Jurnal Ekonomi dan Bisnis Digital (MINISTAL)
Vol. 4, No. 3, 2025: 203-222

Artificial Intelligence and Cloud-Based Accounting Information Systems: Enhancing Financial Reporting Reliability and Cybersecurity in the Digital Era

Putri Nur Aisyah[1*], Rina Tjandrakirana DP[2]
Accounting Department, Faculty of Economics, Universitas Sriwijaya, Indonesia
Corresponding Author: Putri Nur Aisyah putrinura82@gmail.com

A R T I C L E I N F O
Keywords: Digital Accounting, Artificial Intelligence (AI), Cloud-Based Accounting Information Systems (CAIS), Financial Reporting Reliability, Cybersecurity

Received : 16, July
Revised : 30, July
Accepted: 20, August

A B S T R A C T
This study aims to examine how the integration of Artificial Intelligence (AI) and Cloud-Based Accounting Information Systems (CAIS) enhances the reliability of financial reporting and strengthens cybersecurity. Using a qualitative Systematic Literature Review (SLR) and guided by Sociotechnical Systems Theory, the research synthesizes 28 academic sources. Results show that AI and CAIS improve accuracy, fraud detection, and real-time reporting while mitigating cyber threats through encryption and automated monitoring. However, challenges include algorithmic bias, regulatory complexity, and organizational misalignment. The study concludes that joint optimization of technical and social systems is essential for achieving secure, transparent, and resilient digital financial reporting environments.

DOI: https://doi.org/10.55927/ministal.v4i3.14519
ISSN-E: 2827-8259
https://journal.formosapublisher.org/index.php/ministal

INTRODUCTION

In the era of rapid digital transformation, the integrity and security of financial information have become increasingly dependent on the integration of advanced technologies. Artificial Intelligence (AI) and Cloud-Based Accounting Information Systems (CAIS) are at the forefront of this transformation, promising to revolutionize financial reporting processes through automation, real-time analytics, and enhanced cybersecurity (Alkan, 2022; Artene et al., 2024; Kuaiber et al., 2024). However, alongside their potential, these technologies introduce a series of complex challenges that threaten data reliability, organizational transparency, and regulatory compliance (Kuaiber et al., 2024; Matchuk et al., 2024).

Symptoms of the problem are becoming evident in the form of frequent cyberattacks targeting financial databases, inconsistencies in automated financial statements, and ethical concerns arising from algorithmic bias and opaque AI decision-making processes (Bocean & Vărzaru, 2022; Moreira et al., 2025; Shchyrba et al., 2025). Despite the proliferation of AI and cloud solutions in the accounting field, many organizations still struggle to achieve reliable, secure, and accountable financial reporting due to misalignments between technological capabilities and human or institutional readiness (Rodriguez-Barboza et al., 2024; Türegün, 2025).

This study is formulated to address the following research question: *How can the integration of AI and CAIS improve the reliability of financial reporting and mitigate cybersecurity risks, particularly when analyzed through the lens of Sociotechnical Systems (STS) Theory?* The objective is to explore how the interplay between technological advancements and organizational, ethical, and regulatory factors influences the performance and resilience of digital accounting systems (Gopalsamy & Karthick, 2019; Ding, 2024; Mustafa et al., 2024).

The novelty of this research lies in its application of STS Theory as a comprehensive analytical framework, offering a dual focus on the technical and social dimensions of AI-CAIS integration—an area often overlooked in prior literature, which tends to focus narrowly on technical performance (Troyer, 2016; Gonzalez et al., 2025). Moreover, this study bridges the gap between existing research that either champions the benefits of AI and cloud computing in accounting or critiques their associated risks, but rarely integrates both views within a sociotechnical perspective (Kuaiber et al., 2024; Zhang et al., 2023).

The key contribution of this research is its systematic synthesis of current literature to uncover patterns of success and failure in AI and CAIS implementation. By identifying both enablers and barriers to effective digital financial reporting, this study offers actionable insights for practitioners, policymakers, and academics. It proposes a path forward that balances innovation with accountability, reinforcing the need for joint optimization of technological infrastructures and social systems to build trustworthy and future-ready financial ecosystems (Awad et al., 2025; Choudhary et al., 2023; Ali et al., 2024).

LITERATURE REVIEW

Sociotechnical Systems Theory

Recent studies have increasingly emphasized the transformative role of Artificial Intelligence (AI) and Cloud-Based Accounting Information Systems (AIS) in enhancing the reliability of financial reporting and strengthening cybersecurity in the digital era. Sociotechnical Systems Theory (STS) serves as a foundational lens for understanding the integration of these technologies, advocating for the joint optimization of both social (human, organizational) and technical (AI, cloud) subsystems (Twyford & Abbas, 2023). From a technical standpoint, AI enhances reliability by automating repetitive tasks, detecting fraud, and facilitating real-time decision-making based on big data analytics (Yan & Ji, 2024). Cloud-based AIS further supports this by enabling remote access, scalability, and collaborative financial reporting, which contributes to increased transparency and consistency (Vo Van et al., 2024; Wahhab et al., 2024). However, technical advancement alone is insufficient.

STS highlights the need for participatory system design, user training, and ethical governance to ensure effective adoption and minimize risks such as algorithmic bias, system misuse, or organizational resistance (Lacmanovic & Skare, 2025; Ruissalo et al., 2022). In terms of cybersecurity, the literature indicates that AI-driven fraud detection systems and secure cloud infrastructures improve resilience against cyber threats, but their effectiveness depends heavily on organizational maturity, governance policies, and the implementation of sociotechnical safeguards (Abu-Dabaseh et al., 2025; Mauri & Damiani, 2022). Thus, aligning the technological capabilities of AI and cloud systems with ethical, behavioral, and regulatory dimensions is essential to achieving reliable and secure accounting practices in the digital landscape.

Artificial Intelligence

Artificial Intelligence (AI) is a field of computer science focused on creating systems that perform tasks requiring human intelligence, such as learning, reasoning, and problem-solving (Darda & Pendse, 2025; L. Zhang et al., 2021). Key technologies include machine learning, deep learning, natural language processing, computer vision, and robotics, enabling AI to analyze data, interact with language, and operate autonomously (Akpabio et al., 2024; Gehlot & Rana, 2024). AI is widely used in healthcare, education, transportation, industry, and online services, improving efficiency, accuracy, and personalization (Desmal et al., 2023; Jindal et al., 2021). However, AI also raises ethical concerns like bias, privacy, and job displacement, prompting the need for transparent and responsible use (Kamila & Jasrotia, 2025; Sethy et al., 2023). As AI evolves, especially with integration into emerging technologies and the pursuit of Artificial General Intelligence (AGI), its relevance across sectors will continue to grow, demanding careful attention to its societal impacts (Jagatheesaperumal et al., 2022; Meher, 2024).

Cloud-Based Accounting Information Systems (AIS)

Cloud-based accounting information systems (AIS) use cloud computing to improve the efficiency, scalability, and security of financial processes (Ding,

2024; Gade & Rao, 2022). These systems reduce infrastructure costs by eliminating the need for physical servers and allow real-time data access for faster decision-making (Thaher, 2024). They offer flexibility, enabling businesses to scale operations and support remote access for enhanced collaboration (Asatiani & Penttinen, 2015; Lutfi, 2022). Advanced encryption and regular updates provided by service providers also strengthen data security and reliability (Ding, 2024; Yalamati, 2024). For small and medium-sized enterprises (SMEs), cloud-based AIS reduce the need for external auditors and support better financial control (Vo Van et al., 2024; Zebua & Widuri, 2023). However, implementing cloud-based AIS requires careful planning, system integration, and staff training to avoid data migration issues (Khoruzhy et al., 2023; Thaher, 2024). Businesses must also ensure compliance with financial regulations and secure sensitive data (Chen & Xu, 2024; Yalamati, 2024). The integration of technologies such as blockchain and artificial intelligence further enhances these systems by automating processes and improving financial accuracy (Alkan, 2022; Ionescu, 2021). Going forward, making cloud-based AIS more accessible to SMEs will be key to fostering financial efficiency and sustainable growth (Noordin et al., 2024; Vo Van et al., 2024).

Financial Reporting Reliability

Financial reporting reliability refers to the accuracy and trustworthiness of financial information, ensuring it reflects the true financial position of an entity (Maines & Wahlen, 2006). This reliability is essential for stakeholders who depend on financial reports for decision-making (Al-Ramahi & Binsaddig, 2024). The adoption of IFRS improves transparency and comparability but may initially reduce accrual reliability due to implementation challenges (Lai et al., 2013; Quoc et al., 2024). High audit quality, effective audit committees, and strong internal controls enhance reporting reliability by minimizing errors and manipulation (Ibrahim et al., 2024; Lustrilanang et al., 2023; Xi et al., 2019). Regulatory frameworks, like anti-money laundering measures, also support financial integrity (Abdulkareem Al yasiri et al., 2024). However, subjectivity in estimates and changes in accounting standards may still create inconsistencies (Erb & Pelger, 2015; Lugovsky & Kuter, 2020). Overall, reliable reporting is vital for investor confidence, market stability, and regulatory compliance.

Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and data from unauthorized access and cyberattacks, ensuring confidentiality, integrity, and availability (Firmansyah, 2024; Tiwari et al., 2023). Key concepts include authentication, encryption, access control, and threat detection (Firmansyah, 2024; Tiwari et al., 2023). It is vital for safeguarding sensitive information, preventing data breaches, and maintaining organizational trust (Kapoor et al., 2024; Paliwal, 2023). Common threats include malware, phishing, ransomware, DDoS attacks, and insider threats (Kumar & Mandoria, 2024; Shinde et al., 2024). To mitigate these, organizations use tools like IDS/IPS, endpoint protection, and incident response plans, supported by user education (Malasowe et al., 2024; Tiwari et al., 2023). Emerging challenges include quantum computing, regulatory

compliance, and the need for skilled professionals, while AI and machine learning are increasingly used for proactive defense (Bhosale et al., 2023; Chandre et al., 2024; Ullah et al., 2024). Continuous innovation and awareness are essential to ensuring cybersecurity resilience (Kumar Jain et al., 2024).

Previous Research

The Systematic Literature Review (SLR) method in this study refers to the PRISMA guide which broadly provides stages of research selection, starting from the initial discovery of articles through the Scopus database. The following are the filtering stages carried out to obtain a collection of sources according to the criteria of this study.

Table 1. Inclusion and Exclusion Criteria in Source Selection

Criteria	Inclusion	Exclusion
Publication Type	Scientific articles, peer-reviewed journals, academic books	Popular media articles, blog posts, opinion pieces, non-academic reports
Publication Year	2018–2025	Before 2018
Research Topic	• Integration of Artificial Intelligence in Accounting Information Systems • Cloud-based AIS for financial reporting reliability and cybersecurity • Sociotechnical perspectives in digital accounting systems	• Non-AI or non-cloud AIS topics • Studies not addressing financial reporting or cybersecurity • Irrelevant technological or sectoral focus
Journal Index	Scopus Q1–Q4, Taylor & Francis, SpringerLink, IEEE, Elsevier	Journals not indexed in Scopus or other recognized academic databases
Source Content	Ensures consistency between abstract, discussion, and conclusion	Inconsistencies or contradictions between abstract, discussion, and conclusion

From the criteria that have been determined, it is continued with the stage of selecting the number of sources that have been obtained by the provisions of the criteria that have been mentioned in the table so that they become samples in this study. These stages can be described through the following PRISMA diagram.

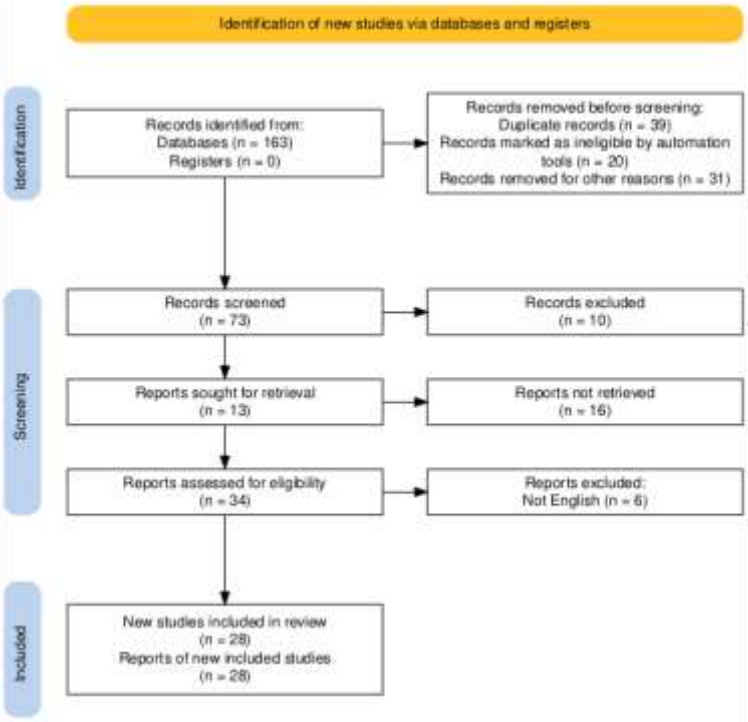

Figure 1. PRISMA diagram.

The majority of studies (61%) emphasized the beneficial impact of integrating AI and cloud technologies into accounting information systems. These positive impacts were primarily centered around three domains. First, the implementation of AI significantly improved the reliability of financial reporting by reducing human error and automating complex tasks such as real-time reconciliation, fraud detection, and predictive analysis. Second, AI-enhanced cloud systems strengthened cybersecurity through tools such as real-time threat detection, encryption algorithms, and blockchain integration. Third, operational efficiency was improved as cloud-based infrastructures enabled system scalability, regulatory compliance, and cost savings through centralized maintenance and updates. These findings align well with Sociotechnical Systems Theory, which highlights the importance of harmonizing human and technological subsystems to achieve optimal performance. Organizations that succeeded in this integration reaped benefits not only in system functionality but also in trust and transparency in financial reporting.

However, 11 studies (39%) pointed to notable challenges and risks associated with these technologies. Cybersecurity vulnerabilities were a recurring theme, particularly the risk of adversarial attacks and reliance on third-party platforms that may not be fully secure. Ethical concerns such as data privacy, algorithmic bias, and lack of transparency in AI decision-making were also prevalent. Additionally, technical and human resource barriers such as integration difficulties with legacy systems and resistance from users due to limited AI literacy were cited as major obstacles. These negative findings illustrate the sociotechnical misalignments that can occur when technological systems outpace organizational readiness or regulatory frameworks.

In conclusion, the PRISMA diagram validates the methodological robustness of this literature review and reflects a well-balanced spectrum of findings. While the integration of AI and cloud-based AIS offers transformative potential for enhancing financial reporting reliability and cybersecurity, it also introduces complex risks that must be addressed through ethical oversight, technical adaptability, and human-centered design. This underscores the necessity of applying a sociotechnical lens to the ongoing digital transformation of accounting practices, ensuring that technological advancement is matched by institutional preparedness and stakeholder engagement.

Table 2. Previous research on Artificial Intelligence & Cloud-Based Accounting Information Systems

Variable	Index	Author	Research Results
Artificial Intelligence and Cloud-Based Accounting Information Systems	Q1	Ali et al., (2024), Kuaiber et al., (2024), Felix et al., (2024), Zadorozhnyi et al., (2021)	(+)
	Q2	Askary et al., (2018), Al-Sammarraee & Alshareeda, (2021), Cazazian, (2022), Ionescu, (2022)	
	Q3	Awad et al., (2025), Shchyrba et al., (2025)	
	Q4	Rahahleh et al., (2021), Shakdwipee et al., (2023), Gopalsamy & Karthick, (2019), Ding, (2024), Qureshi et al., (2024), Kim et al., (2019)	
	Taylor and Francis	Clerkin & McConville, (2022)	
	Q1	Bani Ahmad, (2024a), Zhang et al., (2023)	(-)
	Q2	Bani Ahmad, (2024), Moreira et al., (2025), Türegün, (2025)	
	Q3	Al-Nsour et al., (2021), Bertolini, (2024)	
	Q4	Minz, (2024), Yadav et al., (2023), Mustafa et al., (2024), Rodriguez-Barboza et al., (2024)	
(+) has a positive effect, (-) has a negative effect			

METHODOLOGY

This study employs a qualitative research approach using the Systematic Literature Review (SLR) method. This method involves the systematic collection, evaluation, and synthesis of prior academic studies that specifically examine the integration of Artificial Intelligence (AI) and Cloud-Based Accounting Information Systems (CAIS) in enhancing the reliability of financial reporting and strengthening cybersecurity. The primary objective of this research is to

analyze the development, application, and implications of AI-integrated CAIS through the lens of Sociotechnical Systems Theory, while also identifying potential vulnerabilities and strategic mitigation measures.

The qualitative approach is adopted to allow an in-depth and contextual understanding of complex interactions between technological advancements (AI and cloud computing), organizational processes, and human factors within digital accounting systems. Given the rapidly evolving nature of both AI and cybersecurity threats, qualitative synthesis is particularly valuable in capturing the nuanced, interdisciplinary insights from diverse sources. This method facilitates the identification of patterns, themes, and conceptual frameworks that may not be evident through quantitative methods alone, thus providing a comprehensive foundation for future empirical investigation and policy recommendations.

RESEARCH RESULT

The findings confirm that integrating Artificial Intelligence (AI) with Cloud-Based Accounting Information Systems (CAIS) enhances financial reporting reliability by improving accuracy, timeliness, and fraud detection through automation and real-time analytics (Awad et al., 2025; Askary et al., 2018). Cloud platforms add scalability and data accessibility, fostering transparency and collaboration (Ionescu, 2022; Alkan, 2022). However, consistent with Sociotechnical Systems (STS) Theory, these technological benefits depend on the human subsystem skilled professionals who interpret AI outputs and ensure ethical governance (Al-Sammarraee & Alshareeda, 2021; Troyer, 2016).

Similarly, AI and CAIS strengthen cybersecurity with advanced encryption, real-time threat detection, and blockchain, but their effectiveness requires robust organizational policies, user training, and regulatory compliance (Felix et al., 2024; Moreira et al., 2025). The research highlights that misalignment such as algorithmic bias, transparency issues, and resistance to change can undermine system reliability if social factors are neglected (Kuaiber et al., 2024; Minz, 2024).

This study bridges the gap in literature by integrating technical, ethical, and organizational dimensions, emphasizing that successful AI-CAIS adoption requires joint optimization of technology and human elements. Ultimately, balanced sociotechnical integration is essential for building resilient, transparent, and trustworthy financial reporting systems in the digital era.

DISCUSSION

How AI and Cloud-Based Accounting Information Systems Improve the Reliability of Financial Reporting?

The integration of Artificial Intelligence (AI) and cloud-based Accounting Information Systems (AIS) has transformed financial reporting, improving its reliability and adaptability in the digital age. From the lens of Sociotechnical Systems Theory (STS), this advancement must be viewed not only through technological innovation but also in terms of how these tools interact with human, organizational, and regulatory components.

AI technologies such as machine learning, natural language processing, and robotic process automation reduce manual errors, enhance data processing consistency, and improve fraud detection (Awad et al., 2025; Kuaiber et al., 2024). From a technical subsystem perspective, these capabilities significantly enhance the efficiency and accuracy of information flows, which is critical for financial reporting. However, STS emphasizes that technology alone cannot ensure reliability; it must be harmonized with the human (social) subsystem, including accountants, managers, and auditors, whose trust in AI systems and ability to interpret AI outputs are vital (Rahahleh et al., 2021; Askary et al., 2018).

AI also facilitates predictive analytics and strategic forecasting, offering powerful decision-support capabilities (Shakdwipee et al., 2023; Türegün, 2025). Yet, in line with STS, the full value of these tools is realized only when the organizational culture and skills of professionals are aligned with these innovations. Effective training, cross-functional collaboration, and a shared understanding of how AI works are necessary to bridge the gap between technical potential and actual organizational impact (Al-Sammarraee & Alshareeda, 2021).

Cloud-based AIS, on the other hand, represent the technical infrastructure that enables real-time data processing and global access, boosting the timeliness and transparency of financial reports (Alkan, 2022; Ionescu, 2022). STS suggests that such systems must be embedded within a broader organizational workflow that supports flexible work environments, decentralization, and responsive decision-making. This is especially important for SMEs, where cloud systems can democratize access to high-quality reporting tools (Cazazian, 2022). However, social subsystems must evolve as well adopting new governance models, data stewardship roles, and trust mechanisms to manage the shared nature of cloud environments.

Moreover, when integrated with blockchain and encryption technologies, cloud-based AIS enhance data security and integrity (Alkan, 2022). In STS terms, these technologies form part of the technical subsystem that supports risk management, but their effectiveness also depends on how well users adhere to protocols, understand security risks, and collaborate to maintain system resilience.

The synergy between AI and cloud-based AIS creates a dynamic sociotechnical ecosystem where advanced analytics and automation co-exist with human judgment and governance. This alignment strengthens financial reporting reliability by balancing technical performance (e.g., automation, speed, accuracy) with social values (e.g., accountability, transparency, adaptability) (Ali et al., 2024).

However, STS highlights that misalignment between subsystems can introduce new risks. For instance, AI systems may introduce algorithmic bias or opacity, leading to ethical and interpretability concerns if not matched with appropriate human oversight and regulation (Kuaiber et al., 2024; Shakdwipee et al., 2023). Similarly, cloud migration can create dependency on third-party vendors, requiring new roles and policies to ensure continuity and compliance.

Implementing these systems also demands significant organizational change, including restructuring job roles, retraining staff, and redefining workflows. STS stresses that ignoring the social impacts—such as employee resistance, ethical dilemmas, or loss of human oversight can undermine the very reliability these technologies aim to enhance (Clerkin & McConville, 2022; Minz, 2024).

Ethical challenges such as data privacy, transparency in AI decision-making, and the displacement of accounting roles must be addressed through inclusive governance frameworks that emphasize explainability, fairness, and social accountability (Bani Ahmad, 2024; Yadav et al., 2023). These concerns reflect STS's central principle that technical systems are embedded in broader social contexts, and their success depends on how well they are integrated into those contexts.

Ultimately, from the Sociotechnical Systems Theory perspective, the integration of AI and cloud-based AIS enhances the reliability of financial reporting not merely through technological superiority but through the balanced co-evolution of social and technical subsystems. Achieving trustworthy, transparent, and sustainable financial practices in the digital era requires socio-organizational readiness, ethical stewardship, and continuous adaptation not just advanced tools.

What Role Do Cloud-Based Accounting Information Systems Play in Mitigating Cyber Threats Specific to Financial Data Protection?

Cloud-based accounting information systems (CAIS) play a critical role in safeguarding financial data against an evolving landscape of cyber threats. In today's digitized financial environment, their function extends beyond storage and processing to encompass dynamic, adaptive security frameworks. Equipped with advanced encryption protocols such as RSA and AES, CAIS ensure that financial data remains secure both in transit and at rest (Gopalsamy & Karthick, 2019; Shchyrba et al., 2025). Multi-factor authentication and role-based access controls further fortify system security by limiting access to authorized users only (Shchyrba et al., 2025).

From the perspective of Sociotechnical Systems (STS) Theory, which views organizations as composed of interacting social and technical subsystems, the security effectiveness of CAIS is contingent not just on the technological safeguards in place, but also on the social context in which these systems are embedded. While encryption, intrusion detection systems (IDS), and AI-powered monitoring tools represent the technical subsystem, their success relies heavily on human behavior, organizational policies, and regulatory alignment—the social subsystem.

CAIS platforms are increasingly developed in alignment with global cybersecurity regulations, such as those enforced by the Financial Conduct Authority (FCA) and the Monetary Authority of Singapore (MAS), to ensure robust data protection (Shchyrba et al., 2025). This regulatory compliance strengthens institutional trust and reinforces an organizational culture that values cybersecurity as a shared responsibility. According to STS theory, this

reflects the principle of joint optimization, where both technical capabilities and social structures must be designed in harmony to achieve optimal performance.

Operationally, CAIS reduce overhead costs by centralizing updates and security maintenance in the cloud (Ding, 2024; Qureshi et al., 2024). However, these efficiencies can only be realized if the workforce is adequately trained to engage with new access protocols, interpret system alerts, and respond to cyber incidents. For example, AI-powered anomaly detection is only valuable when users are trained to act upon alerts quickly and effectively. This interdependence reflects the STS emphasis on mutual adaptation, where human roles evolve alongside technological changes.

In addition, CAIS's integration with real-time threat detection tools and automated monitoring systems enables organizations to detect cyber anomalies early and mitigate breaches before they escalate (Kim et al., 2019; Felix et al., 2024). Yet, STS theory warns that over-reliance on automation without human oversight can create blind spots. Ethical and procedural challenges arise when AI-based systems make opaque decisions, emphasizing the need for explainability and governance within the social subsystem to ensure accountability.

Emerging solutions such as the integration of blockchain technology further enhance CAIS security by offering immutable, transparent records of financial transactions (Zadorozhnyi et al., 2021). When implemented within a sociotechnical framework, blockchain strengthens both the technical infrastructure and the institutional trust mechanisms that underlie financial reporting. For instance, blockchain can secure transaction integrity, but only if organizational practices and auditor roles are adjusted to interpret and validate these new forms of digital records.

Despite their potential, CAIS are not without vulnerabilities. Issues such as unauthorized access, insider threats, and misconfigured cloud settings often result from gaps in the social subsystem including poor governance, insufficient training, or unclear responsibility for cybersecurity roles (Al-Nsour et al., 2021). STS theory emphasizes that mitigating these risks requires continuous alignment of technical advancements with human capabilities, ethical norms, and institutional structures.

In conclusion, cloud-based AIS contribute significantly to the protection of financial data through advanced technological defenses and compliance frameworks. However, from a Sociotechnical Systems Theory perspective, their true effectiveness depends on the harmonious integration of secure technologies with competent, well-trained users, robust organizational policies, and a strong culture of accountability. Only through the joint optimization of both technical tools and social practices can CAIS fulfill their potential as secure, resilient pillars of financial data protection in the digital era.

Potential Vulnerabilities of AI-Integrated Cloud Accounting Information Systems (AIS) and Mitigation Strategies

The integration of Artificial Intelligence (AI) into cloud-based Accounting Information Systems (AIS) has significantly advanced the efficiency and accuracy of financial reporting. However, this integration also introduces a range of

vulnerabilities particularly in cybersecurity, data privacy, algorithmic bias, and legal compliance that must be critically examined through the lens of Sociotechnical Systems (STS) Theory.

From a technical standpoint, AI-integrated AIS are susceptible to sophisticated cyber threats, including adversarial attacks that manipulate AI inputs to generate false outputs or unauthorized access (Bani Ahmad, 2024). Their reliance on interconnected platforms, including third-party APIs, introduces additional attack vectors that can compromise data integrity (Mustafa et al., 2024). These technical vulnerabilities cannot be fully addressed in isolation. STS theory asserts that system reliability depends on the interdependence of both technical tools and the social systems that govern their use. For example, while advanced encryption and multi-factor authentication are necessary defenses, their effectiveness depends on user compliance and awareness, reflecting the critical role of the human subsystem.

AI also introduces ethical and privacy concerns, especially when trained on large, heterogeneous datasets that can lead to unauthorized disclosures of sensitive information or perpetuate algorithmic bias (Rodriguez-Barboza et al., 2024). STS theory emphasizes the importance of ethical alignment between technology and organizational values. If the social structures such as ethics guidelines, data governance policies, or user training are underdeveloped, even the most advanced AI can generate biased or non-transparent outputs that undermine trust and accountability (Zhang et al., 2023; Moreira et al., 2025).

The issue of explainability highlights another STS principle: joint optimization. Many AI models embedded in AIS operate as "black boxes," making their decision-making processes opaque to users and regulators. This lack of transparency undermines the auditing and regulatory oversight functions essential to financial systems. Technical solutions such as explainable AI (XAI) must be matched by social practices such as revised audit methodologies, regulatory literacy, and stakeholder engagement to foster understanding and accountability across the system.

Legal and regulatory frameworks, including the European Union's Artificial Intelligence Act (AIA), are also placing increased pressure on organizations to ensure compliance in AI usage (Bertolini, 2024). STS theory suggests that organizational responses must go beyond adopting compliant technologies. They must cultivate adaptive social subsystems that include trained legal teams, compliance officers, and culturally embedded accountability structures to navigate rapidly evolving regulations.

From a systems integration perspective, challenges such as data inconsistency, legacy infrastructure incompatibility, and lack of interoperability are not purely technical barriers they are also symptoms of inadequate communication and coordination across departments (Türegün, 2025). STS theory identifies this as a misalignment between social workflows and technical system design, which can lead to breakdowns in system performance, delayed financial reporting, or increased error rates.

To mitigate these multidimensional vulnerabilities, organizations must adopt strategies that reflect the sociotechnical complexity of AI-integrated AIS.

Technological safeguards including end-to-end encryption, anomaly detection, blockchain-based audit trails, and AI-driven threat detection should be accompanied by robust social practices. These include regular ethics training, reskilling programs, transparent data governance policies, and inclusive stakeholder dialogue (Choudhary et al., 2023; Mathai & Mathew, 2024).

Moreover, adopting continuous monitoring through both technical means (e.g., automated security updates, real-time audits) and human oversight (e.g., independent third-party audits, ethical review boards) ensures system adaptability and resilience. This dual oversight aligns with the STS principle of equifinality, which allows organizations to achieve the same goal system security through multiple coordinated pathways.

To summarize, the vulnerabilities posed by AI-integrated cloud AIS are not merely technical in nature but stem from the complex interplay between people, technology, and organizational systems. Applying Sociotechnical Systems Theory reveals that achieving trustworthy, secure, and efficient financial reporting requires joint optimization of both technological tools and human-centered practices. Effective mitigation strategies must integrate cybersecurity infrastructure, legal compliance, ethical governance, and workforce engagement to build resilient, transparent, and accountable financial ecosystems in the digital era.

CONCLUSION AND RECOMMENDATION

This study systematically examined the integration of Artificial Intelligence (AI) and Cloud-Based Accounting Information Systems (CAIS) in enhancing financial reporting reliability and cybersecurity, framed within the Sociotechnical Systems (STS) Theory. The findings underscore that the synergy between advanced AI capabilities and cloud infrastructures significantly improves the accuracy, timeliness, and security of financial reports by automating routine tasks, enabling real-time analytics, and strengthening fraud detection mechanisms. However, these technological benefits are fully realized only when aligned with organizational readiness, ethical governance, and regulatory compliance, reflecting the core STS principle of joint optimization between social and technical subsystems.

The research revealed that while AI and CAIS enhance financial reporting reliability through predictive analytics and data integrity, they also introduce new vulnerabilities such as algorithmic bias, privacy concerns, cybersecurity threats, and system integration challenges that must be managed through comprehensive sociotechnical strategies. Moreover, the human dimension comprising trained personnel, ethical oversight, and adaptive governance structures is critical for mitigating risks and fostering trust in AI-driven accounting environments.

Despite these insights, the study acknowledges several limitations. The reliance on secondary data from existing literature constrains the ability to capture emerging, real-time technological developments and nuanced organizational dynamics. Additionally, the rapid evolution of AI and cloud technologies means that current findings may quickly become outdated, necessitating continual reassessment. The qualitative nature of the review limits

empirical validation of proposed frameworks, highlighting a need for primary data collection to deepen understanding.

ADVANCED RESEARCH

Future research should focus on longitudinal and mixed-method studies that explore the practical implementation of AI-integrated CAIS across diverse organizational contexts, particularly SMEs and emerging markets. Investigating user experiences, resistance factors, and the socio-cultural aspects of technology adoption can enrich the sociotechnical perspective. Furthermore, there is a pressing need to develop standardized ethical guidelines and regulatory frameworks that specifically address AI transparency, fairness, and accountability in financial reporting. Experimental research on explainable AI (XAI) and blockchain applications within cloud AIS would provide valuable evidence for optimizing both technical and social components.

In conclusion, this study contributes to bridging the gap between technology-centric and human-centric approaches to digital accounting transformation. It recommends a balanced, integrative approach that advances financial reporting reliability and cybersecurity not merely through technological innovation but through sustained organizational learning, ethical stewardship, and proactive policy engagement. Embracing this sociotechnical outlook will be essential for organizations aiming to harness AI and cloud technologies responsibly and effectively in the digital era.

REFERENCES

Abdulkareem Al yasiri, H. A., Samimi, A. J., & Tehranchian, A. M. (2024). The Impact of Anti-Money laundering Policies of Iraq Central Bank on the Quality of Financial Reports of Private Iraqi Banks. *Pakistan Journal of Life and Social Sciences*, *22*(1), 6481–6508. https://doi.org/10.57239/PJLSS-2024-22.1.00476

Abu-Dabaseh, F., Khtatbeh, M. M., Al'ararah, K., & Alassuli, A. (2025). Exploring the Role of Digital Transformation in Mitigating Accounting Fraud: A Cybersecurity Perspective. *International Review of Management and Marketing* , *15*(3), 398–405. https://doi.org/10.32479/irmm.18490

Akpabio, E., Narad, S., & Ulhe, P. (2024). The Evolution and Impact of Artificial Intelligence its Applications, Challenges, and Future Directions: A Review. *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Applications, ICAIQSA 2024 - Proceedings*. https://doi.org/10.1109/ICAIQSA64000.2024.10882203

Al-Nsour, E., Weshah, S., & Dahiyat, A. (2021). Cloud accounting information systems: Threats and advantages. *Accounting*, *7*(4), 875–882. https://doi.org/10.5267/j.ac.2021.1.021

Al-Ramahi, N., & Binsaddig, R. (2024). THE IMPACT OF THE QUALITY OF FINANCIAL REPORTS OF JORDANIAN PUBLIC SHAREHOLDING COMPANIES ON INVESTORS' DECISIONS. *International Journal of Economics and Finance Studies*, *16*(2), 409–442. https://doi.org/10.34109/ijefs.202416220

Al-Sammarraee, A., & Alshareeda, N. (2021). The role of artificial intelligence by

using automatic accounting information system in supporting the quality of financial statement. *Information Sciences Letters*, *10*(2), 223–254. https://doi.org/10.18576/isl/100208

Ali, S. A. M., Metwally, A. B. M., & Mohamed, A. T. I. (2024). Enhancing AIS Reliability: Suggested Framework for the Role of Trust Service and Artificial Intelligence. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2024*, 520–525. https://doi.org/10.1109/ICETSIS61505.2024.10459587

Alkan, B. (2022). *How Blockchain and Artificial Intelligence Will Effect the Cloud-Based Accounting Information Systems?* (pp. 107–119). https://doi.org/10.1007/978-981-16-8997-0_6

Asatiani, A., & Penttinen, E. (2015). Managing the move to the cloud - analyzing the risks and opportunities of cloud-based accounting information systems. *Journal of Information Technology Teaching Cases*, *5*(1), 27–34. https://doi.org/10.1057/jittc.2015.5

Askary, S., Abu-Ghazaleh, N., & Tahat, Y. A. (2018). Artificial intelligence and reliability of accounting information. In M. M., A.-S. S.A., S. A.C., T. L., M. I., A. T.M., J. M., D. Y.K., & R. N.P. (Eds.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11195 LNCS* (pp. 315–324). Springer Verlag. https://doi.org/10.1007/978-3-030-02131-3_28

Awad, A., Akola, O., Amer, M., & Mousa, E. K. A. (2025). Artificial intelligence in financial statement preparation: Enhancing accuracy, compliance, and corporate performance. *International Journal of Innovative Research and Scientific Studies*, *8*(2), 361–374. https://doi.org/10.53894/ijirss.v8i2.5166

Bani Ahmad, A. Y. A. (2024a). CS Challenge in Creating AI-Integrated System. *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2024*, 1515–1520. https://doi.org/10.1109/ICACITE60783.2024.10617153

Bani Ahmad, A. Y. A. (2024b). Ethical implications of artificial intelligence in accounting: A framework for responsible ai adoption in multinational corporations in Jordan. *International Journal of Data and Network Science*, *8*(1), 401–414. https://doi.org/10.5267/j.ijdns.2023.9.014

Bertolini, A. (2024). The European framework on the liability arising from the use of Artificial Intelligence systems and its impact on UAS. In *Civil Regulation of Autonomous Unmanned Aircraft Systems in Europe* (pp. 64–79). Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781035312344.00009

Bhosale, K. S., Ambre, S., Valkova-Jarvis, Z., Singh, A., & Nenova, M. (2023). Quantum Technology: Unleashing the Power and Shaping the Future of Cybersecurity. *Proceedings of 2023 8th Junior Conference on Lighting, Lighting 2023*. https://doi.org/10.1109/Lighting59819.2023.10299447

Cazazian, R. (2022). Blockchain Technology Adoption in Artificial Intelligence-based Digital Financial Services, Accounting Information Systems, and Audit Quality Control. *Review of Contemporary Philosophy*, *21*, 55–71. https://doi.org/10.22381/RCP2120224

Chandre, P., Shinde, M. B., Tilwant, S. V, Ghandat, A. B., Shendkar, B. D., & Dhotre, P. (2024). A Deep Q-Learning Approach to Intrusion Detection and

Prevention Systems: Enhancing Cybersecurity through Intelligent Adaptation. *2024 IEEE 4th International Conference on ICT in Business Industry and Government, ICTBIG 2024*. https://doi.org/10.1109/ICTBIG64922.2024.10911733

Chen, Y., & Xu, P. (2024). The Research on Cross-enterprise Collaborative Information System Based on NGIT. *ACM International Conference Proceeding Series*, 329–333. https://doi.org/10.1145/3671151.3671211

Clerkin, B., & McConville, D. (2022). INTEGRATING AIS AND CONTEMPORARY TECHNOLOGIES. In *The Routledge Handbook Of Accounting Information Systems, Second Edition* (pp. 303–317). Taylor and Francis. https://doi.org/10.4324/9781003132943-24

Darda, P., & Pendse, M. K. (2025). The impact of artificial intelligence (AI) transformation on the financial sector from the trading to security operations. In *Shaping Cutting-Edge Technologies and Applications for Digital Banking and Financial Services* (pp. 322–339). Taylor and Francis. https://doi.org/10.4324/9781003501947-20

Desmal, A. J., Alsaeed, M., Hamid, S., & Zulait, A. H. (2023). The Automated Future: How AI and Automation Are Revolutionizing Online Services. *International Conference on Engineering Technologies and Applied Sciences: Shaping the Future of Technology through Smart Computing and Engineering, ICETAS 2023*. https://doi.org/10.1109/ICETAS59148.2023.10346472

Ding, J. (2024). Application and Optimization of Cloud Computing in Financial Management Information Systems. *Learning and Analytics in Intelligent Systems*, *42*, 189–198. https://doi.org/10.1007/978-3-031-70598-4_18

Erb, C., & Pelger, C. (2015). "Twisting words"? A study of the construction and reconstruction of reliability in financial reporting standard-setting. *Accounting, Organizations and Society*, *40*, 13–40. https://doi.org/10.1016/j.aos.2014.11.001

Felix, A. Y., Sharmila, V., Devi, S. N., Deena, S., Yadav, A. S., & Jeyalakshmi, K. (2024). IoT based deep learning approach for online fault diagnosis against cyber attacks. In D. A., S. K., M. P.S., & S. D.K. (Eds.), *Artificial Intelligence, Blockchain, Computing and Security - Proceedings of the International Conference on Artificial Intelligence, Blockchain, Computing and Security, ICABCS 2023* (Vol. 1, pp. 569–573). CRC Press/Balkema. https://doi.org/10.1201/9781003393580-87

Firmansyah, B. (2024). Cybersecurity fundamentals. In *Challenges in Large Language Model Development and AI Ethics* (pp. 280–320). IGI Global. https://doi.org/10.4018/979-8-3693-3860-5.ch009

Gade, S., & Rao, K. M. (2022). Adoption of Cloud Computing to Accounting: Benefits and Challenges. *7th International Conference on Communication and Electronics Systems, ICCES 2022 - Proceedings*, 1652–1656. https://doi.org/10.1109/ICCES54183.2022.9835895

Gehlot, V., & Rana, P. S. (2024). AI in Mechatronics. In *Computational Intelligent Techniques in Mechatronics* (pp. 1–39). wiley. https://doi.org/10.1002/9781394175437.ch1

Gopalsamy, S., & Karthick, A. V. (2019). Security enhancement of online accounting data from cyber attacks. *International Journal of Recent Technology*

and Engineering, *8*(2 Special Issue 10), 427–431. https://doi.org/10.35940/ijrte.B1071.0982S1019

Ibrahim, M., Arabi, A. J., & Gurama, Z. (2024). Corporate attributes, audit committee and financial reporting quality of listed non-financial firms in Nigeria. *SN Business and Economics*, *4*(11). https://doi.org/10.1007/s43546-024-00719-1

Ionescu, L. (2021). Big Data Analytics Tools and Machine Learning Algorithms in Cloud-based Accounting Information Systems. *Analysis and Metaphysics*, *20*, 102–115. https://doi.org/10.22381/am2020217

Ionescu, L. (2022). Big Data Algorithms and Artificial Intelligence Technologies in Cloud-based Accounting Information Systems. *Analysis and Metaphysics*, *21*, 42–57. https://doi.org/10.22381/AM2120223

Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2022). The Duo of Artificial Intelligence and Big Data for Industry 4.0: Applications, Techniques, Challenges, and Future Research Directions. *IEEE Internet of Things Journal*, *9*(15), 12861–12885. https://doi.org/10.1109/JIOT.2021.3139827

Jindal, S., Sharma, A., Joshi, A., & Gupta, M. (2021). Artificial intelligence fuelling the health care. In M. N., T. C.C., K. D., & J. S. (Eds.), *Lecture Notes in Networks and Systems* (Vol. 140, pp. 501–507). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-15-7130-5_40

Kamila, M. K., & Jasrotia, S. S. (2025). Ethical issues in the development of artificial intelligence: recognizing the risks. *International Journal of Ethics and Systems*, *41*(1), 45–63. https://doi.org/10.1108/IJOES-05-2023-0107

Kapoor, M., Aggarwal, R., & Madan, S. (2024). Cyber-Security: Critical Analysis on Attacks, Classification, and Issues. In H. A.E., A. S., J. A., & K. P. (Eds.), *Lecture Notes in Networks and Systems: Vol. 1020 LNNS* (pp. 495–510). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-97-3588-4_40

Khoruzhy, L. I., Katkov, Y. N., & Romanova, A. A. (2023). Cloud Technologies in the Accounting Information System of Interorganizational Cooperation. In *Innovation, Technology and Knowledge Management* (pp. 25–37). Springer. https://doi.org/10.1007/978-3-031-13913-0_4

Kim, K., Park, C., Lee, W., Kim, S., & Seok, W. (2019). Large-scale threat traffic analysis and IDS development using software. *International Journal of Innovative Technology and Exploring Engineering*, *8*(3), 346–350. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85064673367&partnerID=40&md5=30d910deee2719fb4a94898474bec367

Kuaiber, M. Q., Ali, Z. N., Al-Yasiri, A. J., Kareem, A. J., Ali, M. A., & Almagtome, A. (2024). Automation and the Future of Accounting: A Study of AI Integration in Financial Reporting. *2024 International Conference on Knowledge Engineering and Communication Systems, ICKECS 2024*. https://doi.org/10.1109/ICKECS61492.2024.10616967

Kumar Jain, Y., Dhaarna Singh Rathore, C. A., Johrawanshi, A., Gupta, M., Choudhary, D. K., & Pandey, A. (2024). Cybersecurity Frameworks: A Roadmap for Business Resilience. *2024 International Conference on Cybernation*

and Computation, CYBERCOM 2024, 102–108. https://doi.org/10.1109/CYBERCOM63683.2024.10803234

Kumar, K., & Mandoria, H. L. (2024). Cybersecurity Threats, Forensics, and Challenges. In S. S., L. S., & K. M.S. (Eds.), *Lecture Notes in Electrical Engineering: Vol. 1220 LNEE* (pp. 281–295). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-97-4650-7_21

Lacmanovic, S., & Skare, M. (2025). Artificial intelligence bias auditing – current approaches, challenges and lessons from practice. *Review of Accounting and Finance*. https://doi.org/10.1108/RAF-01-2025-0006

Lai, C. Y., Li, Y., Shan, Y., & Taylor, S. (2013). Costs of mandatory international financial reporting standards: Evidence of reduced accrual reliability. *Australian Journal of Management*, *38*(3), 491–521. https://doi.org/10.1177/0312896213511089

Lugovsky, D., & Kuter, M. (2020). Accounting Policies, Accounting Estimates and Its Role in the Preparation of Fair Financial Statements in Digital Economy. In *Lecture Notes in Networks and Systems* (Vol. 78, pp. 165–176). Springer. https://doi.org/10.1007/978-3-030-22493-6_15

Lustrilanang, P., Arif, B., & Subowo, H. (2023). The effect of auditing quality and internal control on financial resilience in public sector organizations: Information quality as the mediating factor. *International Journal of Data and Network Science*, *7*(4), 1573–1580. https://doi.org/10.5267/j.ijdns.2023.8.006

Lutfi, A. (2022). Understanding the Intention to Adopt Cloud-based Accounting Information System in Jordanian SMEs. *International Journal of Digital Accounting Research*, *22*, 47–70. https://doi.org/10.4192/1577-8517-v22_2

Maines, L. A., & Wahlen, J. M. (2006). The nature of accounting information reliability: Inferences from archival and experimental research. *Accounting Horizons*, *20*(4), 399–425. https://doi.org/10.2308/acch.2006.20.4.399

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). *NIPES - Journal of Science and Technology Research*, *6*(2), 293–311. https://doi.org/10.5281/zenodo.12617068

Mauri, L., & Damiani, E. (2022). Modeling Threats to AI-ML Systems Using STRIDE †. *Sensors*, *22*(17). https://doi.org/10.3390/s22176662

Meher, A. (2024). Revolution ethics of data science and AI. In *The Ethical Frontier of AI and Data Analysis* (pp. 245–256). IGI Global. https://doi.org/10.4018/979-8-3693-2964-1.ch015

Minz, N. K. (2024). Ethical considerations in AI applications in finance: Frameworks, transparency, accountability, and case studies. In *Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security* (pp. 277–290). IGI Global. https://doi.org/10.4018/979-8-3693-2185-0.ch012

Moreira, N. A., Freitas, P. M., & Novais, P. (2025). Towards Transparent AI: How will the AI Act Shape the Future? In S. M.F., M. J., N. P., C. P., & M. P.M. (Eds.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) : Vol. 14967 LNAI* (pp. 296–307). Springer Science and Business Media Deutschland GmbH.

https://doi.org/10.1007/978-3-031-73497-7_24

Mustafa, F. M., Salman, A. S., Shukur, M., & Al-Nuiami, S. A. W. A. R. (2024). Strategies for Strengthening Security in Accounting Information Systems. *Journal of Ecohumanism*, *3*(5), 293–315. https://doi.org/10.62754/joe.v3i5.3902

Noordin, N. A., Hayek, A., Sejdini, M., Humaid, A., Sultan, N., Abdulla, B., & Yousif, M. (2024). Financial Information Quality: Analysis of Cloud Accounting Adoption on UAE Firms. In *Lecture Notes in Operations Research: Vol. Part F3798* (pp. 325–340). Springer Nature. https://doi.org/10.1007/978-3-031-61589-4_25

Paliwal, M. (2023). A review on cyber security. In A. R., S. R., G. T.K., M. N.K., T. A., & A. null (Eds.), *AIP Conference Proceedings* (Vol. 2427). American Institute of Physics Inc. https://doi.org/10.1063/5.0101190

Quoc, T. N. K., Hong, V. T., Van, T. L., Minh, H. N., & Ngoc, O. 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://doi.org/10.15549/jeecar.v11i1.1432

Qureshi, K., Sadeq, S. H., & Manuel, P. (2024). Analysis of Security Challenges in Cloud Computing Adoption for the Banking Sector. *International Journal of Computers and Their Applications*, *31*(4), 308–320. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85215948301&partnerID=40&md5=ddf11d09d203cac2a4998f711e2ce5b9

Rahahleh, M. H., Hamzah, A. H. B., & Rashid, N. (2021). The Artificial Intelligence in the Audit on Reliability of Accounting Information and Earnings Manipulation Detection. In *Studies in Computational Intelligence* (Vol. 974, pp. 315–323). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-73057-4_24

Rodriguez-Barboza, J. R., Carreño-Flores, O. D., Davila-Zamora, L. M., Jalixto-Erazo, H. M., Santos, M. A. O., Cruces-Torres, O. J., Ruiz-Villavicencio, R. E., & Villegas-Rivas, D. (2024). Posthumanist Technologies in Business: AI and Cloud Computing for Global Optimization and Ethical Challenges. *Advance Sustainable Science, Engineering and Technology*, *6*(4). https://doi.org/10.26877/asset.v6i4.1064

Ruissalo, J., Penttinen, E., & Asatiani, A. (2022). Fluid Socio-Technical (Trans)formation of an AI system. In B. T.X. (Ed.), *Proceedings of the Annual Hawaii International Conference on System Sciences* (Vols. 2022-Janua, pp. 6964–6973). IEEE Computer Society. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85152238883&partnerID=40&md5=5a6509a17d8081fe11725a58050d8e8f

Sethy, A., Shaik, N., Yadavalli, P. K., & Anandaraj, S. P. (2023). AI: Issues, concerns, and ethical considerations. In *Toward Artificial General Intelligence: Deep Learning, Neural Networks, Generative AI* (pp. 189–211). De Gruyter. https://doi.org/10.1515/9783111323749-009

Shakdwipee, P., Agarwal, K., Kunwar, H., & Singh, S. (2023). Artificial Intelligence in Finance and Accounting: Opportunities and Challenges. In T.

M., A. S., & J. A. (Eds.), *Lecture Notes in Networks and Systems: Vol. 765 LNNS* (pp. 165–177). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-99-5652-4_17

Shchyrba, I., Lagovska, O., Demianyshyna, O., Myronchuk, Z., & Shebeshten, E. (2025). Regulatory Challenges and Cybersecurity Approaches in Cloud-Based Accounting Systems. *Journal of Information Systems Engineering and Management*, *10*, 443–452.

Shinde, S. S., Kale, G. M., Nalbalwar, S. L., & Deosarkar, S. B. (2024). Navigating the Cyber Battlefield: Understanding Threats and Safeguarding Digital Frontiers. *2024 International Conference on Electrical, Electronics and Computing Technologies, ICEECT 2024*. https://doi.org/10.1109/ICEECT61758.2024.10739310

Thaher, M. S. (2024). Cloud Computing: Enhancing or Compromising Accounting Data Reliability and Credibility. *International Journal of Advanced Computer Science and Applications*, *15*(12), 159–164. https://doi.org/10.14569/IJACSA.2024.0151217

Tiwari, M., Tiwari, T., Ticku, A., Dadhwal, H., & Singh, T. (2023). Methodologies and Challenges of Cybersecurity Techniques in Cloud Computing Environment. In G. D., K. A., S. D., P. M., J. P., G. B.B., & S. U.P. (Eds.), *ACM International Conference Proceeding Series*. Association for Computing Machinery. https://doi.org/10.1145/3647444.3652492

Türegün, N. (2025). Challenges and Opportunities: Integrating AI Into Accounting Systems. *Journal of Corporate Accounting and Finance*. https://doi.org/10.1002/jcaf.22788

Twyford, E. J., & Abbas, R. (2023). Broadening the boundaries of accounting: a call for interdisciplinarity in the calculative era. *Meditari Accountancy Research*, *31*(1), 187–211. https://doi.org/10.1108/MEDAR-06-2021-1338

Ullah, M. W., Alam, M. T., Sultana, T., Rahman, M. M., Faraji, M. R., & Ahmed, M. F. (2024). A systematic review on information security policies in the USA banking system and global banking: Risks, rewards, and future trends. *Edelweiss Applied Science and Technology*, *8*(6), 8437–8453. https://doi.org/10.55214/25768484.v8i6.3816

Vo Van, H., Abu Afifa, M., & Saleh, I. (2024). Accounting information systems and organizational performance in the cloud computing era: evidence from SMEs. *Sustainability Accounting, Management and Policy Journal*. https://doi.org/10.1108/SAMPJ-01-2024-0044

Wahhab, A., Alkhafaji, B. K. A., & Raji, S. M. (2024). THE SIGNIFICANCE OF CLOUD ACCOUNTING IMPLEMENTING AND ITS INFLUENCE ON ENHANCING THE QUALITY OF FINANCIAL REPORTING: EVIDENCE FROM EMERGING MARKETS. *Financial and Credit Activity: Problems of Theory and Practice*, *1*(54), 146–159. https://doi.org/10.55643/fcaptp.1.54.2024.4293

Xi, S. N., Yee, T. P., & Nair, R. K. (2019). Factors affect the audit quality of external auditor at klang valley. *ACM International Conference Proceeding Series*, 18–23. https://doi.org/10.1145/3377817.3377821