedt, B. L., & Pagano, M. (2011). Health indicators: Eliminating bias from convenience sampling estimators. *Statistics in Medicine, 30*(5), 560–568. https://doi.org/10.1002/sim.3920

Heggestad, E. D., Scheaf, D. J., Banks, G. C., Monroe Hausfeld, M., Tonidandel, S., & Williams, E. B. (2019). Scale adaptation in organizational science research: A review and best-practice recommendations. *Journal of Management, 45*(6), 2596–2627. https://doi.org/10.1177/0149206319850280

Herdati, J. P., & Claudia, M. (2024). Innovative human resource management strategies: Improving organisational performance in a global context. In *Proceedings of the Bengkulu International Conference on Economics, Management, Business and Accounting (BICEMBA)* (Vol. 2, pp. 1587–1592). https://doi.org/10.33369/bicemba.2.2024.128

Hossain, M. Z. (2026). Emerging trends in forensic accounting: Data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology for fraud investigation and prevention. *Journal of Artificial Intelligence and Technological Development, 2*(2), 183–208. https://doi.org/10.59324/jaitd.2026.2(2).14

Howard, M. C., Boudreaux, M., & Oglesby, M. (2024). Can Harman's single-factor test reliably distinguish between research designs? Not in published management studies. *European Journal of Work and Organizational Psychology, 33*(6), 790–804. https://doi.org/10.1080/1359432X.2024.2393462

Huang, F., & Teo, T. (2020). Influence of teacher-perceived organisational culture and school policy on teachers' intention to use technology: An extension of TAM. *Educational Technology Research and Development, 68*(3), 1547–1567. https://doi.org/10.1007/s11423-019-09722-y

Huang, S. Y., Lin, C. C., Chiu, A. A., & Yen, D. C. (2017). Fraud detection using fraud triangle risk factors. *Information Systems Frontiers, 19*(6), 1343–1356. https://doi.org/10.1007/s10796-016-9647-9

Huy, P. Q., & Phuc, V. K. (2024). Contribution to accelerated internationalization with digital forensic accounting and metaverse circular business model innovation for Vietnam-based SMEs. *Journal of Innovation and Entrepreneurship, 13*(1), Article 88. https://doi.org/10.1186/s13731-024-00442-z

Igonor, O. S., Amin, M. B., & Garg, S. (2025). The application of blockchain technology in the field of digital forensics: A literature review. *Blockchains, 3*(1), Article 5. https://doi.org/10.3390/blockchains3010005

Iipumbu, E., Nhamu, I., & Chitauro, M. (2023, November). A comparative analysis of information systems audit and digital forensics processes. In *Proceedings of the International Conference on Information Systems and Emerging Technologies (ICISET)*. SSRN. https://doi.org/10.2139/ssrn.4648699

Ilori, O., Lawal, C. I., Friday, S. C., Isibor, N. J., & Chukwuma-Eke, E. C. (2022). The role of data visualization and forensic technology in enhancing audit effectiveness: A research synthesis. *Journal of Frontiers in Multidisciplinary Research, 3*(1), 188–200. https://doi.org/10.54660/.IJFMR.2022.3.1.188-200

Imjai, N., Promma, W., Visedsun, N., Usman, B., & Aujirapongpan, S. (2025). Fraud detection skills of Thai Gen Z accountants: The roles of digital competency, data science literacy and diagnostic skills. *International Journal of Information Management Data Insights, 5*(1), Article 100308. https://doi.org/10.1016/j.jjimei.2024.100308

Imjai, N., Swatdikun, T., Rungruang, P., Basiruddin, R., & Aujirapongpan, S. (2024). Empowering Generation Z accountants in the era of data complexity and open innovation: Nurturing big data analytics, diagnostic, and forensic accounting skills. *Journal of Open Innovation: Technology, Market, and Complexity, 10*(2), Article 100308. https://doi.org/10.1016/j.joitmc.2024.100308

Ishengoma, F. (2024). Revisiting the TAM: Adapting the model to advanced technologies and evolving user behaviours. *The Electronic Library, 42*(6), 1055–1073. https://doi.org/10.1108/EL-06-2024-0166

Jakobsen, M., & Jensen, R. (2015). Common method bias in public management studies. *International Public Management Journal, 18*(1), 3–30. https://doi.org/10.1080/10967494.2014.997906

Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science, 3*(6), e1418. https://doi.org/10.1002/wfs2.1418

Jebreel, M., Magboul, I., Qudah, H. A., & Herzallah, F. (2025). User-related antecedents and perceived audit quality outcome of CAATTs usage among auditors. *Human Systems Management*. https://doi.org/10.1177/0167253325137784

Karpoff, J. M. (2021). The future of financial fraud. *Journal of Corporate Finance, 66*, Article 101694. https://doi.org/10.1016/j.jcorpfin.2020.101694

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

Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K. K. R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Science International: Reports, 2*, Article 100117. https://doi.org/10.1016/j.fsir.2020.100117

Khatib, S. F. A., Sulimany, H. G. H., Alshareef, M. N., et al. (2024). Catalysts of audit excellence: Competitive advantage, intellectual capital and auditing quality. *Quality & Quantity, 58*, 4915–4939. https://doi.org/10.1007/s11135-024-01885-y

Kishore, K., Jaswal, V., Kulkarni, V., & De, D. (2021). Practical guidelines to develop and evaluate a questionnaire. *Indian Dermatology Online Journal, 12*(2), 266–275. https://pubmed.ncbi.nlm.nih.gov/33959523/

Kock, N. (2017). Common method bias: A full collinearity assessment method for PLS-SEM. In H. Latan & R. Noonan (Eds.), *Partial least squares path modeling: Basic concepts, methodological issues and applications* (pp. 245–257). Springer. https://doi.org/10.1007/978-3-319-64069-3_11

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change, 80*(3), 541–555. https://doi.org/10.1016/j.techfore.2012.07.002

Lardo, A., Corsi, K., Varma, A., & Mancini, D. (2022). Exploring blockchain in the accounting domain: A bibliometric analysis. *Accounting, Auditing & Accountability Journal, 35*(9), 204–233. https://doi.org/10.1108/AAAJ-10-2020-4995

Li, S., Qin, T., & Min, G. (2019). Blockchain-based digital forensics investigation framework in IoT and social systems. *IEEE Transactions on Computational Social Systems, 6*(6), 1433–1441. https://ieeexplore.ieee.org/document/8777292

Liengaard, B. D., Sharma, P. N., Hult, G. T. M., Jensen, M. B., Sarstedt, M., Hair, J. F., & Ringle, C. M. (2021). Prediction: Coveted, yet forsaken? Introducing a cross-validated predictive ability test in partial least squares path modeling. *Decision Sciences, 52*(2), 362–392. https://doi.org/10.1111/deci.12445

Lioukas, C. S., Reuer, J. J., & Zollo, M. (2016). Effects of information technology capabilities on strategic alliances: Implications for the resource-based view. *Journal of Management Studies, 53*(2), 161–183. https://doi.org/10.1111/joms.12179

Maket, L., & Korir, M. (2017). Resource inimitability: The strategic resource characteristic for sustainable competitiveness in universities. *European Journal of Business and Innovation Research, 5*(1), 67–82.

Mandal, A., & S, A. (2024). Fathoming fraud: Unveiling theories, investigating pathways and combating fraud. *Journal of Financial Crime, 31*(5), 1106–1125. https://doi.org/10.1108/JFC-06-2023-0153

Mehta, K., Mittal, P., Gupta, P. K., & Tandon, J. K. (2022). Analyzing the impact of forensic accounting in the detection of financial fraud: The mediating role of artificial intelligence. In A. Khanna, D. Gupta, S. Bhattacharyya, A. E. Hassanien, S. Anand, & A. Jaiswal (Eds.), *International Conference on Innovative Computing and Communications* (Vol. 1388, pp. 533–543). Springer. https://doi.org/10.1007/978-981-16-2597-8_50

Mishra, A. K., Hemamalini, V., & Tyagi, A. K. (2024). Digital forensics with emerging technologies: Vision and research potential for future. *Conversational Artificial Intelligence*, 675–697. https://doi.org/10.1002/9781394200801.ch37

Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A framework for enterprise risk identification and management: The resource-based view. *Managerial Auditing Journal, 34*(2), 162–188. https://doi.org/10.1108/MAJ-12-2017-1751

Montasari, R., & Hill, R. (2019). Next-generation digital forensics: Challenges and future paradigms. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 205–212). IEEE. https://doi.org/10.1109/ICGS3.2019.8688020

Nayak, M. (2024, September 29). How is the artificial intelligence of today's time, ChatGPT and Blackbox.ai, helpful in machine learning? SSRN. https://doi.org/10.2139/ssrn.4996043

Ndenje-Sichalwe, E., & Elia, E. F. (2021). Research methodology practices among postgraduate information studies students in Tanzania. *IFLA Journal, 47*(2), 129–141. https://doi.org/10.1177/03400352209659

Netshifhefhe, K., Netshifhefhe, M. V., Naphtali, M., & Mupa, K. A. M. (2024). The role of forensic audits in strengthening corporate governance and mitigating compliance risks. *Iconic Research and Engineering Journals, 8*(4), 427-445. https://www.irejournals.com/paper-details/1706420

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Nissan, E. (2012). Accounting for social, spatial, and textual interconnections. In *Computer applications for handling legal evidence, police investigation and case argumentation* (Law, Governance and Technology Series, Vol. 5). Springer. https://doi.org/10.1007/978-90-481-8990-8_6

Olorunlana, T. J. (2025). Harnessing technology for effective fraud detection: Tools, trends, and case studies. *International Journal of Science, Architecture, Technology, and Environment, 2*(6), 579. https://doi.org/10.63680/ijsate0525190.48

Othman, R., Aris, N. A., Mardziyah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector. *Procedia Economics and Finance, 28*, 59–67. https://doi.org/10.1016/S2212-5671(15)01082-5

Oyedokun, G. E. (2015, March 7). *Approach to forensic accounting and forensic audit*. SSRN. https://doi.org/10.2139/ssrn.2575168

Pearson, T. A., & Singleton, T. W. (2008). Fraud and forensic accounting in the digital environment. *Issues in Accounting Education, 23*(4), 545–559.

Peng, Y., Ahmad, S. F., Ahmad, A. Y. B., Al Shaikh, M. S., Daoud, M. K., & Alhamdi, F. M. H. (2023). Riding the waves of artificial intelligence in advancing accounting and its implications for sustainable development goals. *Sustainability, 15*(19), 14165. https://doi.org/10.3390/su151914165

Petraşcu, D., & Țieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance, 16*, 489–497. https://doi.org/10.1016/S2212-5671(14)00829-6

Pham, Q. H., & Vu, K. P. (2024). Insight into how cyber forensic accounting enhances the integrated reporting quality in small and medium enterprises. *Cogent Business & Management, 11*(1). https://doi.org/10.1080/23311975.2024.2364053

Pham, Q. H., & Vu, K. P. (2024). Insight into how digital forensic accounting and metaverse circular business model innovation contribute to accelerated internationalization: Evidence from Vietnam-based SMEs. *Cogent Business & Management, 11*(1), 2320203. https://doi.org/10.1080/23311975.2024.2320203

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Polas, M. R. H. (2025). Common method bias in social and behavioral research: Strategic solutions for quantitative research in doctoral research. *Journal of Comprehensive Business Administration Research*. https://doi.org/10.47852/bonviewJCBAR52024285

Prenzler, T. (2020). What works in fraud prevention: A review of real-world intervention projects. *Journal of Criminological Research, Policy and Practice, 6*(1), 83–96. https://doi.org/10.1108/JCRPP-04-2019-0026

Qasim, A., & Kharbat, F. F. (2020). Blockchain technology, business data analytics, and artificial intelligence: Use in the accounting profession and ideas for inclusion into the accounting curriculum. *Journal of Emerging Technologies in Accounting, 17*(1), 107–117. https://doi.org/10.2308/JETA-52649

Quang Huy, P., & Kien Phuc, V. (2025). Insight into how legal and ethical considerations of artificial intelligence enhance the effectiveness of cyber forensic accounting. *Journal of Global Information Technology Management, 28*(2), 136–166. https://doi.org/10.1080/1097198X.2025.2480972

Quoc, T. N. K., Van, T. H., Le, T. V., Minh, H. N., & Ngoc, H. N. T. (2024). Financial statements' reliability affects firms' performance: A case of Vietnam. *Journal of Eastern European and Central Asian Research, 11*(1), 143–155. https://ieeca.org/journal/index.php/JEECAR/article/view/1432

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences, 6*(2), 1–5.

Ramachandran, R., Babu, V., & Murugesan, V. P. (2023). The role of blockchain technology in the process of decision-making in human resource management: A review and future research agenda. *Business Process Management Journal, 29*(1), 116–139. https://doi.org/10.1108/BPMJ-07-2022-0351

Rantatalo, O., Lindberg, O., Lindholm, A., & Lundmark, R. (2025). Co-creation to increase cross-functional collaboration in police investigations of online child sexual abuse:

A qualitative study protocol. *International Journal of Qualitative Methods, 24*, Article 16094069251333592. https://doi.org/10.1177/16094069251333592

Ravichandran, T., Lertwongsatien, C., & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: A resource-based perspective. *Journal of Management Information Systems, 21*(4), 237–276. https://doi.org/10.1080/07421222.2005.11045820

Rezaee, Z., & Wang, J. (2019). Relevance of big data to forensic accounting practice and education. *Managerial Auditing Journal, 34*(3), 268–288. https://doi.org/10.1108/MAJ-08-2017-1633

Rezaee, Z., Wang, J., & Lam, B. (2018). Toward the integration of big data into forensic accounting education. *Journal of Forensic and Investigative Accounting, 10*(1), 87–99.

Richard III, G. G., Roussev, V., & Marziale, L. (2007). Forensic discovery auditing of digital evidence containers. *Digital Investigation, 4*(2), 88–97. https://doi.org/10.1016/j.diin.2007.04.002

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*(1), 25–41. https://doi.org/10.1080/14780887.2013.801543

Rodgers, W., Söderbom, A., & Guiral, A. (2015). Corporate social responsibility–enhanced control systems reducing the likelihood of fraud. *Journal of Business Ethics, 131*(4), 871–882. https://doi.org/10.1007/s10551-014-2152-5

Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change, 17*(2), 164–196. https://doi.org/10.1108/JAOC-09-2019-0098

Saá-Pérez, P. D., & García-Falcón, J. M. (2002). A resource-based view of human resource management and organizational capabilities development. *The International Journal of Human Resource Management, 13*(1), 123–140. https://doi.org/10.1080/09585190110092848

Sau, A., Banerjee, A., & Vedhavathy, T. R. (2025). Improving fraud detection efficiency: Leveraging machine learning strategies. In *Hybrid and Advanced Technologies* (pp. 33–40). CRC Press.

Sewpersadh, N. S. (2025). Adaptive structural audit processes as shaped by emerging technologies. *International Journal of Accounting Information Systems, 56*, Article 100735. https://doi.org/10.1016/j.accinf.2025.100735

Shazzad Hasan, M. M., Abdul Latiff, A. R., Zainl Abidin, Z., & Motahar Hossain, M. (2024). Adoption of blockchain technologies into forensic accounting practices. In R. Kumar, A. K. Verma, O. P. Verma, & T. Wadehra (Eds.), *Soft Computing: Theories and Applications (SoCTA 2023)* (Vol. 971, pp. 287–298). Springer. https://doi.org/10.1007/978-981-97-2089-7_23

Simsek, Z., & Veiga, J. F. (2000). The electronic survey technique: An integration and assessment. *Organizational Research Methods, 3*(1), 93–115. https://doi.org/10.1177/109442810031004

Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2006). *Fraud auditing and forensic accounting*. John Wiley & Sons. http://ndl.ethernet.edu.et/bitstream/123456789/28491/1/178.pdf.pdf

Sirmon, D. G., & Hitt, M. A. (2009). Contingencies within dynamic managerial capabilities: Interdependent effects of resource investment and deployment on firm performance. *Strategic Management Journal, 30*(13), 1375–1394. https://doi.org/10.1002/smj.791

Sudarmadi, D. (2023). Forensic accounting and investigative audit on the effectiveness of implementing audit procedures in fraud disclosure. *JASa, 7*(2), 400–405. https://doi.org/10.36555/jasa.v7i2.2350

Sirmon, D. G., & Hitt, M. A. (2009). Contingencies within dynamic managerial capabilities: Interdependent effects of resource investment and deployment on firm performance. *Strategic Management Journal, 30*(13), 1375–1394. https://doi.org/10.1002/smj.791

Tageldin, L., & Venter, H. (2023). Machine-learning forensics: State of the art in the use of machine-learning techniques for digital forensic investigations within smart environments. *Applied Sciences, 13*(18), 10169. https://doi.org/10.3390/app131810169

Taher, M. (2011). Resource-based view theory. In *Information Systems Theory* (pp. 151–163). Springer. https://doi.org/10.1007/978-1-4419-6108-2_8

Taherdoost, H. (2021). A review on risk management in information systems. *Electronics, 10*(24), 3065. https://doi.org/10.3390/electronics10243065

Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation, 40*, Article 301348. https://doi.org/10.1016/j.fsidi.2022.301348

Teece, D. J. (2019). A capability theory of the firm: An economics and (strategic) management perspective. *New Zealand Economic Papers, 53*(1), 1–43. https://doi.org/10.1080/00779954.2017.1371208

Tharsika, K., Varanitha, S., & Thaneshan, G. (2025) Artificial intelligence and audit quality: A comparative study of big four and non-big four audit firms in Sri Lanka. International *Journal of Accounting & Business Finance 11*(1), 82-95. DOI: https://doi.org/10.4038/ijabf.v11i1.169

Thompson, C. G., Kim, R. S., Aloe, A. M., & Becker, B. J. (2017). Extracting the variance inflation factor and other multicollinearity diagnostics from typical regression results. *Basic and Applied Social Psychology, 39*(2), 81–90. https://doi.org/10.1080/01973533.2016.1277529

Tiron-Tudor, A., Faragalla, W. A., & Pianoschi, A. (2025). The role of the accountancy professionals in detecting and preventing fraud in a digital landscape: A systematic

literature review. *Digital Finance, 7*, 745–786. https://doi.org/10.1007/s42521-025-00138-3

Turner, J. E. (2011). *Money laundering prevention: Deterring, detecting, and resolving financial fraud*. Wiley. https://doi.org/10.1002/9781119200604

Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial intelligence-based cybersecurity and digital forensics: A review. https://doi.org/10.1002/9781394303601.ch18

Umrani, W. A., Ahmad, I., Rasheed, M. I., Ahmed, U., Pahi, M. H., Jhatial, A., & Abbasi, G. A. (2022). Managing intellectual capital: Role of corporate entrepreneurship and absorptive capacity on firm performance. *Knowledge Management Research & Practice, 20*(5), 719–731. https://doi.org/10.1080/14778238.2022.2041374

Vijayalakshmi, D., & Jeevan, J. (2024). Forensic accounting: Uncovering fraud with advanced analytics. *Library of Progress–Library Science, Information Technology & Computer, 44*(3), 22014.

Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: An analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science, 44*(1), 119–134. https://doi.org/10.1007/s11747-015-0455-4

Wahyuandari, W. (2025). The role of forensic auditing in detecting and preventing financial fraud in organizations. *The Journal of Academic Science, 2*(1), 212–221. https://doi.org/10.59613/1hay7432

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5*(2), 171–180. https://doi.org/10.1002/smj.4250050207

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47–66. https://doi.org/10.1016/j.cose.2015.09.005

Xu, D., Huo, B., & Sun, L. (2014). Relationships between intra-organizational resources, supply chain integration and business performance: An extended resource-based view. *Industrial Management & Data Systems, 114*(8), 1186–1206.

Yarovenko, H., Bilovodska, V., Bylbas, R., Pankiv, O., Baghirzade, M., Niemi, O., & Djakons, D. (2025). Digital readiness of European countries to combat corruption and cyber threats: Panel analysis. *Business Ethics and Leadership, 9*(2), 238–265. https://doi.org/10.61093/bel.9(2).238-265.2025

Yoshimura, M., Fujimi, Y., Izui, K., & Nishiwaki, S. (2006). Decision-making support system for human resource allocation in product development projects. *International Journal of Production Research, 44*(5), 831–848.

Zott, C. (2003). Dynamic capabilities and the emergence of intraindustry differential firm performance: Insights from a simulation study. *Strategic Management Journal, 24*(2), 97–125. https://doi.org/10.1002/smj.288