Management (Montevideo). 2025; 3:252
doi: 10.62486/agma2025252
ISSN: 3046-4048

ORIGINAL

Challenges of Cloud Accounting Systems Landscape within the Context of Cybersecurity Paradigm

Retos del panorama de los sistemas de contabilidad en nube en el contexto del paradigma de la ciberseguridad

Iryna Shchyrba[1,2], Olena Lagovska[3], Olesia Demianyshyna[4], Zoriana Myronchuk[5], Edina Shebeshten[6]

[1]West Ukrainian National University, Department of Financial Control and Audit. Ternopil, Ukraine.
[2]Nottingham University Business School (NUBS). Nottingham, United Kingdom.
[3]Zhytomyr Polytechnic State University. Zhytomyr, Ukraine.
[4]Pavlo Tychyna Uman State Pedagogical University, Department of Finance, Accounting and Economic Security. Uman, Ukraine.
[5]Lviv National Environmental University, Faculty of Economics, Management and Law. Lviv, Ukraine.
[6]Ferenc Rakoczi II Transcarpathian Hungárián College of Higher Education, Department of Accounting and Auditing. Berehove, Ukraine.

Cite as: Shchyrba I, Lagovska O, Demianyshyna O, Myronchuk Z, Shebeshten E. Challenges of Cloud Accounting Systems Landscape within the Context of Cybersecurity Paradigm. Management (Montevideo). 2025; 3:252. https://doi.org/10.62486/agma2025252

Submitted: 17-06-2024 **Revised:** 12-01-2025 **Accepted:** 10-06-2025 **Published:** 11-06-2025

Editor: Ing. Misael Ron

Corresponding author: Iryna Shchyrba

ABSTRACT

Introduction: the evolution of cloud-based systems of accounting and the regulatory backing for them between 2020 and 2024 are examined in this article
Objective: identifying the current challenges experienced by corporate sector in cloud accounting systems operation, in particular in the landscape of the effects of cybersecurity tactics and legal requirements is the goal of this study.
Method: based on the methodology of comparative analysis and synthesis, with an emphasis on data security and risk management, the contemporary cybersecurity challenges of cloud-based accounting practices and the features of appropriate regulatory requirements landscape are examined.
Results: the authors emphasize the difficulties posed by rising cyberthreats in the context of the expanding use of cloud-based systems for processing financial data. The primary multi-factor authentication and data encryption-based cybersecurity tactics are described. The essay examines how, in light of rising transaction volumes and cyberthreats, industrialized nations are strengthening their cybersecurity and financial regulation standards. The market for cloud accounting systems is expected to grow in the following five years in the following primary directions. The paper focuses in particular on how government organizations are involved in creating regulations for cloud accounting systems. Consideration is given to the tactics of the of imposing technology standards on cloud providers in order to guarantee market stability and security.
Conclusions: the significance of adhering to global standards for cloud systems is discussed in the article.

Keywords: Cloud Computing; Cloud Solutions; Accounting Systems; Regulations; Cybersecurity; Cyber Threats.

RESUMEN

Introducción: en este artículo se examina la evolución de los sistemas de contabilidad en la nube y su respaldo normativo entre 2020 y 2024.
Objetivo: encontrar los efectos de las tácticas de ciberseguridad y los requisitos legales en el desarrollo de

los sistemas de contabilidad en la nube en el sector empresarial es el objetivo de este estudio.
Método: sobre la base de la metodología de análisis comparativo y síntesis, con énfasis en la seguridad de los datos y la gestión de riesgos, se examinan los desafíos contemporáneos de ciberseguridad de las prácticas contables basadas en la nube y las características del panorama de requisitos regulatorios apropiados.
Resultados: los autores destacan las dificultades que plantea el aumento de las ciberamenazas en el contexto del uso creciente de sistemas basados en la nube para el tratamiento de datos financieros. Se describen las principales tácticas de ciberseguridad basadas en la autenticación multifactor y el cifrado de datos. El ensayo examina cómo, a la luz del aumento del volumen de transacciones y de las ciberamenazas, las naciones industrializadas están reforzando sus normas de ciberseguridad y regulación financiera. Se espera que el mercado de los sistemas de contabilidad en la nube crezca en los próximos cinco años en las siguientes direcciones principales. El documento se centra en particular en cómo las organizaciones gubernamentales participan en la creación de normativas para los sistemas de contabilidad en nube. Se considera la táctica de imponer normas tecnológicas a los proveedores de la nube para garantizar la estabilidad y seguridad del mercado.
Conclusiones: en el artículo se discute la importancia de adherirse a estándares globales para los sistemas en nube.

Palabras clave: Computación en Nube; Soluciones en Nube; Sistemas Contables; Normativa; Ciberseguridad; Ciberamenazas.

INTRODUCTION

In today's business landscape, which evolves quickly, cloud solutions in finance and accounting have emerged as indispensable tools for market players striving to optimization of their financial operations. Cloud-based accounting solutions have grown dramatically in recent years as a result of rapid technological improvement in the financial management of corporate sector initiatives. In the digital transformation era, businesses choose solutions that assure automation, business continuity, and security of business processes. Accounting systems are actively implementing cloud-based infrastructure, which provides remote access to financial data and integrates with other corporate systems to automate routine activities to a high extent. The concepts of effective data processing and openness of accounting operations help organizations improve their efficiency in global trading activities.[1]

The swift expansion of the transactions and data handled by cloud platforms has led to heightened legal regulation. To guarantee that cloud systems adhere to legal and financial standards, government regulators in numerous nations including the US Federal Reserve and the European Union through the GDPR are enforcing stringent data security regulations. The objectives of these steps are to lower the risk of financial fraud, preserve sensitive data, and increase operational transparency.

Cloud system cybersecurity has emerged as a focal point of international conflicts under ongoing economic strains. The increasing frequency of cyberattacks as a tactic in trade conflicts is a clear example of this. According to Yin,[2] among the most well-known cases, there are the actions taken by the DPRK, China, and the United States within the activities on carrying out such operations. There is an evident necessity of modernizing cloud infrastructure to ensure a proper level of resistance to cyberattacks and data leaks in light of the emerging geopolitical conflicts that governments and businesses face and must deal with. Traditional security mechanisms can be improved, data encryption can be strengthened, and also adding multi-factor authentication mechanisms can be applied. At the same time, businesses are increasingly implementing cutting-edge artificial intelligence technologies to automate threat detection. Large organizations are employing rather creative cyber defense methods intended to ensuring business continuity, lowering system vulnerability to attacks, and limiting the dangers associated with cloud platforms functioning.

The shift to cloud-based software for accounting, which allows accounting professionals to access and handle financial data in real-time, not depending on any location, is marking a new era of efficiency and collaboration in accounting domain. The usage of cloud accounting systems is being stimulated by the prospect of more flexibility, adaptability, and the potential for ensuring higher-quality products and services. As businesses and accounting practices go over this digital horizon, this is a pivotal moment in the history of the accounting industry with important ramifications for practice efficient management, achieve client communication, and data protection.

With the process of active integration of technological advancements into business operations in 2020s, the issues of cloud accounting systems and their effects on the corporate sector received significant attention. Accounting process automation was evidently facilitated by cloud platforms.[3] As a result, firms, especially

large ones, now are capable of managing financial data more efficiently.[4] The ability to centrally store and manage financial transactions represents a crucial component of such systems in view of diminishing the possibility of human mistake. According to the study by Kmaleh,[5] cloud platform adoption is now essential for modernizing financial management systems in multinational firms. In particular, scalability is supported by these technologies, which offer constant access to data from any device.

Enhacing the legislative landscape governing cloud accounting systems in various nation-states in in regional plane is another important study concern. According to Abdo et al.,[6] new rules have been introduced to safeguard financial data as a result of the increase in data volumes. One of the most important and known laws governing the processing and storage of financial data in cloud systems is the General Data Protection Regulation (GDPR), adopted in the European Union. In turn, in the U.S., according to Kawar and Daviglus,[7] the Federal Reserve is essential agency within the landscape of these matters regulation. It establishes guidelines for risk management when conducting financial transactions using cloud platforms. The function of such legislative base highlights the worldwide trend toward more data security and transparency.

With the rise in cyberattacks globally, cloud accounting system cybersecurity has become even more crucial. Musyaffi et al.[8] found that throughout the previous three years, there has been a 30 % increase in cloud platform attacks. This motivates businesses to create fresh approaches to cyber defense. The paper by Yin[2] explains how, in the face of increasing cyberattacks, data encryption, traffic monitoring technologies, and multi-factor authentication have become crucial for safeguarding financial data. The author also discusses the function of the Salesforce and SAP Cloud platforms, which integrate contemporary automation techniques to guarantee the security of sensitive data.

Academics argue over the underlying reasons behind the financial industry's quick adoption of digital technologies, which is part of the global trend toward digitalization.[9] According to Malusare,[10] cloud platforms automate tasks and lower the cost of IT infrastructure while increasing productivity. According to the Levytska et al.[11] study, automating the majority of cloud system operations is crucial for enhancing financial data analytics. This enables companies to react to shifts in the economic landscape faster. Machine learning technologies are mostly utilized to forecast financial performance and possible chances for lowering business risks, according the findings of the King et al.[12] research.

A major focus of current study is the question of cloud accounting systems' legal regulation. Data storage in cloud systems is now governed by the General Data Protection Regulation in the European Union. The legislative requirements for cloud platforms in different locations applying cybersecurity methods are examined in the Pradesa et al.[13] study. In order to safeguard global financial transactions, the paper also emphasizes how crucial it is that G7 nations standardize their cybersecurity regulations for 2025–2026.[13]

Researchers prioritize cyberattack prevention because early identification reduces negative repercussions by securely protecting data. According to Thaher,[14] cloud systems require stronger data access control and multi-factor authentication installation to protect against intruders. Liu[15] investigates the influence of implementing new encryption technologies on financial data security. According to the author, innovative cybersecurity solutions based on new tools that will be actively implemented in 2023-2024 are critical for defending cloud systems from escalating threats. Thus, scientific research analyzes the uniqueness of cloud systems operating in a dynamic environment, which necessitates continuous monitoring for regulatory compliance.

Finding the effects of cybersecurity tactics and legal requirements on the development of cloud accounting systems in the corporate sector is the goal of this study. The analysis focuses on contemporary technology platforms and how they affect data management and financial process automation. The foundation of the study is an examination of the ways in which government agencies in different jurisdictions implement legislative regulations and how they actually contribute to the security of financial data in cloud systems. The article examines the components of cybersecurity tactics intended to thwart cyberattacks, as well as their variants and the challenges associated with detection in a forward-thinking digital marketplace.

METHOD

Two categories of methodologies were employed in the research methodology: theoretical and empirical. Based on recent studies, we traced scientific data on the evolution of cloud accounting systems using synthesis and analytic techniques. Information on current cybersecurity trends and legislative needs in various nations was compiled with the aid of data synthesis from multiple sources. Then, the dynamics of the cloud accounting systems market from 2020 to 2024 were evaluated using statistical analysis and comparative research techniques. The efficacy of several cloud systems with respect to data security and regulatory compliance was compared.

The research process included analyzing current data security requirements and determining the key trends in the development of cloud technologies in accounting. During the initial phase, we examined critical cloud systems with an emphasis on adherence to global cybersecurity guidelines. The second phase examined

cybersecurity tactics, such as threat detection systems, access control, and data encryption techniques. Based on an analysis of the most widely used corporate platforms in international business, the systems were chosen. Technology's effect on accounting process automation was used to evaluate how the business sector changed in reaction to the advent of cloud technologies.

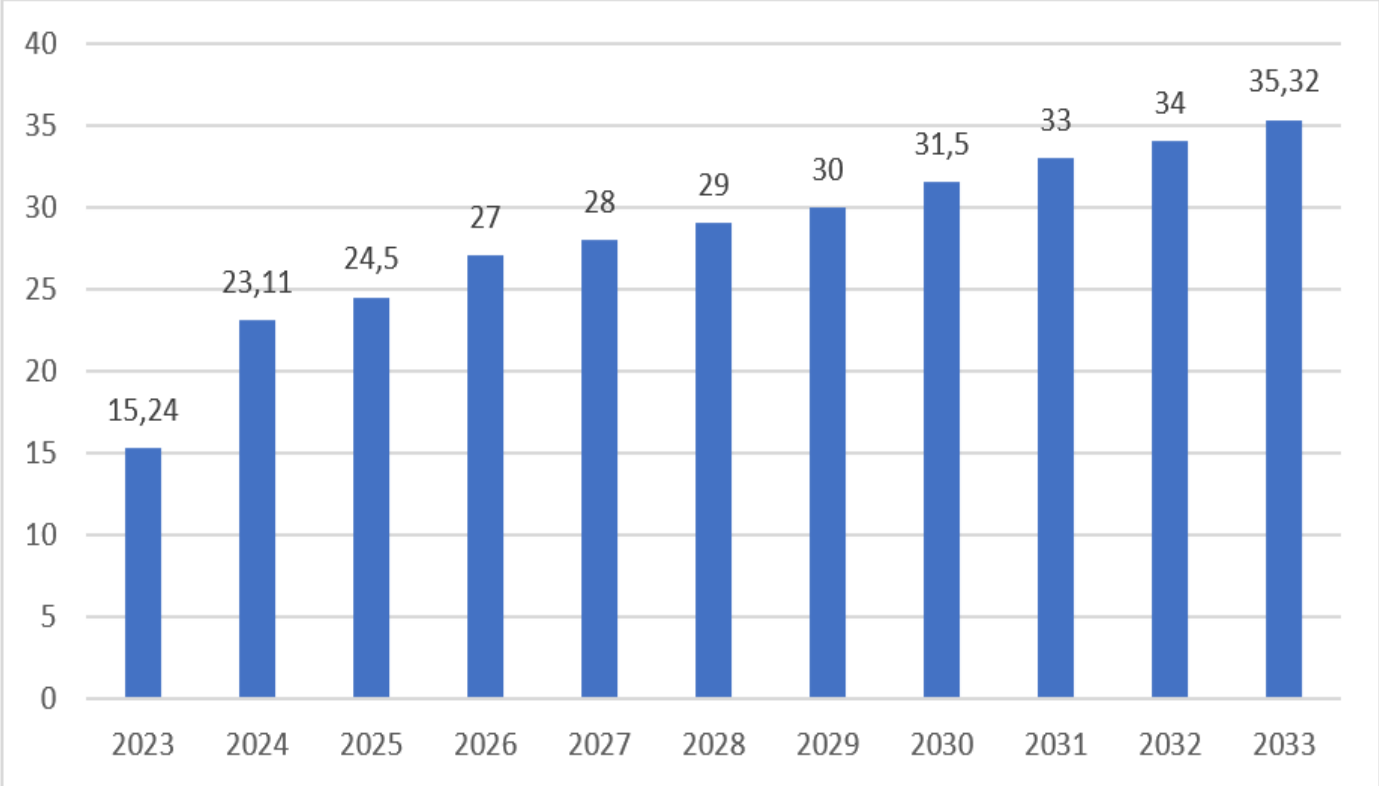
Using cloud-based technology has increased the efficiency of financial management, and the article examines how businesses have adjusted their business models to the new environment. The research employed comparative analysis techniques to assess various strategies for integrating regulatory requirements into cloud accounting systems across several nations, in particular, in Gulf countries. This methodology facilitated the identification of similarities and distinctions between data management and cybersecurity strategies. Data privacy regulations and cyber threat mitigation techniques were integrated with special attention.

RESULTS AND DISCUSSION

Accounting data and financial activities can be accessed online through cloud-based accounting systems, which are interconnected technological platforms. According to its etymology, the term "cloud" refers to the metaphorical representation of the Internet as a cloud that first surfaced in the 1990s to denote remote access to resources that were not part of the local infrastructure.

Cloud systems are epistemologically significant because they represent a new paradigm for data management that prioritizes accessibility, mobility, and scalability over the physical location of information. Cloud accounting solutions are being used to lower IT infrastructure costs, streamline reporting, and automate financial processes. They provide useful resources for tracking spending, managing cash flows, and predicting financial outcomes. These elements make them indispensable in the globalized economy and dynamic markets of today.

Small and medium-sized enterprises, in particular, view cloud systems as a chance to lower the cost of maintaining their IT infrastructure. Predictive statistics of global cloud accounting technology market is presented in figure 1. The Cloud Accounting Software Market is expected to increase from USD 26,78 billion in 2025 to USD 77,29 billion by 2034, with a compound yearly growth rate (CAGR) of 12,83 % over the forecast period (2025–2034). Furthermore, Dhapte[16] estimated that the Cloud Accounting Software Market was USD 23,11 billion in 2024 (figure 1). Cloud accounting has a number of key benefits, briefly summarized in table 1, in particular in comparison with traditional accounting software.



Source: Spherical Insights[17]

Figure 1. Global cloud accounting tecgnology market, 2023–2033 (in USD bln)

Table 1. Key benefits of cloud accounting

Benefits	Details	Cloud Accounting in comparison with Traditional Accounting Software
Visibility and Reporting	A wide variety of new capabilities in reporting and analytics are available through cloud accounting software to create financial statements, monitor key performance indicators (KPIs), and deliver the data on the company's financial health. These characteristics assist companies in efficiently tracking their financial performance and making well-informed decisions	*Flexibility*: How they are accessible and hosted is where cloud accounting and traditional accounting software diverge most. Usually deployed on local PCs or servers, traditional accounting software necessitates manual upkeep and upgrades. Because it functions within a closed network, only users connected to the network or via remote desktop connections can access it. Cloud-based accounting software, on the other hand, is accessible online and housed on distant servers. With online browsers or specialized apps, users may access their financial information and do accounting activities at any time and from any location
Accessibility	With internet-connected devices, customers may access their financial data and do accounting duties from any location at any time thanks to cloud accounting. For companies with numerous locations or remote staff, this accessibility allows for flexibility and real-time cooperation	*Cost structure and scalability*: Purchasing hardware, software licenses, and IT infrastructure up front is frequently necessary for traditional accounting software. Moreover, cloud accounting software is based on a model of subscription. With this subscription approach, it is no longer necessary to bear significant upfront expenses; also, it enables greater flexibility in scaling accounting processes as necessary
Real-Time Data	Financial data synchronization and real-time changes are offered via cloud accounting. This guarantees accurate and fast financial reporting by giving customers access to the most recent data, including bank transactions, invoices, and expenses	*Collaboration*: Enhanced opportunities for collaboration represent another benefit of cloud-based accounting. The ability provided for multiple users to view and operate on the same financial data simultaneously promotes real-time cooperation and contributes to enhancing companies internal communication. On the contrary, using traditional accounting software, as a rule, implies manual data transfers or backups to share information
Automation	A broad range of accounting procedures, in particular bank reconciliations, invoice creation, and spending tracking, are automated by software for cloud accounting. Companies may concentrate on more critical financial tasks thanks to this automation, which decreases human data entry, lowers errors, and saves time	*Automatic updates*: Without the need for manual upgrades, cloud accounting software ensures that companies always have access to the newest features, security patches, and bug fixes. Traditional accounting software may not always keep up with the most recent regulations and standards and needs manual changes
Integration	Integrations with various business apps, including inventory management software, payment gateways, and CRM systems, are frequently provided by cloud accounting solutions. By removing the need for manual data entry and streamlining operations, this integration capability promotes smooth data interchange and increases overall efficiency	*Flexible General Ledger*: A customizable general ledger provided by cloud financial systems enables companies to adjust their reporting hierarchies, account structures, and chart of accounts to meet their unique requirements. Business sector players can adjust their financial management procedures to changing needs, including adding new accounts or modifying current ones, thanks to this flexibility. At the same time, the rigid frameworks of traditional accounting software limits the general ledger's flexibility and adaptability
Scalability	Software for cloud accounting is made to grow with the demands of companies. It does not have a need in major hardware or infrastructure changes even in case of significant increase in volume transactions, number of users, and scope of data. Thanks of its scalability, the cloud accounting software is capable of adjusting to evolving needs of the company	*Automated Billing Processes*: Cloud financial solutions enable full automation of billing procedures, in particular, invoice production, payment reminders, and reconciliation. This automation contributes to minimizing human factor impact, saves time, and enhances cash flow management. In contrast, traditional accounting software often involves manual entry and processing of invoices, resulting in errors, inefficiencies and delays in billing procedures
Security	Data security is a top priority for cloud accounting providers, who take strong precautions to safeguard private financial data. This implies extensive access controls, frequent backups, and data encryption. To guarantee data privacy and adherence to industry laws, cloud accounting systems frequently feature specialized security teams and infrastructure	*Security*: Cloud accounting offers a safe way to store financial data, frequently outperforming traditional software in terms of security. Because data access is password-protected and encrypted, there is less chance of data breaches involving misplaced or stolen devices

Collaboration	Collaboration between team members, accountants, and financial consultants is made possible by cloud accounting software. The ability for multiple people to view and operate on the same financial data at once promotes cooperation and enhances internal communication	*Intelligent Analytics*: Cloud finance solutions give firms actionable insights into their financial data by utilizing advanced analytics capabilities. These systems are capable of processing and analysing significant amounts of financial data, as well as identifying trends, patterns, and anomalies properly, with the use of machine learning algorithms and data visualization tools. This enables making data-driven decisions, maximizing financial performance, and using all the potential of opportunities for development. Naturally, these analytics features are usually lacked in traditional accounting software, which implies manual data analysis and reporting

Source: compiled by the authors based on Spherical Insights[17]

In May 2024, AI Account presented and launched the first in Asia cloud-based accounting solution designed specifically for SMEs. It employs AI technology for verifying compliance with local regulatory frameworks in real-time, providing SMEs with a powerfull and at the same time user-friendly platform tailored to their specific needs. The cloud accounting software intends to remove barriers for SMEs looking to simplify their financial business processes. AI Account allows customers to see firsthand the promise of AI-driven accounting by providing access to its many possibilities.

One of the Asian countries characterized with the rapid development of cloud-based accounting is Malaysia. In particular, ABBAZ Advisory Sdn Bhd (AASB) is a leading audit firm in Malaysia that offers virtual chartered accountant services. The company has served over 100 clients since its establishment in 2012, the majority of which are local companies. The business has a strong presence in Malaysia's manufacturing, services, financial, commercial, and public sectors. AASB started using QuickBooks accounting software in 2012. The program's main target audience is small business owners that need flexibility in managing accounting data in addition to an easy-to-use software package and framework to support their operations.

Previously, the software was available as desktop apps and was installed using a CD-ROM. QuickBooks is currently the application that its clients favor because to its cloud-based software offerings. With the help of this tailored cloud-based solution, the business can use a mobile workforce to provide better customer care and support. Data can be accessed from anywhere at any time using a laptop, smartphone, or tablet. The company's employees can access their PCs, data, and programs remotely. The enhanced mobility and connection have led to a rise in employee productivity and client service.[18]

Because of their simplicity of use, global data accessibility, and rapid business needs adaptation, cloud-based accounting solutions are frequently employed. Notwithstanding its many benefits, each system has drawbacks that affect businesses' choices to use it. Because they have an impact on data protection and the financial success of the business, regulatory compliance and maintaining a sufficient degree of cybersecurity are particularly important challenges. The transition from legacy systems to cloud-based solutions has improved operational processes such as accuracy and real-time data access, but data security and service reliability remain pressing concerns. The core challenges of cloud-based accounting systems are summarized in table 2.

Table 2. Core challenges of cloud-based accounting systems

Challenge	Essence description
Data Security and Privacy Risks	Relying on outside cloud providers to protect private financial information creates risks of data breaches, illegal access, and cyberattacks, which can have detrimental effects on one's finances, reputation, and legal standing
Service Interruptions	Because cloud computing depends on internet access, there is a chance that services could be interrupted, which could affect productivity and corporate operations. This issue has been brought to light by significant failures by cloud services like Microsoft Azure and Amazon Web Services (AWS)
Vendor Lock-In	When switching to alternative solutions, an over-reliance on one cloud provider can lead to challenges and expensive costs, which could inhibit innovation and increase operating costs
Regulatory Compliance	Maintaining compliance is made more difficult by the disparities in data protection laws throughout jurisdictions, which is essential for businesses managing sensitive financial data
Integration Issues	The accuracy of financial data may be jeopardized by the difficult and error-prone process of integrating cloud-based systems with legacy technologies

Source: compiled by the authors based on Raza[19]

As more people utilize cloud-based accounting solutions, worries about data security are growing. The move to the cloud makes it more difficult to defend sensitive financial information against internet threats. The best

cloud accounting systems are designed with highly functional security features to maintain data confidentiality and integrity. Multi-factor authentication, data encryption, and regular security audits to ensure compliance with regulations and industry standards represent some examples of these advantages.

Moreover, the inherent flexibility of cloud itself enables real-time upgrades and repairs, significantly reducing exposure to cyber-attacks and unauthorized intrusions. Despite these possibilities, however, everyone in the organization is accountable for data security. Users should act with caution and adhere to suggested practices such as using secure passwords and limiting access. Actually, a proactive strategy is required to handle data security in the cloud, combining cutting-edge technology with users' awareness to create a secure online environment for financial management.

One should bear in mind that accounting information systems (AIS) are particularly vulnerable to cyber incidents since they are dealing with sensitive financial data. Data breaches and cyber-attacks determine the necessity for excellence in designing security mechanisms to safeguard cloud-based accounting systems.[20] It should be emphasised that, back in 2021, more than 1,200 data breaches were reported in the United States, with many of them involving cloud platforms.

Evidently, such breaches can result in financial losses, legal liabilities, and reputational harm. To manage these risks, firms must skillfully combine purely technical and organizational approaches. Encryption, access control systems, and frequent regular security audits are critical for improving the security of cloud-based AIS.[21] Moreover, as it is known, multi-factor authentication (MFA) inhibits unauthorized access.[22]

Backup and recovery techniques are key components of a secure cloud-based AIS, since they provide data recovery in the event of a security compromise or system failure. Compliance with international security standards, such as ISO 27001 and SOC 2, is rather critical condition for cyber protection of cloud-based accounting systems. These compliance frameworks represent sound assistance for firms in developing, implementing, and managing security measures while adhering to regulatory obligations.[23]

Moreover, employee training and awareness initiatives are critical in preventing security breaches, since often namely human error is a common element within the array security incidents causes. Thus, educating personnel on security best practices can diminish the possibility of breaches due to negligence or a lack of awareness.[5]

Evidently, data encryption is a critical security element for cloud-based accounting systems, ensuring that unauthorized users cannot access information without a decryption key. In particular, Advanced Encryption Standards (AES) and Secure Socket Layer (SSL) encryption are widely used to safeguard data, adding an extra layer of security.[24] Role-based access control (RBAC) improves security by limiting access to critical data based on user responsibilities within an organization.[14] Moreover, implementing strong backup and recovery methods is highly important for reducing data loss in the event of a cyber-attack, system failure, or even natural disaster.[25] To preserve data integrity, organizations should implement complete and comprehensive backup procedures, which include regular backups, safe storage, and scheduled routine recovery tests.

No doubt that namely compliance with security requirements represents critical framework for improving the security of cloud-based accounting systems. Adhering to frameworks such as Europe's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA) indicates an organization's dedication to data security and legal compliance.[26]

It is worth noting that many cloud service providers perform third-party audits to ensure compliance, reassuring clients that their data is secure.[5] Furthermore, personnel training and security awareness programs are essential components of a comprehensive security strategy. Human errors causes a substantial percentage of security breaches.[27] Organizations must invest in ongoing security awareness training to educate staff on current and potential security threats, as well as effective data protection methods.[27]

Interestingly, however, the study by Sanusi et al.[27] integrates regression and artificial neural network (ANN) analyses to validate the importance of key security measures, offering a thorough understanding of the factors influencing the security of cloud-based accounting information systems. According to the regression results, presented by the authors, security is greatly improved by data encryption, access control systems, backup and recovery protocols, and adherence to security standards, whereas user awareness and training have no statistically meaningful impact. These conclusions are further supported by the ANN model, which ranks data encryption as the most important element, followed by access control methods, adherence to security standards, and backup and recovery protocols. User awareness and training are ranked as the least important factors.[28]

Speaking about practical examples, it is worth mentioning that one of the largest financial services companies in the UAE experienced a significant cybersecurity breach in 2021, which exposed private financial information and prevented regular business operations. That served as an example of how accounting processes on digital platforms are becoming more and more vulnerable as the area increasingly experiences an accelerated digital revolution.

The area has embraced modern technologies like BI and ERP at a quick pace because to the ambitious Saudi

Vision 2030, UAE Smart Government Strategy, and Qatar National Vision 2030.[29] By guaranteeing increased operational efficiency, the spread of cutting-edge technologies has changed the character of accounting procedures toward more real-time analytics and insights-driven decision-making. However, it is also the source of significant cybersecurity concerns, including the possibility of ransomware, phishing attempts, and insider breaches, which jeopardize the confidentiality, integrity, and availability of financial information. In order to make digital accounting systems reliable and resilient, the region must address these vulnerabilities, which is a difficult task.[30]

Moreover, the socioeconomic and regulatory environment of the Gulf region complicates achieving appropriate level of cybersecurity, in particular due to differences in national cybersecurity policies, workforce diversity, and varying organizational readiness levels that leave the accounting processes environment vulnerable to intrusion of malevolent actors.[31] Digital accounting systems would be greatly protected if the region were harmonized into a kind of single, cohesive entity with technical safeguards, ethical accountability, and a regulatory oversight framework, which has not yet been achieved despite the widespread adoption of cybersecurity measures.[32] Moreover, the currently available discourse does not address breach disclosure or data protection regulations from an ethical standpoint. To increase the robustness and trustworthiness of digital accounting infrastructures throughout the regional area, these deficiencies must be filled.

Despite the advancements in the cybersecurity framework in the United Arab Emirates, Qatar, and Saudi Arabia, a number of enduring obstacles still need to be addressed before they can be fully implemented. These obstacles include financial limitations, skill shortages in the workforce, inconsistent regulations, and delays in the adoption of new technologies.[22] The adoption of cloud accounting by Saudi Arabian businesses is heavily influenced by technological, environmental, and regulatory considerations.[33] Despite the previously mentioned technology's potential to generate competitive advantage and operational and strategic advantages, cloud accounting implementation has not yet reached significant levels.

Financial obstacles continue to be a major issue for small and medium-sized businesses. The majority of Saudi Arabian SMEs' budgets cannot support ISO 27001 compliance, which hinders the adoption of security standards.[3] In fact, Mumford and Shires[34] pointed out that many aspects of Qatar's cybersecurity framework are still lacking as a result of the uneven funding of cybersecurity. However, as Al-Kumaim and Alshamsi[35] point out, a number of UAE government incentives have reduced the financial burden, which is why cybersecurity solutions are being widely adopted. Cloud accounting software is frequently updated to suit the most recent financial and tax rules in the UAE, such as VAT and other compliance criteria. This means that firms that use these systems can maintain compliance with minimal manual work, lowering the chance of errors and penalties.

Another development which is worth mentioning is the use of artificial intelligence (AI) within cloud-based accounting systems. AI-powered solutions improve operational accuracy and efficiency thanks to enhancing data analytics, automating repetitive activities, and enabling predictive forecasting. The strategic benefits of AI in accounting, such as enhanced fraud detection and compliance monitoring, are highlighted, in particular, in a publication by Brynjolfsson and McAfee.[36] According to their findings, if companies put in place appropriate governance and oversight procedures, AI-driven solutions can greatly improve the legitimacy and dependability of financial data.

Furthermore, AI's capacity for adaptation and learning from massive datasets makes it possible for accounting procedures to be continuously improved, eventually lowering a scale of human errors. As a result, integrating AI into cloud-based systems is turning into a key component of creating accounting frameworks that are more inventive and resilient.

Regarding the market development projections for cloud accounting systems, it is worth noting that the industry is expected to increase steadily over the next several years. The market is projected to reach $5.89 billion in 2024 and may reach the amount of $12,34 billion by 2030.[16]

There are a number of reasons for this quick rise. First of all, firms are looking for ways to guarantee data security and compliance due to stricter regulatory requirements and expanding comprehension and description of cyberthreats landscape. Second, since cloud-based technologies are accessible, flexible, and can automate repetitive and routine tasks, more companies are adopting them. Thirdly, the advancement of AI technology makes it possible to include it into cloud platform APIs. Consequently, it improves financial management's effectiveness and security. It is expected that the need for cloud accounting solutions will only increase in the upcoming years, influencing emerging financial technology trends.

The practical observance of regulatory requirements for cloud accounting systems seeks to assure data security and compliance with regulations in various jurisdictions. In particular, regulatory restrictions in the United States and Europe are critical to securing personal and financial information. In the United States, organizations such as the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) work together to enforce third-party risk management standards, including those intended for cloud providers' activities regulation.

With the help of the General Data Protection Regulation, the European Commission imposes stringent

rules on service providers such as Google Cloud. For businesses that operate internationally, the pertinent regulations represent an essential concern, since they guarantee security and improve the transparency of financial activities.

The particulars of each nation's laws and the range of platforms used dictate which regulatory bodies are chosen and what their needs are for each cloud system. The primary objective of the Cloud Security Alliance's (CSA) security standards, which serve as a reference for Amazon Web Services (AWS), is to guarantee risk management and transparency in the financial industry. Oracle Cloud is one example of how the Financial Conduct Authority (FCA) in the UK controls cloud providers by imposing standards on financial institutions' outsourced management.

Technology risk management regulations are enforced by the Monetary Authority of Singapore (MAS) and are applicable to Singaporean providers. The fundamentals of risk management and data security are universal, even though different nations have different regulatory frameworks.[37] As shown in table 3, this reflects a global trend toward standardizing cybersecurity and data protection guidelines for cloud systems.

Table 3. Peculiarities of cloud accounting systems regulatory requirements in the world

Solution	Regulatory agents	Purpose
Google Cloud	European Commission, General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)	Lays down specifications for safeguarding private information while processing and storing data in the cloud. The right to be forgotten, stringent criteria for transparency, and limitations on data transfers outside the EU are all in place.
Microsoft Azure	U.S. Federal Banking Agencies (FRB, OCC, FDIC), Joint TPRM Guidance	Banks must perform due diligence on cloud service providers and make sure they adhere to banking security regulations in accordance with the joint third-party risk management standards.
Oracle Cloud	Financial Conduct Authority (FCA, UK), FCA Handbook SYSC 8	Requirements for employing cloud providers and outsourcing risk management in the financial services industry. Business continuity and other aspects of contingent risk management are governed by the Resolution.
SAP Cloud	Monetary Authority of Singapore (MAS), Technology Risk Management Guidelines	Controlling the technological risks such as privacy, data security, and service continuity requirements that come with employing cloud services in the financial industry.

Between 2020 and 2024, there was a notable increase in cyberattacks against cloud accounting systems. As companies have shifted to cloud-based data management platforms in large numbers, the COVID-19 pandemic and the explosive expansion of remote work have led to an increase in cyber risks. Weak access control, improperly configured credentials, and inadequately protected APIs (application programming interfaces) are the main technological weaknesses of cloud-based systems. In 2021, around 100 million user records were compromised due to an improper security setup at Amazon Web Services. Using credentials that have been stolen or hacked is another serious risk, accounting for almost 30 % of all occurrences. The rise of new digital platforms presents another difficulty since they are frequently targeted because of their great value and lack of control. IBM claims that in 2023, the popularity of new decentralized technologies and inadequate user security measures led to a record number of cyberattacks on cloud services.[38]

Strong data encryption is the first step in any effective cybersecurity strategy for cloud accounting systems. Both data transmission (data-in-transit) and data storage (data-at-rest) require encryption. The risk of unauthorized access is greatly decreased by using TLS (Transport Layer Security) for data transmission and AES-256 encryption standards for data on cloud servers. A further line of defense against credential theft is added by implementing multi-factor authentication. Automated solutions for traffic anomaly detection are crucial for enhancing cybersecurity because they enable prompt response to possible threats and the identification of suspicious activities. Businesses can monitor and analyze events in real time to identify assaults thanks to innovative technologies like SIEM (Security Information and Event Management). The cybersecurity market's size is continuously evolving. The global market for cloud security was valued at USD 7,1 billion in 2019 and is expected to expand at a compound annual growth rate (CAGR) of 14,64 % between 2020 and 2027. Cloud security includes the strategies, rules, and execution controls necessary to secure and preserve data, infrastructure, and cloud-related compliance.[39] One should emphasize that the sector of financial services occupies one of the leading positions in this market, following IT and Telecom and surpassing even Government sector.

More stringent regulations and the introduction of new cybersecurity standards are linked to the development of cloud accounting systems in the upcoming five years. Europe will keep putting the GDPR's improved personal data protection measures into effect. The rule gives cloud providers additional guidelines for transmitting and

storing data. The Federal Reserve and the Office of the Comptroller of the Currency in the United States will keep enforcing stricter regulations for third-party risk management and confirming that cloud providers adhere to cybersecurity standards. In order to reduce technological risks associated with cloud systems, Singapore will strengthen regulations through the Monetary Authority of Singapore. Soon, businesses will likely invest in security by putting in place automated risk monitoring and forecasting systems. In cloud accounting systems, this strategy will emerge as the main cybersecurity development vector.

Importantly, cloud-based accounting software frequently offers sophisticated reporting features including drill-down functionality, configurable report formats, and predictive analytics in addition to traditional financial reports. By empowering customers to create informative reports customized to their unique business requirements, these capabilities facilitate strategic planning and well-informed decision-making.[40] Additionally, cloud-based accounting software systems frequently come with features like audit trails, compliance alerts, and automatic tax computations that are intended to make regulatory compliance easier. By assisting companies' adherence to current tax laws and accounting standards, these features lower the possibility of fines and legal issues.[41]

The outcomes of cloud accounting systems development prove their significance for corporate financial processes automation. Our research, in particular, supports assertions of Kmaleh[5] that cloud platforms' scalability is critical for multinational enterprises. Incorporating AI into cloud accounting systems improves data processing efficiency and enables better responsiveness to changes in the business environment, which is consistent with the findings of Abdo et al.[6] According to Avanija et al.[24] government regulations are crucial to guaranteeing the security of cloud systems. Moreover, according to Moron and Diokno's[42] analysis, government policies have an impact on how cloud platforms grow. Our research on the effects of regulators' activities, in particular in Gulf countries, is in line with this assertion. Also, Ukpong's[43] findings, which emphasize the significance of traffic monitoring in cloud systems to thwart cyberattacks, are likewise consistent with our study' results. The paper by Huxley and Brivot,[44] which highlights the necessity of international coordination to adequately govern the cybersecurity of cloud platforms, is also on point. According to Folami,[45] multi-factor authentication represents the best method for safeguarding credentials in cloud systems, and our findings support this claim. These results are also consistent with those of Shivarajappa,[4] who claims that cloud platforms dramatically increase productivity and lower infrastructure costs in big businesses. Thus, the adoption of cloud-based accounting systems in conjunction with strong cybersecurity measures is essential in preserving competitive advantages and high performance of any company.

The evaluation of cloud computing' impact on accounting field allow revealing useful insights regarding the dynamics of modern financial practices. Efficiency improvements, ensured by automation and collaborative tools, are redefining the landscape of traditional accounting procedures. Scalability represents a crucial element that helps companies adapt to changing workloads and navigate highly dynamic business environment. However, data security which is reinforced by encryption and improved protocols remains essential for safeguarding sensitive financial information. Meanwhile, the efficiency benefits of automation and real-time cooperation should be considered in line with the potential risks of cybersecurity vulnerabilities and data privacy threats. Although offering a competitive advantage, scalability still necessitates thorough cost analysis and infrastructure optimization. Firms can use strategic insights as a guide while navigating the cloud computing environment in the field of accounting: cloud technology must be adopted by businesses in strategic manner, and its deployment must be aligned with corporate objectives. Optimal efficiency gains can be achieved only when cloud solutions are customized to meet the specific needs of the business. The strategy for cloud integration should include effective risk mitigation tactics. This means implementing preemptive data protection measures, adhering to compliance rules, and comprehending evolving cybersecurity threats. Businesses may maintain their flexibility in a rapidly evolving digital landscape by continuous tracing emerging trends and technology. With this in mind, also, facilitating communication and collaboration among accounting experts and educating corporate teams on the subtleties of cloud computing promotes an adaptable organisational culture within the domain of accounting practices cybersecurity.

CONCLUSIONS

In the process of achieving the goal set identifying the current challenges experienced by corporate sector in cloud accounting systems operation – it was revealed that despite representing a huge array of benefits, cloud computing is still not commonly employed in accounting, which is explained by significant barriers, the most important of which are cybersecurity issues and the necessity of regulatory compliance. Moreover, for multinational corporations, the absence of standardization in global scope poses further difficulties. Given the rising frequency of cyberattacks globally, cloud system cybersecurity continues to be a critical concern. Multi-factor authentication, encryption technology, and threat detection monitoring systems are 'contributors' in preventing data breaches and other adverse consequences of cyber attacks. It seems necessary to continuously upgrade infrastructure and adjust it to emerging cyberthreats as cloud platforms expand. Effective cybersecurity

tactics can facilitate businesses in preserving high competitiveness level within the global marketplace. In the upcoming years, cybersecurity tactics should be the main focus of research, to guarantee the seamless, secure, and highly effective operation of businesses' financial systems.

REFERENCES

1. Stankovic MI, Golubitsky SG. Economic security through criminal policies: A comparative study of western and european approaches. Revista Cientifica General Jose Maria Cordova 2022;20(38):265–285. https://doi.org/10.21830/19006586.899

2. Yin FDesign and Implementation of Financial Accounting System Based on Cloud Computing Technology. In: Proceedings – 2023 Asia-Europe Conference on Electronics, Data Processing and Informatics, ACEDPI 2023. (pp. 58–62). Institute of Electrical and Electronics Engineers Inc., 2023. https://doi.org/10.1109/ACEDPI58926.2023.00018

3. Al-Dosari K, Fetais N, Kucukvar M. Artificial Intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. Cybernetics and Systems 2024;55(2):302–330. https://doi.org/10.1080/01969722.2022.2112539

4. Shivarajappa M. The impact of cloud computing on financial accounting – evaluating the impact of cloud computing on accounting firms. ShodhKosh Journal of Visual and Performing Arts 2024;5(3):992–998. https://doi.org/10.29121/shodhkosh.v5.i3.2024.3566

5. Kmaleh A. The impact of using the cloud computing upon the quality of accounting information and its reflection upon the development of the world standards of financial reports in Jordanian corporations. International Journal of Professional Business Review 2023;8(9):1–24. https://doi.org/10.26668/businessreview/2023.v8i9.3771

6. Abdo H, Owusu FB, Mangena M. Accounting practices and regulations for extractive industries: A framework for harmonisation. Journal of Financial Reporting and Accounting 2024;22(1):147–180. https://doi.org/10.1108/JFRA-07-2023-0425

7. Kawar M, Daviglus M. Federal Reserve Policies and Their Role in Advancing Cloud Computing for Technology Startups, 2024. https://doi.org/10.13140/RG.2.2.14273.06247

8. Musyaffi AM, Oli MC, Afriadi B. Drivers of Student Technology Readiness in Using Cloud Accounting to Improve Student Performance. International Journal of Information and Education Technology 2023;13(8):1169–1176. https://doi.org/10.18178/ijiet.2023.13.8.1918

9. Fahmi M, Muda I, Kesuma SA. Digitisation Technologies and Contributions to Companies towards Accounting and Auditing Practices. International Journal of Social Service and Research 2023;3(3):639–643. https://doi.org/10.46799/ijssr.v3i3.298

10. Malusare L. A study of the impact of cloud-based accounting on maintenance of Accounting Records. International Journal of Scientific Research in Engineering and Management 2024;9(4):41–45. https://doi.org/10.55041/IJSREM33357

11. Levytska S, Pershko L, Akimova L, Akimov O, Havrilenko K, Kucherovskii O. A risk-oriented approach in the system of internal audit of the subjects of financial monitoring. International Journal of Applied Economics, Finance and Accounting 2022;14(2):194–206. https://doi.org/10.33094/ijaefa.v14i2.715

12. King S, Agra R, Zolyomi A, Keith H, Nicholson E, de Lamo X, ... Brown C. Using the system of environmental-economic accounting ecosystem accounting for policy: A case study on forest ecosystems. Environmental Science and Policy 2024;152:103653. https://doi.org/10.1016/j.envsci.2023.103653

13. Pradesa E, Syahrani T, Sakti RE. Transformasi Digital Adopsi Software as a Service Layanan Cloud Accounting oleh UMKM. BUDGETING: Journal of Business, Management and Accounting 2023;5(1):155–169. https://doi.org/10.31539/budgeting.v5i1.7049

14. Thaher M. 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

15. Liu Y. Enterprise Comprehensive Budget Informatisation Management Based on Cloud Accounting and Blockchain Technology. International Journal on Recent and Innovation Trends in Computing and Communication 2023;11(10):2489–2498. https://doi.org/10.17762/ijritcc.v11i10.9253

16. Dhapte A. Cloud Accounting Software Market Overview. Market Research Future. [Internet]. 2025 [cited 28 May 2025]; Available in: https://www.marketresearchfuture.com/reports/cloud-accounting-software-market-28846

17. Spherical Insights. Global Cloud Accounting Technology Market Insights Forecasts to 2033. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.sphericalinsights.com/reports/cloud-accounting-technology-market

18. Laili NH, Khairi KF, Masruki R. An analysis of the use of accounting system on-cloud: A case study in Abbaz Advisory. International Journal of Islamic Economics and Finance Research 2022;5:13–23.

19. Raza H. Cloud Accounting in 2024: Pros and Cons. Expertise Accelerated. [Internet]. 2024, April 30 [cited 28 May 2025]; https://expertiseaccelerated.com/cloud-accounting-pros-and-cons/

20. Kumar R, Kaur J. Analysis of Cloud Computing Security Challenges and Threats for Resolving Data Breach Issues. In: 2023 International Conference on Computer Communication and Informatics (ICCCI). (pp. 1–6). Coimbatore, India, 2023. https://doi.org/10.1109/ICCCI56745.2023.10128329.

21. Syah D, Muda I, Lumbanraja P, Kholis A. The Role of Cloud Computing on Accounting Information System Quality: A Study in Hotel Industry. TEM Journal 2023;12(3):1890–1901. https://doi.org/10.18421/TEM123-72

22. Morshed A, Khrais LT. Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. Journal of Risk and Financial Management 2025;18(1):41. https://doi.org/10.3390/jrfm18010041

23. Khanom M. Cloud accounting: A theoretical overview. IOSR Journal of Business and Management 2017;19(06):31–38. https://doi.org/10.9790/487X-1906053138

24. Avanija J, Goundar S, Konduru R. Convergence of cybersecurity and cloud computing. Engineering Science Reference, 2024. https://doi.org/10.4018/979-8-3693-6859-6

25. Kesa DM. Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. World Journal of Advanced Research and Reviews 2023;18(3):970–992. https://doi.org/10.30574/wjarr.2023.18.3.1166

26. Isibor E. Regulation of healthcare data security: Legal obligations in a digital age. SSRN, 2024. https://doi.org/10.2139/ssrn.4957244

27. Bhadouria AS. Study of: impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. International Journal of Scientific and Research Publications 2022;10(10):1–11.

28. Sanusi I, Sanusi A, Shamwill A, Yinisa S, Iliyasu R. Evaluation of cloud based computing in security accounting information system. World Journal of Advanced Research and Reviews 2025;25(03):1073–1086. https://doi.org/10.30574/wjarr.2025.25.3.0734

29. Arif M, Aldosary AS. Urban spatial strategies of the Gulf Cooperation Council: A comparative analysis and lessons learned. Sustainability 2023;15(18):13344. https://doi.org/10.3390/su151813344

30. Martins A, Bianchi de Aguiar MT, Sambento M, Branco MC. Business intelligence system adoption and the leveraging of reporting process capabilities. Journal of Accounting Organizational Change, 2024. https://doi.org/10.1108/JAOC-11-2023-0204

31. Morshed A. Evaluating the influence of advanced analytics on client management systems in UAE telecom firms. Innovative Marketing 2024;20(4):41–51. https://doi.org/10.21511/im.20(4).2024.04

32. Zhang X, Liu Y, Yu S, Lin O, Meng L. Impact of environmental protection tax on enterprise digital transformation: Evidence from Chinese listed firms. International Review of Economics Finance 2025;97:103743. https://doi.org/10.1016/j.iref.2024.103743

33. Mujalli A, Wani M, Almgrashi A, Khormi T, Qahtani M. Investigating the factors affecting the adoption of cloud accounting in Saudi Arabia's small and medium-sized enterprises (SMEs). Journal of Open Innovation: Technology, Market, and Complexity 2024;10(2):100314. https://doi.org/10.1016/j.joitmc.2024.100314

34. Mumford D, Shires J. Toward a decolonial cybersecurity: Interrogating the racial-epistemic hierarchies that constitute cybersecurity expertise. Security Studies 2023;32(4–5):622–652. https://doi.org/10.1080/09636412.2023.2230879

35. Al-Kumaim NH, Alshamsi SK. Determinants of cyberattack prevention in UAE financial organizations: Assessing the mediating role of cybersecurity leadership. Applied Sciences 2023;13(10):5839. https://doi.org/10.3390/app13105839

36. Brynjolfsson E, McAfee A. The business of AI: Applications and implications for accounting. Harvaed Business Review 2017. https://hbr.org/2017/07/the-business-of-artificial-intelligence

37. Oliinyk OS, Shestopalov RM, Zarosylo VO, Stankovic MI, Golubitsky SG. Economic security through criminal policies: A comparative study of Western and European approaches. Revista Cientifica General Jose Maria Cordova 2022;20(38):265–285. https://doi.org/10.21830/19006586.899

38. IBM. IBM X-Force Threat Intelligence Index 2024. [Internet]. 2024 [cited 28 May 2025]; Available in: https://www.ibm.com/reports/threat-intelligence

39. Million Insights. Cloud Security Market Analysis Report by Application, by Company Size, by Solution, by Deployment and Segment Forecasts From 2020 to 2027. [Internet]. 2020 [cited 28 May 2025]; Available in: https://www.millioninsights.com/industry-reports/global-cloud-security-market

40. Meng L. The Promotion Effect of the Improved ISCA Model on the Application of Accounting Informatization in Small-and Medium-Sized Enterprises in the Cloud Computing Environment. Mobile Information Systems 2022;2:1–13. https://doi.org/10.1155/2022/4228178

41. Agrawal S, Jethy J. An Analysis of Cloud-Based Accounting Software: A Literature Review on Features, Performance, and User Satisfaction. International Journal for Multidisciplinary Research 2024;6(2):1–12. https://doi.org/10.36948/ijfmr.2024.v06i02.15692

42. Moron CE, Diokno COB. Level of Readiness and Adoption on the Use of Artificial Intelligence Technologies in the Accounting Profession. Open Journal of Accounting 2023;12(03):37–54. https://doi.org/10.4236/ojacct.2023.123004

43. Ukpong EG. Scholastic Analysis of the Impact of Digital Technologies on the Accountancy Profession in Nigeria. European Journal of Accounting, Auditing and Finance Research 2023;11(6):41–69. https://doi.org/10.37745/ejaafr.2013/vol11n64169

44. Huxley Z, Brivot M. On professional destabilisation and accounting self-regulation. British Accounting Review 2024;57(3):101358. https://doi.org/10.1016/j.bar.2024.101358

45. Folami R. Cloud-Based Accounting and Cybersecurity: Safeguarding Financial Data. ICAN Abeokuta and District Society, 2024. https://doi.org/10.13140/RG.2.2.32813.19685

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Olena Lagovska.
Data curation: Olesia Demianyshyna.
Formal analysis: Olesia Demianyshyna, Zoriana Myronchuk.
Research: Olesia Demianyshyna.
Methodology: Iryna Shchyrba.
Project management: Zoriana Myronchuk.
Resources: Zoriana Myronchuk, Edina Shebeshten.
Software: Olesia Demianyshyna.
Supervision: Edina Shebeshten.
Validation: Edina Shebeshten.
Display: Edina Shebeshten.
Drafting - original draft: Iryna Shchyrba, Olena Lagovska.
Writing - proofreading and editing: Iryna Shchyrba, Olena Lagovska.