Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 10, Issue 2 (July-December) 2025
*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 225/E/KPT/2022).*
Available online at: http://apfjournal.or.id/index.php/apf

The Role of Accounting Technology in Preventing Cyberfraud: A Systematic Literature Review

✉Indah Dwi Novianti & Totok Dewayanto
Faculty of Economics and Business, Diponegoro University, Indonesia

ARTICLE INFORMATION
Article History:
Received November 29, 2024
Revised August 3, 2025
Accepted November 10, 2025

DOI:
10.21532/apfjournal.v10i2.383

ABSTRACT
In a state-of-the-art virtual generation, the fast improvement of statistical technology has significantly impacted many industries. This consists of the global economy, but this virtual revolution has additionally delivered another main trouble: the spread of online fraud. Internet fraud is more than just a hazard. This research explores the role of accounting technology in preventing cyber fraud. Based on the theories of the Technology Acceptance Model (TAM) and the Fraud Triangle, this research investigates the accounting technology used to avoid cyber fraud and the effectiveness of the technology in detecting and reducing cyber fraud. Method: A literature review using the PICO approach was used to define the research questions and collect relevant data. The analysis reveals trends in document production, Authors' contributions, and keywords related to accounting technology. In conclusion, this study provides information for future research to conduct longitudinal studies to assess accounting technology's effectiveness and long-term challenges.

Keywords: Accounting, Accounting Technology, Prevention, Cyberfraud, Fraud.

How to Cite:
Novianti, I. D., & Dewayanto, T. (2025). The Role of Accounting Technology in Preventing Cyberfraud: A Systematic Literature Review. *Asia Pacific Fraud Journal, 10*(2), 209-226. http://doi.org/10.21532/apfjournal.v10i2.383.

✉Corresponding author :
Email: indhhdw@gmail.com

1. INTRODUCTION

In a state-of-the-art virtual generation, the rapid advancement of information technology has significantly impacted various industries, including the global financial system. However, this digital transformation has also introduced a significant threat: the widespread increase in online fraud. Cyber fraud is more than just a risk-it is a serious and pressing issue organizations face worldwide. Sophisticated cyberattacks are escalating yearly, leading to billions of dollars in financial losses (Ghann et al., 2022; Granato & Polacek, 2019; Sonkar et al., 2024). The 2023 IBM Security Report reveals that the financial services sector suffers the highest average cost of cyberattacks, reaching USD 5.9 million per incident (Chatterjee et al., 2023). Moreover, notable cases like the Equifax data breach and fraudulent financial reporting in fintech companies like Wirecard have underscored the severe consequences of inadequate cyber fraud prevention(Abubakar et al., 2024; Daswani & Elbayadi, 2021).

The growing urgency to mitigate these risks has pushed organizations to adopt modern technologies (Rufus & Isaac, 2024). These tools are especially crucial in enhancing data privacy protection and fraud resilience, as they integrate technologies like artificial intelligence, encryption standards, and anomaly detection techniques (Mishra, 2023; Paul et al., 2023; Schweitzer, 2024). While general cybersecurity frameworks, such as firewalls and intrusion detection systems, remain vital, they are often limited to external threat detection. They may fail to uncover internal manipulations, such as fictitious transactions or misreported entries. Detecting internal fraud requires more advanced systems that leverage behavioural analytics and machine learning to identify abnormal patterns in financial data (Ndubuisi, 2024; Thakkar et al., 2025).

Although many articles mention various cybersecurity tasks, there remains a significant gap in our understanding of the specific role of accounting technology in preventing cyber fraud. This gap in research (Ahmad et al., 2024; Alrawashdeh & Ghazalat, 2022; Chavali et al., 2024; Ghann et al., 2022; Pillay et al., 2023; Rufus & Isaac, 2024; Tetteh & Otioma, 2024; Zadorozhnyi et al., 2023). It is critical because accounting systems unlike conventional cybersecurity tools are embedded within the financial operations of organizations and thus offer unique, internal vantage points for detecting fraud through real-time analysis of transactions, ledger patterns, and compliance anomalies (Adelakun et al., 2024; Mahtani, 2022). In sectors like banking, fintech, and government procurement, failure to leverage accounting technology means missed opportunities to detect fraud from within the system (Kangkpang & Ogar-Abang, 2024; Mustafa, 2024). While technical solutions such as firewalls and intrusion detection systems are essential for perimeter defence, they do not address internal manipulations such as fictitious entries or misreporting (Akinbowale et al., 2023).

Therefore, this study addresses a vital research gap by exploring how accounting technologies, such as AI-driven audit tools, blockchain-based ledgers, and automated compliance systems, can serve as an integrated layer of defence and contribute to a more holistic cyberfraud prevention strategy.

Recent industry data further underscores the urgency of this research. According to the Association of Certified Fraud Examiners (ACFE, 2024), organizations worldwide lose approximately 5% of their annual revenues to fraud, amounting to trillions in global losses(Arel et al., 2023). Many of these losses are cyber-enabled, involving increasingly complex schemes that bypass traditional cybersecurity systems. Remeikienė et al. (2024) e-crime poses a huge threat to the global economy. According to the World Cyber Security Report (2023). Moreover, a 2023 PwC Global Economic Crime Survey reported that 46% of organizations experienced fraud, corruption, or other economic crimes

in the last two years, many undetected by conventional IT-based controls. These trends illustrate that current solutions are insufficient, particularly in identifying fraud within financial records. As a result, there is a growing need for integrated accounting technologies that offer internal, data-driven prevention strategies (Meiryani et al., 2023). This represents a promising future for online fraud prevention.

This systematic literature evaluation explores the accounting era's function in preventing online fraud by answering the following primary research questions.

a. What accounting technologies (e.g., ERP systems, audit analytics, AI, and blockchain) are currently used to detect and prevent cyber fraud?
b. How effective are these accounting technologies in reducing fraud occurrences in organizational contexts?
c. What are the key barriers and implementation challenges organizations face using accounting technologies for cyber fraud prevention?
d. What research gaps remain, and what future directions are needed to improve the use of accounting technology in this area?

From the definition of hassle above, the targets of this observation are:

a. Identify and classify specific accounting technologies to prevent cyber fraud (e.g., ERP-integrated audit tools, AI-powered analytics, blockchain ledgers).
b. Evaluate the effectiveness of these technologies in detecting and reducing cyber fraud based on empirical evidence.
a. Examine organizations' main challenges and limitations in adopting such technologies.
a. Propose future research directions to bridge the empirical and practical gaps in accounting-based cyber fraud prevention.

2. LITERATURE REVIEW AND HYPOTHESIS

This study adopts theTheory of Acceptance Model (TAM) and the Fraud Triangle Theoryas its theoretical foundation to bridge the identified gap in the literature. TAM explains and evaluates how accounting practitioners accept and use technologies such as AI, blockchain, and ERP systems in fraud prevention efforts. By analyzing perceived usefulness and ease of use, TAM helps to understand the drivers and barriers to adopting these tools within organizational settings (Alhumoudi & Johri, 2024; Dowuna, 2024; Ummah & Sofyani, 2024).

Meanwhile, the Fraud Triangle Theory provides a behavioural framework to understand why cyber fraud occurs (i.e., driven by pressure, opportunity, and rationalization). Accounting technologies address this model by limiting "opportunity" through real-time monitoring and reducing "rationalization" via transparent audit trails and automated controls (Adeboye, 2024; Musyoki, 2023). Integrating both theories enables this study to examine how accounting technologies are implemented and aligned with organizational and psychological mechanisms to prevent fraud. Thus, this theoretical perspective directly supports the study's goal of exploring practical, tech-based solutions to mitigate fraud risks that prior studies have not sufficiently addressed (Gabriela, 2023; Shandu & Saluja, 2023).

The Technology Acceptance Model (TAM), developed by Davis (1989) And adapted from the Theory of Reasoned Action (TRA), aims to predict how individuals accept and use information technology systems (Marikyan & Papagiannidis, 2006). TAM is particularly relevant for this study as it provides a structured lens for examining the acceptance of accounting technologies, such as ERP systems, AI-driven audit tools, and blockchain applications, used to prevent fraud.

The Technology Acceptance Model (TAM)comprises four essential constructs that influence users' decisions to adopt technology:

a. Perceived ease of use affects whether users, such as accountants or internal auditors, feel confident using tools like ERP-based fraud modules or AI-enabled audit software without excessive training or complexity (Wiryanti et al., 2020).
b. Perceived usefulness reflects users' belief that these technologies will enhance their performance, such as detecting suspicious transactions more efficiently or ensuring real-time compliance with financial regulations (Kusumathias et al., 2023; Meiryani et al., 2021).
c. Behavioural intention to use represents the user's readiness to adopt fraud prevention technology in their daily tasks, which may depend on organizational culture, perceived value, or prior experiences with similar systems (Ardila et al., 2025; Ilona & Zaitul, 2021).
d. Actual system usage refers to how these tools are integrated into regular workflows. High usage rates indicate successful adoption, enabling more accurate, timely, and automated detection of potential fraud.

These factors provide a structured lens to evaluate why accounting technology is or is not effectively used in fraud prevention, bridging the gap between technology design and behavioural acceptance.

The Fraud Triangle Theory, introduced by Donald Cressey in 1953, explains that fraud typically occurs due to three key factors: pressure, opportunity, and rationalization. This study applies the theory by analyzing how accounting technologies can reduce the "opportunity" for fraud, such as through real-time monitoring, automated alerts, and blockchain-based transparency (Chen, 2022; Gabriela, 2023). These technologies can also address "rationalization" by establishing clear audit trails that make unethical behaviour harder to justify (Shandu & Saluja, 2023). While the theory does not directly address technological interventions, it provides a behavioural foundation for understanding how such tools can prevent fraud from occurring within organizational systems.

The Association of Certified Fraud Examiners (ACFE, 2024) categorizes fraud into three main types:

a. Fraudulent Financial Reporting, such as misstating revenues or expenses to present a healthier financial position, can be identified through AI-powered audit tools and continuous auditing systems that flag inconsistencies in real time (Chen, 2022; Hasibuan et al., 2023)
b. Corruption, including bribery and conflicts of interest, can be monitored using segregation of duties modules in ERP systems and automated approval workflows to prevent unauthorized transactions (Gabriela, 2023).
c. Asset Misappropriation, such as skimming or misusing company resources, can be detected using transaction monitoring tools, inventory tracking systems, and blockchain to ensure transparency and immutability in financial records (Chen, 2022).

These classifications help link specific fraud types to corresponding technological solutions, reinforcing the practical application of the theoretical framework in analyzing and mitigating cyber fraud within accounting systems.

3. METHODS

This study employs a Systematic Literature Review (SLR) to examine the role of accounting technologies in preventing cyber fraud. The methodology consists of two main components: (1) the use of the PICO framework to define the scope and focus of the research, and (2) the application of the PRISMA protocol to guide the literature identification and selection process.

Although the PICO framework is traditionally applied in clinical research, it was adapted in this study as a tool to structure the formulation of research

questions in a clear and focused manner. PICO helps this study maintain clarity and replicability in the literature selection process and enhances the analytical rigour of identifying how accounting technologies perform across different organizational contexts.Furthermore, prior research in information systems and management science has demonstrated that PICO can be adapted successfully when the study includes interventions and observable outcomes, even outside medical research (Alhadi et al., 2025; Nishikawa-Pacher, 2022; Sharoni et al., 2023).

a. Population: Organizations vulnerable to cyber fraud use digital financial systems, specifically: fintech companies, financial institutions, and government agencies with digital accounting functions.
b. Intervention: Application of accounting technologies designed to detect and prevent cyber fraud, including: blockchain-based accounting, AI/ML-powered fraud detection, ERP systems with real-time controls, and continuous monitoring tools.
c. Comparison: Traditional fraud prevention approaches include manual audits, non-integrated financial systems, or paper-based internal controls.
d. Outcome: Effectiveness measured by: fraud reduction, anomaly detection speed, financial transparency, audit efficiency, and cost/time savings in fraud management.

In this study, Scopus was selected as the primary database for the systematic literature review. Scopus is one of the largest and most reputable abstract and citation databases of peer-reviewed literature, encompassing journals across multiple disciplines, including accounting, information systems, and cybersecurity. Its advanced search features allow for precise filtering based on keywords, document types, and publication years, which supports a rigorous and replicable review process. Moreover, Scopus indexes a wide range of high-quality international journals, ensuring that the articles analyzed in this study are relevant and credible. This broad and multidisciplinary coverage makes Scopus suitable for capturing the intersection between accounting technology and cyber fraud prevention.

While this study includes international literature, particular attention is given to research trends in Indonesia. As the largest digital economy in Southeast Asia, Indonesia is experiencing rapid digitalization in both the public and private sectors, which increases its vulnerability to cyber fraud. According to recent reports from Badan Siber dan Sandi Negara Indonesia (BSSN, 2022), financial and government institutions have become primary targets for cybercrime. Despite this, research examining the application of accounting technologies (such as ERP, audit analytics, and blockchain) for fraud prevention in the Indonesian context is still limited. This geographic focus is important for identifying local research gaps and offering region-specific recommendations for policy and practice.

SLR (Systematic Literature Review) is a scientific, explicit, and reproducible research approach for amassing relevant evidence on a topic that meets predetermined inclusion and exclusion criteria (Shaheen et al., 2023; Satnarine, 2023).To ensure the relevance and quality of the articles included, the following inclusion criteria were applied:

a. Articles published between 2020 and 2024
b. Written in English
c. Peer-reviewed journal articles only
d. Directly related to accounting technology (e.g., blockchain, ERP, AI/ML) and cyber fraud or financial fraud prevention
e. Available in full-text through the Scopus database

Exclusion criteria included:

a. Non-peer-reviewed documents (e.g., editorials, opinion pieces, book reviews)

b. Articles outside the accounting or cyber fraud scope
c. Duplicate records or incomplete metadata.

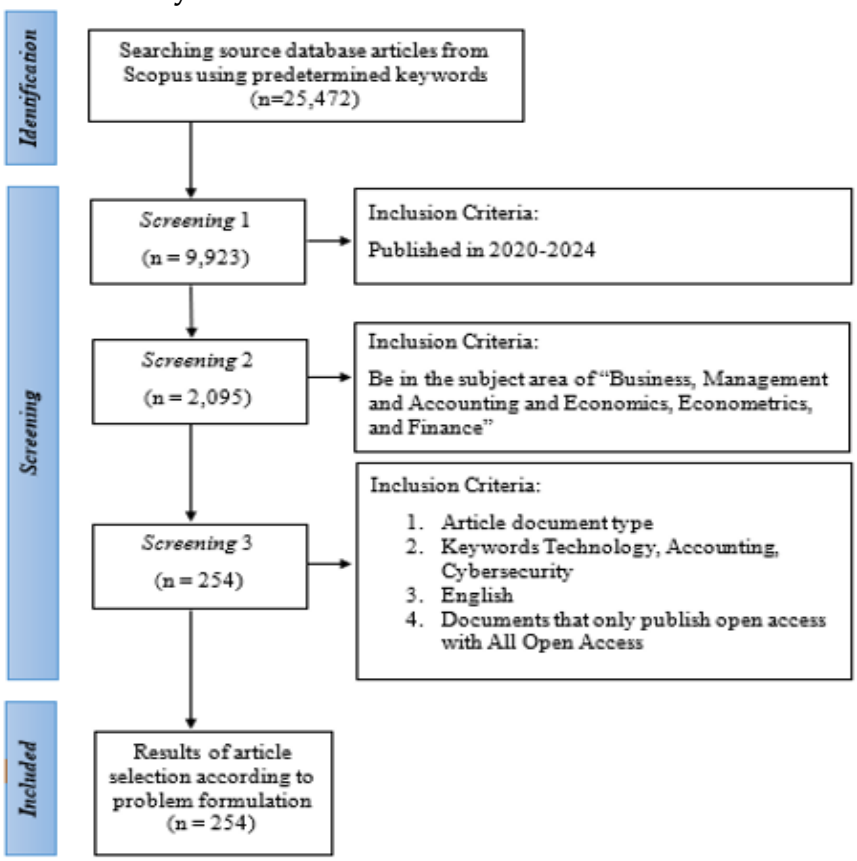
The systematic literature review (SLR) process followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure methodological rigour.

The PRISMA flowchart (Figure 1) presents the systematic process of selecting relevant literature for this study, covering the stages of identification, screening, eligibility, and inclusion.

The article selection process began with an initial search in the Scopus database using general keywords related to technology, accounting, and cyber fraud, generating 25,472 articles. To ensure the relevance and timeliness of the literature, a publication year filter (2020–2024) was applied, reducing the number of results to 9,923 articles.To narrow the scope further and align with the focus of the study, subject area filters were implemented, selecting only articles under "Business, Management and Accounting" and "Economics, Econometrics and Finance", resulting in 2,095 articles.

Subsequent screening was conducted based on specific inclusion criteria, including: (1) document type, limited to peer-reviewed journal articles; (2) keyword relevanceTheBeyond generic keywords like "Technology," "Accounting," and "Cyberfraud," the search string was expanded to include domain-specific terms such as "Financial Technology," "Fintech," "Blockchain in Accounting," "Cloud Accounting," "Digital Accounting Tools," "Artificial Intelligence in Accounting," "Cyber Fraud Detection," and "Cybersecurity in Accounting." The inclusion of these terms enabled the study to capture a broader yet focused selection of articles directly related to the intersection of accounting technology and cyber fraud prevention. (3) accessibility, prioritizing open-access articles to facilitate full-text review and transparency.Following this

Figure 1. **PRISMA Study Selection**



multi-stage filtering process, 254 articles were deemed eligible for in-depth review and bibliometric analysis by the study's objectives.

4. RESULTS AND DISCUSSION

Results

Figure 2 illustrates the number of publications by country between 2020 and 2024, offering insight into the global distribution of research on accounting technology and cyber fraud prevention. The United States leads with the most documents (19), followed by Italy and the United Kingdom, each contributing 10 publications. This output concentration may reflect several structural advantages, such as greater access to research funding, leading academic institutions specializing in accounting and cybersecurity, and robust industry-academia collaborations that drive innovation in digital fraud prevention.

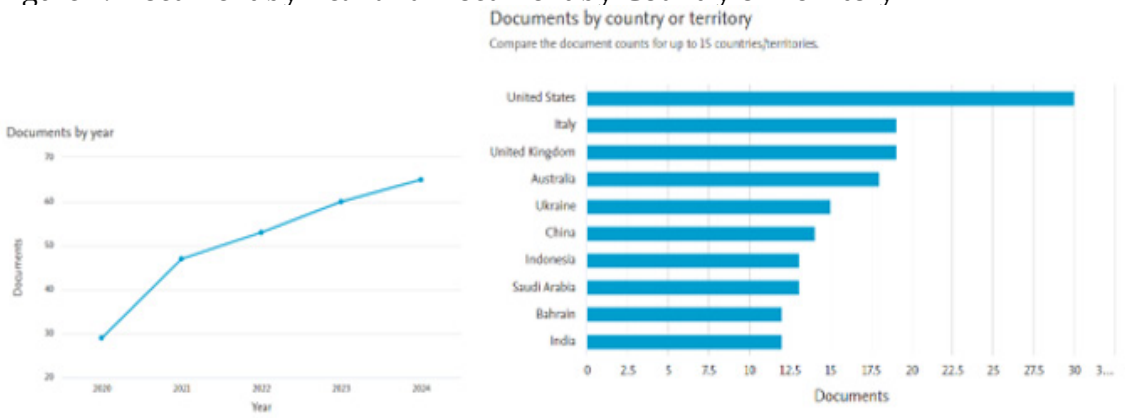
In contrast, countries with fewer publications may have limited research budgets for niche areas like accounting technology or may prioritize other related disciplines, such as general cybersecurity, information systems, or public sector governance. The variation in publication volume across regions offers valuable insight into how national research agendas and institutional capabilities influence contributions to this emerging field.

Figure 3 displays the distribution of publications by subject area, where Business, Management, and Accounting represent the largest segment (37.1%), followed by Economics, Econometrics, and Finance (23.5%), and other areas such as Decision Sciences (10.3%) and Computer Science (6.1%). This distribution demonstrates the multidisciplinary nature of cyber fraud prevention research, which lies at the intersection of financial control, technological innovation, and risk analysis.

Taken together, these figures highlight the field's geographical and disciplinary dynamics. While countries like the U.S., Italy, and the U.K. drive publication output, the research's thematic scope spans technical and managerial domains. These patterns suggest that regional priorities and the integration of diverse disciplinary perspectives shape the advancement of accounting technology in fraud prevention. The following is a description of the primary information about the records:

a. Timespan: Records cover the period 2020 to 2024.
b. Sources (Journals, Books, many others): There are 138 statistics resources used, including journals, books, and others.
c. Documents: There are 254 files within the dataset.
d. Annual Growth Rate %: The annual growth rate of the file is 22.36%.
e. Average Document Age: The average document age is 1.67 years.
f. Average Citations per Document: Every record was cited 10.96 times.

Figure 2. **Document by Year and Document by Country or Territory**



Source: Processed Data

g. References: There are 13322 references inside the information.

Document Contents:

a. Plus Keywords (ID): 511 extra key phrases are inside the facts.
b. Author Keywords (DE): The authors inside the facts provide 884 keywords.

Authors:

a. Authors: There are 721 authors within the statistics.
b. Single Authors of Documents: 39 authors wrote the document individually.

Collaboration between Authors:

a. Documents written by one author: One author writes 40 documents.
b. Co-Authors per Document: On average, there are 3.02 co-authors per document.
c. International Co-Authorship %: 26.77% of documents have authors from multiple states.

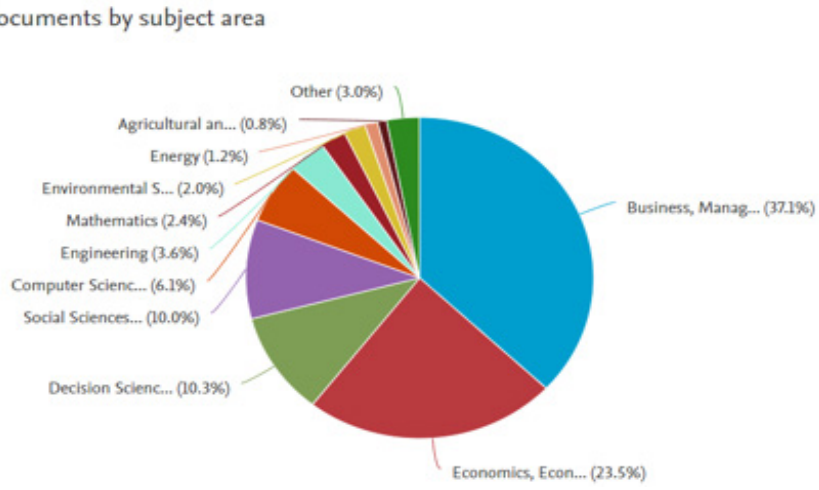
Document Type:

a. Articles: There are 180 articles.
b. Books: There are three books
c. Book Chapters: There are 32 e-book chapters.
d. Conference Papers: There are 17 conference papers.
e. Note: There are two notes.
f. Conference Reviews: There are 20 conference reviews.

The co-word network analysis presents several metrics to understand the relationships between keywords in the research corpus. These include betweenness centrality, closeness centrality, and Page Rank, each offering a different dimension of keyword significance.

a. Node: Represents a keyword or concept in the research corpus.
b. Cluster: Indicates the grouping or thematic area a keyword belongs to. Keywords in the same cluster are more closely related to one another.
c. Betweenness centrality: Measures how often a keyword is a bridge on the shortest path between other keywords. A high betweenness score suggests a keyword connects diverse research topics and plays a crucial integrative role.
d. Closeness centrality: Reflects how quickly a keyword can interact with all other keywords in the network, indicating its accessibility and importance in disseminating information.
e. Page Rank: A measure of overall influence, based on the number and quality of connections. Like how search engines rank web pages, a high PageRank indicates frequent use and strategic centrality in the research network.

Figure 3. **Document by Subject Area**



Source: Processed Data

Table 1. **Main Information Bibliometrix**

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2020:2024
Sources (Journals, Books, etc)	138
Documents	254
Annual Growth Rate %	22.36
Document Average Age	1.67
Average citations per doc	10.96
References	13322
DOCUMENT CONTENTS	
Keywords Plus (ID)	511
Author's Keywords (DE)	884
AUTHORS	
Authors	721
Authors of single-authored docs	39
AUTHORS COLLABORATION	
Single-authored docs	40
Co-Authors per Doc	3.02
International co-authorships %	26.77
DOCUMENT TYPES	
articles	180
book	3
book chapter	32
conference paper	17
note	2
review	20

Source: Processed Data

For example, the keyword "accounting" demonstrates a high betweenness (164.3), closeness (0.023), and PageRank (0.133), confirming its role as a central and integrative concept within the research network. It bridges themes such as digital auditing, fraud analytics, and financial reporting, and connects various clusters such as finance, technology, and cybersecurity.

Similarly, the keyword "technology" shows even higher betweenness (220.47) and strong PageRank (0.120), reinforcing its overarching role in fraud prevention discussions. Meanwhile, terms such as "artificial intelligence" and "blockchain", though they have moderate centrality values, indicate emerging yet less integrated themes, suggesting future interdisciplinary growth areas.

Table 2. **Co-Word Network Bibliometrics**

Node	Cluster	Betweenness	Closeness	PageRank
accounting	1	164.3	0.023	0.133
articles	1	117,903	0.022	0.118
artificial intelligence	1	0	0.015	0.025
finance	1	30,767	0.016	0.05
human	1	39.34	0.019	0.061
blockchain	1	0.667	0.014	0.026
blockchain	1	0	0.014	0.021
China	1	0	0.013	0.01
female	1	0	0.012	0.01
adult	1	0	0.015	0.02
algorithm	1	0	0.014	0.015
Back propagation neural networks	1	0	0.014	0.015
cyber security	1	0	0.011	0.01
technology	2	220.47	0.021	0.12
innovation	2	4,416	0.016	0.024
energy efficiency	2	0	0.013	0.011
public policy	2	0	0.013	0.011
acceptance	2	0	0.013	0.018
coal	2	0	0.013	0.011
engineering education	2	0	0.013	0.011
controlled study	3	17,137	0.018	0.051
cost-benefit analysis	3	0	0.015	0.03
Spain	3	0	0.014	0.015
cost-benefit analysis	3	0	0.015	0.03
economic evaluation	3	0	0.015	0.03
information systems	4	0	0.014	0.021
information use	4	0	0.014	0.021
metal	5	0	0.013	0.02
metal recovery	5	0	0.013	0.02
carbon	6	0	0.013	0.02
energy	6	0	0.013	0.02

Source: Processed Data

These insights indicate that co-word network metrics offer statistical indicators and qualitative interpretations of how knowledge is organized and connected in the field. A high betweenness value signals a strategic bridging role, while a high PageRank reflects conceptual influence across the domain. Therefore, understanding these metrics is essential for identifying which topics are foundational, which are growing, and how they interact. This helps prioritize themes for future research and guides theoretical development in accounting technology and cyber fraud prevention.

Figure 4. **Thematic Map Terms Bibliometrics**

Cluster	CallonCentrality	CallonDensity	RankCentrality	RankDensity	ClusterFrequency
accounting	11,962	101,578	10	8	70
algorithm	1	75	5,5	6	6
coal	0,75	62,5	4	3,5	4
cost benefit analysis	3,75	137,5	8	9	16
data analytics	1	62,5	5,5	3,5	4
efficiency	0,25	62,5	3	3,5	4
innovation	3,1	84,375	7	7	19
literature reviews	0	50	1,5	1	2
matthiola	0	62,5	1,5	3,5	4
technology	11,705	146,333	9	10	58

Source: Processed Data

Thematic map analysis is used to visualize and interpret the relationships among keywords related to accounting technology and cyber fraud. It identifies key themes based on their centrality (importance in the network) and density (degree of internal development within a theme). The analysis provides both quantitative indicators and qualitative insights into the structure of the research domain.

The keyword analysis reveals several terms with high centrality and frequency, indicating their pivotal role in shaping the intellectual structure of the research landscape.

The keyword "accounting" consistently emerges as a central term across clusters, with a Callon Centrality value of 11.962 and a Callon Density of 101.578. This highlights its foundational role as a discipline and a critical system for ensuring financial integrity, compliance, and internal control. In the context of cyber fraud prevention, accounting functions as both a source and a safeguard of financial data, anchoring discussions on technological interventions.

The keyword "technology" represents the digital transformation tools, such as AI, blockchain, and ERP systems, that enable automation, anomaly detection, and secure data management. Its presence as a high-centrality term reflects the research community's growing emphasis on integrating digital technologies into financial and accounting systems.

The term "cost-benefit analysis" is another influential concept, indicating a practical and evaluative dimension in current research. Its prominence underscores scholars' focus on assessing the feasibility and economic justification of implementing accounting technologies. This is particularly relevant for SMEs and public institutions, where resources are limited, and return on investment is a key concern.

Together, these keywords represent three intersecting domains: theoretical foundations (accounting), enabling mechanisms (technology), and applied evaluation (cost-benefit analysis). Their interconnectedness suggests that fraud prevention is no longer treated solely as a technical issue but as a multidisciplinary challenge, involving system design, financial management, and strategic decision-making.

In addition, the thematic metrics show that the word "accounting" is located in Cluster 1, which appears 70 times in the dataset, further reinforcing its dominant position. The analysis also identifies "algorithm," "coal," and "energy efficiency" as peripheral terms with lower centrality and density, suggesting that they are either niche or emerging topics.

This thematic mapping provides a snapshot of current research priorities and reveals areas for future investigation. For instance, the strong emphasis on accounting and technology calls for deeper

empirical studies into their combined effectiveness in fraud prevention. At the same time, economic evaluation highlights the need for cost-impact research.

In summary, understanding these influential terms and their network positioning helps clarify the field's strategic direction, uncover potential research gaps, and inform future research agendas in the intersection of accounting technology and cyber fraud prevention.

DISCUSSION

This review identifies several key insights regarding the role of accounting technology in preventing cyber fraud. First, recent advancements have enhanced real-time fraud detection and response. Technologies such as anomaly detection and predictive analytics allow organizations to proactively monitor unusual patterns and address threats. (Adelakun et al., 2024; Lentner et al., 2019; Li et al., 2024).

Second, integrating artificial intelligence (AI) and machine learning (ML) into accounting systems has significantly improved detection precision. These systems adapt to new fraud patterns by learning from historical data, uncovering sophisticated schemes that might evade traditional rule-based systems (Adelakun et al., 2024; Supriadi, 2024).

Third, blockchain technology has emerged as a promising tool in fraud prevention due to its core characteristics: decentralization, transparency, and immutability. In the financial sector, platforms like IBM Food Trust and TradeLens use blockchain to create secure, tamper-proof transaction records, reducing fraud in supply chains. Firms like Deloitte and PwC have adopted blockchain to generate continuous, real-time audit trails in auditing (Chen, 2022; Han et al., 2023a; Kao & Tsay, 2023). The Walmart China Blockchain Initiative is another illustrative case, where provenance tracking helped significantly reduce counterfeit goods, an essential application in fraud prevention.

These real-world implementations substantiate blockchain's effectiveness in reducing fraud risks by improving data integrity and traceability. Blockchain operates as a decentralized, immutable ledger, recording transactions across distributed networks. Once validated through consensus, entries cannot be altered without network agreement, ensuring tamper-resistance (Odeyemi et al., 2024). A notable technical advantage is smart contracts self-executing code that automatically enforces predefined conditions. In financial transactions, payments can only be released once all contractual criteria are satisfied, reducing fraud risk from manual intervention or manipulation. Furthermore, consensus mechanisms strengthen data validity by ensuring all network nodes verify every transaction.

These features enable rapid anomaly detection, robust audit trails, and high data integrity, which are crucial for cyber fraud prevention. Beyond fraud prevention, blockchain also improves operational efficiency. Blockchain streamlines audit processes through automated reconciliation, reducing costs and time (Han et al., 2023a). The World Economic Forum (2020) affirms that immutable ledgers enhance audit transparency by allowing real-time access to verified financial data. After implementing block-chain systems, firms like Maersk and IBM report increased operational efficiency and lower fraud risks, confirming their dual role in control and performance enhancement (Kao & Tsay, 2023).

Regarding research methodologies, the reviewed studies employ a wide range of approaches:

a. Experimental designs, such as randomized controlled trials, offer strong causal evidence of technology effectiveness, particularly in AI-based fraud detection. However, they often involve controlled environments with limited generalizability.

b. Large-scale surveys and secondary data analyses provide high external validity and help understand broader industry patterns.
c. Descriptive and qualitative studies contribute context-specific insights, exploring barriers, user perceptions, and organizational readiness. Though rich in detail, they may lack measurable outcome data(Supriadi, 2024).

Notably, studies grounded in real-world case data provide the most actionable insights, ensuring relevance to actual operational environments (Adelakun et al., 2024; Han et al., 2023). However, several studies rely heavily on self-reported data (e.g., surveys, interviews) and are prone to social desirability bias, recall errors, or inflated compliance claims. Adelakun et al. (2024) found discrepancies between reported adherence to fraud controls and actual behavior.Similarly, studies with small sample sizes often suffer from reduced statistical power and limited generalizability. A meta-analysis by Shaheen et al. (2023) underscores that smaller samples in fraud-related research increase the risk of Type II errors, weakening confidence in the findings. This indicates bias that can affect the generalizability of effects (Han et al., 2023).

5. CONCLUSION

This study underscores the vital contribution of accounting technologies particularly artificial intelligence (AI), machine learning (ML), blockchain, and real-time monitoring systems in combating the rising threat of cyber fraud. These tools support proactive anomaly detection, secure financial documentation, and streamlined audit workflows, collec-tively strengthening fraud resilience.

The review reveals that AI and ML improve the accuracy and adaptability of fraud detection models, while blockchain enhances transparency and traceability across financial transactions. These innovations are especially beneficial for fintech firms, small and medium enterprises (SMEs), and government institutions that often face high fraud risks with limited control resources.

Moreover, this study is among the few that systematically integrate the Technology Acceptance Model (TAM) and the Fraud Triangle Theory to explore the behavioral and technological dimensions of cyber fraud prevention within accounting systems.

Practical Implications

a. For practitioners: Organizations should prioritize adopting fraud-focused accounting tools, such as AI-driven analytics, ERP-integrated monitoring, and blockchain-based ledgers, to enhance detection and response capabilities.
b. For policymakers: There is a need to establish regulatory frameworks and incentives that encourage implementing secure digital accounting systems, especially in vulnerable sectors.
c. For educators and training providers: Programs must be updated to equip accounting professionals with the technical skills to manage and interpret outputs from advanced fraud prevention technologies.

These insights highlight the urgent need for organizations to embed fraud prevention technologies within core accounting functions, not as separate cybersecurity measures but as integral parts of financial governance and decision-making processes.

This study is not without limitations:

a. The literature reviewed was limited to peer-reviewed, English-language articles indexed in Scopus between 2020 and 2024, potentially omitting relevant local studies or grey literature.
b. The synthesis relies on secondary data with varying methodological quality, limiting the comparability of results.
c. Some included studies used self-reported data or small samples, introducing potential bias and reducing the robustness of conclusions.

d. These limitations restrict the generalizability of findings, particu-larly to underrepresented sectors or geographic contexts.

These limitations imply that the conclusions drawn from this review may not fully represent the perspectives or outcomes found in underrepresented regions, non-English speaking contexts, or grey literature. Consequently, the findings should be interpreted cautiously, especially when generalizing across different organizational settings or regulatory environments.

To enhance the evidence base, future studies should:

a. Include multi-database searches and non-English sources to capture a broader view of global research.
b. Conduct empirical case studies or experiments to measure the actual impact of accounting technologies on fraud outcomes.
c. Explore sector-specific challenges, especially in SMEs and developing economies, where technology adoption remains limited.
d. Evaluate the cost-effectiveness and sustainability of accounting technologies in long-term fraud prevention.

Future research should also explore the intersection of accounting technologies with regulatory compliance systems, especially in emerging markets, and examine user behaviour through longitudinal studies to understand sustained adoption and impact over time. Additionally, cost-effectiveness studies should focus on financial aspects and consider risk mitigation and operational resilience as key performance indicators.

REFERENCES

Abubakar, N. S. J., Paradji, N. U., Saggap, S., Anding, N. S., Tano, R. M., Arasani, A. H., Ahadain, D. R., Banda, B., Jayari, R., Alamhalil, A., Alih, S. H., & Tahil, P. S. K. (2024). Hacking Incidents and Their Long-Term Implications for User Privacy and Trust. *Cognizance Journal of Multidisciplinary Studies, 4*(12), 443–454. https://doi.org/10.47760/cognizance.2024.v04i12.041.

ACFE. (2024). *Association of Certified Fraud Examiners. The Nation's Occupational Fraud 2024 :A Report To The Nations*. Association of Certified Fraud Examiners.

Adeboye, E. O. (2024). Strengthening Fraud Prevention in Small Businesses : An Analysis of Practical Accounting and Auditing Practices. *International Journal of Science and Research Archive*, *13*(2), 590–595.

Adelakun, B. O., Antwi, B. O., Fatogun, D. T., & Olaiya, O. P. (2024). Enhancing Audit Accuracy: The Role of AI in Detecting Financial Anomalies and Fraud. *Finance & Accounting Research Journal*, *6*(6), 1049–1068. https://doi.org/10.51594/farj.v6i6.1235.

Adelakun, B. O., Onwubuariri, E. R., Adeniran, G. A., & Ntiakoh, A. (2024). Enhancing Fraud Detection in Accounting Through AI: Techniques and Case Studies. *Finance & Accounting Research Journal*, *6*(6), 978–999. https://doi.org/10.51594/farj.v6i6.1232.

Ahmad, A. Y. A. B., Abusaimeh, H., Rababah, A., Alqsass, M., Al-Olima, N. H., & Hamdan, M. N. (2024). Assessment of the Effects of Advances in Accounting Technologies on the Quality of Financial Reports in the Jordanian Public Sector. *Uncertain Supply Chain Management*, *12*(1), 133–142. https://doi.org/10.5267/j.uscm.2023.10.011.

Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). Integrating Forensic Accounting and Big Data Technology Frameworks for Internal Fraud Mitigation in the Banking Industry. *Cogent Business and Management*, *10*(1), 1-22. https://doi.org/10.1080/23311975.2022.2163560.

Alhadi, A., Tom, B., & Yacine, R. (2025). Enhancing asset Management: Integrating Digital Twins for Continuous Permitting And Compliance-A Systematic Literature Review. *Journal of Building Engineering*, *99*, 111515. https://doi.org/10.1016/j.jobe.2024.111515.

Alhumoudi, H., & Johri, A. (2024). Examining the role of Accounting Information Systems on a Firm's Performance: A Technology Acceptance Model Approach. *Edelweiss Applied Science and Technology*, *8*(5), 1831–1842. https://doi.org/10.55214/25768484.v8i5.1917.

Alrawashdeh, B., & Ghazalat, A. (2022). A Review on the Challenges and Connections between Cybersecurity and Accounting in Saudi Arabia. *Journal of System and Management Sciences*, *12*(5), 282–296. https://doi.org/10.33168/JSMS.2022.0517.

Ardila, I., Sembiring, M., & Astuti, R. (2025). The Role of Security Perception and Usage Impact of Mobile Accounting Applications. *Jurnal Akuntansi E-JA*, *29*(1), 186–205.

Arel, B., Tomas, M. J., & Stark, L. (2023). The Effect of Fraud Diamond Capability Measures on Fraud Occurrence. *Journal of Forensic Accounting Research*, *8*, 141–159. https://doi.org/10.2308/JFAR-2021-024.

BSSN. (2022). *BSSN: Industri Keuangan Rawan Serangan Siber, Lakukan Update Aplikasi Digital Secara Berkala*. Badan Siber dan Sandi Negara. https://www.bssn.go.id/bssn-industri-keuangan-rawan-serangan-siber-lakukan-update-aplikasi-digital-secara-berkala/.

Chatterjee, P., Das, D., & Rawat, D. B. (2023). Next Generation Financial Services: Role of Blockchain-enabled Federated Learning and Metaverse. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*. https://doi.org/10.1109/CCGridW59191.2023.00025.

Chavali, K., Kumar, A. V. V, Mavuri, S., Tiwari, C. K., & Pal, A. (2024). Investigation and Modelling of Barriers in Adopting Blockchain Technology for Accounting and Finance: An ISM Approach. *Journal of Global Information Management*, *32*(1), 1-23. https://doi.org/10.4018/JGIM.353960.

Chen, T. (2022). Blockchain and Accounting Fraud Prevention: A Case Study on Luckin Coffee. *Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)*, *652*(ICSSED), 44–49. https://doi.org/10.2991/aebmr.k.220405.009.

Daswani, N., & Elbayadi, M. (2021). *The Equifax Breach.* Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6655-7_4.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly: Management Information Systems*, *13*(3), 319–339. https://doi.org/10.2307/249008.

Dowuna, G. (2024). Fraud Risk Management Using AI. *I Texhika Hayka*, *10*(38), 28–38.

Gabriela, M. B. (2023). Influence of Fraud Triangle Framework on the Fraud Prevention and Detection Programs in PT. XX. *Journal Integration of Social Studies and Business Development*, *1*(2), 46–60. https://doi.org/10.58229/jissbd.v1i2.83.

Ghann, P., Owiredu, J., & Afotey, S. (2022). The effect of Cybercrime on Financial Institutions: A case study of Mumuadu Rural Bank, Osino in the Fanteakwa District, Eastern Region, Ghana. *Research Square*, *1*(12), 78–90. https://doi.org/10.21203/rs.3.rs-2209860/v1.

Granato, A., & Polacek, A. (2019). The growth and challenges of cyber insurance. *Chicago Fed Letter*, *426*. https://doi.org/10.21033/cfl-2019-426.

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*, 1-16. https://doi.org/10.1016/j.accinf.2022.100598.

Hasibuan, M. R. R., Siregar, S., & Harahap, M. I. (2023). The Effect of Internal Audit and External Audit on Accounting Fraud in View from The Fraud Triangle Theory (Study of Soe Companies in Medan City). *Journal of Management, Economic, and Accounting*, *2*(2), 275–286. https://doi.org/10.37676/jmea.v2i2.178.

Ilona, D., & Zaitul. (2021). *Behavioural Intention to Use Accounting Application: Perceived Ease of Use as Mediating Variable*. *Urban growth and access to opportunities: A challenge for Latin America*. CAF | Development Bank of Latin America and the Caribbean.

Kangkpang, A. K., & Ogar-Abang, J. O. (2024). Aksu Journal of Management Sciences (Aksujomas) vol 9 No. 1, June 2024. *Aksu Journal Of Management Sciences (Aksujomas)*, *9*(1), 106–128.

Kao, J.-H., & Tsay, R.-S. (2023). Preventing Financial Statement Fraud with Blockchain-based Verifiable Accounting System. *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*.

Kusumathias, I. P., Rahayu, S., & Wiralestari, W. (2023). the Influence of Accounting Information System Implementation on Performance with Technology Acceptance Model (TAM) Approach in Jambi Province Public Service Agencies. *Marginal Journal of Management Accounting General Finance and International Economic Issues*, *3*(1), 211–230. https://doi.org/10.55047/marginal.v3i1.949.

Lentner, C., Vasa, L., Kolozsi, P. P., & Zéman, Z. (2019). New dimensions of internal controls in banking after the GFC. *Economic Annals-XXI*, *176*(3–4), 38–48. https://doi.org/10.21003/ea.V176-04.

Li, W., Liu, X., & Zhou, S. (2024). Deep learning model-based research on anomaly detection and financial fraud identification in corporate financial reporting statements. *Journal of Combinatorial Mathematics and Combinatorial Computing*, *123*, 343–355. https://doi.org/10.61091/jcmcc123-24.

Mahtani, U. S. (2022). Fraudulent Practices and Blockchain Accounting Systems. *Journal of Accounting, Ethics and Public Policy*, *23*(1), 97–148.

Marikyan, D., & Papagiannidis, S. (2006). *Technology Acceptance Model. Handbook of Research on Electronic Surveys and Measurements*. IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-59140-792-8.ch038.

Meiryani, Chang, A., Lorenzo, B. A., & Daud, Z. M. (2021). Analysis of Technology Acceptance Model (TAM) Approach to the Quality of Accounting Information Systems. *ICCCM'21: Proceedings of the 9th International Conference on Computer and Communications Management*, 37–45. https://doi.org/https://doi.org/10.1145/3479162.3479168.

Meiryani, Patricia, S., & Presillia, S. (2023). The Effect of Computerized Accounting Information Systems, Big Data Analysis, and Internal Audit in Accounting Fraud Detection. *ICBDC '23: Proceedings of the 2023 8th International Conference on Big Data and Computing*. https://doi.org/10.1145/3624288.3624290.

Mishra, S. (2023). Exploring the Impact of AI-Based Cybersecurity Financial Sector Management. *Applied Sciences (Switzerland)*, *13*(10), 5875. https://doi.org/10.3390/app13105875.

Mustafa, M. A. (2024). *Role System Control Internal In Accounting Fraud Prevention 1,2,3)*. *3*(1), 242–248.

Musyoki, K. M. (2023). Internal Control Systems and Their Role in Financial Fraud Prevention in Kenya. *African Journal of Commercial Studies*, *3*(3), 173–180. https://doi.org/10.59413/ajocs/v3.i3.4.

Ndubuisi, A. F. (2024). *International Journal of Research Publication and Reviews: The Intersection of False Projections, Identity Manipulation, and Emerging Financial Cybercrime Threats*. *5*(12), 5529–5546.

Nishikawa-Pacher, A. (2022). Research Questions with PICO: A Universal Mnemonic. *Publications*, *10*(3), 1–21 https://doi.org/10.3390/publications10030021.

Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., & Ajayi-Nifise, A. O. (2024). Integrating AI with Blockchain for Enhanced Financial Services Security. *Finance & Accounting Research Journal*, *6*(3), 271–287. https://doi.org/10.51594/farj.v6i3.855.

Paul, E. O., Callistus, O., Somtobe, O., Esther, T., Somto, K.-A., Clement, O., & Ejimofor, I. (2023). Cybersecurity Strategies for Safeguarding Customers' Data and Preventing Financial Fraud in the United States Financial Sectors. *International Journal on Soft Computing*, *14*(3), 1–16. https://doi.org/10.5121/ijsc.2023.14301.

Pillay, P., Ntuli, P. N., & Ehiane, S. O. (2023). Exploring the Prevalence of Cybercrime in the Banking Industry in KwaZulu-Natal, South Africa. *International Journal of Membrane Science and Technology*, *10*(1), 1763–1775. https://doi.org/10.15379/ijmst.v10i1.3283.

Remeikienė, R., Trajanauskas, A., & Gasparėnienė, L. (2024). The development of e-crimes in the digital economy: Causes and consequences. *International May Conference on Strategic Management*, *XX*(1), 318–326. https://doi.org/10.5937/imcsm24032r.

Rufus, O. S., & Isaac, O. O. (2024). Forensic Accounting and Cybercrime Prevention in Listed Deposit Money Banks in Nigeria. *The Akungba Administrators and Management Scientists (TAAMS), 1*, 15-26.

Schweitzer, B. (2024). Artificial Intelligence (AI) Ethics in Accounting. *Artificial Intelligence (AI) Ethics in Accounting Journal of Accounting*, *25*(1), 67-103. https://doi.org/10.60154/jaepp.2024.v25n1p67.

Shaheen, N., Shaheen, A., Ramadan, A., Hefnawy, M. T., Ramadan, A., Ibrahim, I. A., Hassanein, M. E., Ashour, M. E., & Flouty, O. (2023). Appraising Systematic Reviews: A Comprehensive Guide to Ensuring Validity and Reliability. *Frontiers in Research Metrics and Analytics*, *8*, 1-9 https://doi.org/10.3389/frma.2023.1268045.

Shandu, N., & Saluja, S. (2023). Fraud Triangle as an Audit Tool. *Management and Labour Studies*, *48*(3), 418-443.

Sharoni, L.-O., Sacks, R., Yeung, T., Alhava, O., Laine, E., & Ribon, J. M. (2023). The PICO Framework for Analysis and Design of Production Systems for Construction. *Proceedings of the 31st Annual Conference of the International Group for Lean Construction (IGLC31)*, 1522–1533.

Sonkar, N., Verma, N., Kumar, A., Naqvi, D., & Nisa, Z. (2024). An Empirical Study on the Economic Impact of Cybersecurity Breaches and Computer Fraud on SMEs. *Journal of Information Systems Engineering and Management*, *10*, 730–735. https://doi.org/10.52783/jisem.v10i7s.986.

Supriadi, I. (2024). The Audit Revolution: Integrating Artificial Intelligence in Detecting Accounting Fraud. *Akuntansi dan Teknologi Informasi*, *17*(1), 48–61. https://doi.org/10.24123/jati.v17i1.6279.

Tetteh, G. K., & Otioma, C. (2024). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Business Economics, 64,* 1493–1514. https://doi.org/10.1007/s11187-024-00946-8

Thakkar, H., Fanuel, G. C., Datta, S., Bhadra, P., & Dabhade, S. B. (2025). Optimizing Internal Audit Practices for Combatting Occupational Fraud: A Study of Data Analytic Tool Integration in Zimbabwean Listed Companies. *International Research Journal of Multidisciplinary Scope*, *6*(1), 22–36. https://doi.org/10.47857/irjms.2025.v06i01.02164.

Travis Satnarine. (2023). Systematic Review Methodology: Conducting High-Quality Reviews and Understanding Their Significance in Evidence-Based Practice. *Journal For International Medical Graduates*, *2*(1). https://doi.org/10.56570/jimgs.v2i1.76.

Ummah, R. S., & Sofyani, H. (2024). Testing the Intention of Employees in Local Government to Adopt Blockchain Technology in Accounting Information Systems (AIS). *Public Accounting and Sustainability*, *1*(1), 1–18. https://doi.org/10.18196/pas.v1i1.3.

Wiryanti, K., &. F. (2020). The Effect of Perceived Ease of Use on the Quality of Accounting Information Systems and Its Impact on the Quality of Accounting Information. *Saudi Journal of Business and Management Studies*, *5*(12), 571–577. https://doi.org/10.36348/sjbms.2020.v05i12.004.

Zadorozhnyi, Z.-M., Muravskyi, V., Pochynok, N., & Ivasechko, U. (2023). Application of The Internet of Things and 6G Cellular Communication to Optimize Accounting and International Marketing. *Virtual Economics*, *6*(1), 38–56. https://doi.org/10.34021/VE.2023.06.01(3).