International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 14 Issue 2, February, 2025

Cloud Computing and the Protection of Financial and Accounting Information

Ali Mohammed Almohsen[1], Mohammed Abdulrahman Almubireek[2], Omar Ahmad Aldhuawyhi[3], Ibrahim BakeAlbak[4], Mohammed Ahmed Al Rebh[5]

[1]Accounting trainer, at TVTC Dammam College of Technology Saudi Arabia
[2]Accounting trainer, at TVTC Hafer Albatin College of Technology Saudi Arabia
[3]Accounting trainer, at TVTC Hafer Albatin College of Technology Saudi Arabia
[4]Accounting trainer, at TVTC Hafer Albatin College of Technology Saudi Arabia
[5]Accounting trainer, at TVTC Al QatifCollege of Technology Saudi Arabia

Work at Technical and Vocational Training Corporation, Saudi Arabia

INTRODUCTION

Cloud computing has been among the most revolutionary technologies of the contemporary era. Cloud computing has transformed the way businesses store, process, and secure data. Cloud computing refers to the provision of computer services, such as servers, storage space, databases, programs, and analytics, over the internet rather than through an office environment (McKinsey & Company, 2022). Revolutionization began early in the 2000s, when advances in virtualization and networking enabled the development of scale on-demand computing. Cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud are the foundation for most business activities, including finance- and accounting-related activities (Opiyo, 2025). In the modern world, an increasing number of accounting and financial institutions are employing cloud solutions to simplify their activities, ease access to corporate information, as well as give them the capability to make instant decisions. The motive for doing so lies in the fact that there is an increasing demand for safe, flexible, and inexpensive technology that is capable of processing huge volumes of delicate financial information. Cloud computing assists businesses in saving money on in-office infrastructure through streamlined reporting, automated repeat activities, as well as simplified cooperation among individuals across borders.Adoption has also turned out to be an intelligent business strategy and an imperative for gathering and processing financial and accounting data in an increasingly digital world market.

From “Financial Institutions are shifting their workload to the cloud in 2024” by McKinsey, 2024

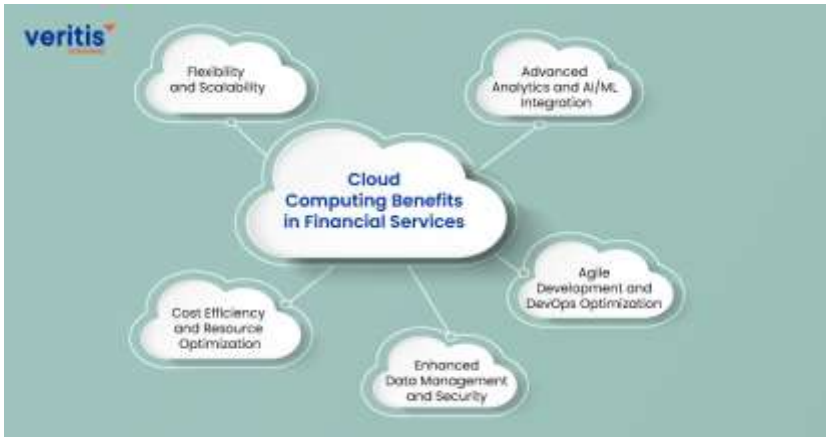
Cloud computing has become a strategic idea rather than an operational decision-making tool because of the growing importance of information technologies. In the past, financial information was stored in separate systems that were costly to manage, difficult to scale, and prone to hardware failures. Businesses may securely access their information from a central location, pay less for infrastructure, and get financial reports quickly with them. It is most

useful on days when real-time market information about finances is available and clients want to be able to get the right information right away. Cloud computing also makes it possible for businesses to work together across borders, giving them easier access to financial papers that can be easily updated in multiple places. This sets the stage for more efficiency and higher levels of transparency.

Benefits of Cloud Computing for Financial and Accounting Information

One of the best things about cloud computing for accounting and financial systems is that it can help you save money by being able to grow. Businesses would have to spend a lot of money on server infrastructure, data warehouses, and maintenance staff if they used traditional accounting systems. This would be a huge burden on their finances and operations. With cloud solutions, organizations only pay for the assets they utilize, which is like a pay-as-you-go service. Firms that have implemented the use of cloud systems are able to carry out modification of their computer power such that they can alter the speed of their operation depending with the need (Pollard, 2024). For instance, during the peak times, such as the time when firms need to conduct filing or when they are carrying out audits, they can alter with the power for the system to work at high speed and handle more work at a time. Then, when business slows down again, they might lower assets or downsize to reduce costs but remain productive. This type of flexibility allows cloud computing to be an optimal option for businesses that would prefer to use their assets to the best extent yet also not risk committing to the high capital outlay over the long term.

Cloud finance also bring the advantage of its capacity of accessing, collaborating and automation in real time. Accountants who use cloud systems in their firms have the benefit of working from anywhere in the world provided that their gadgets are internet enables and are featured with the appropriate security barriers. With this, accountants and other financial specialists will be more productive since they can access and share most recent financial data from anywhere in the world. Firms that use automated systems usually ease the burden of carrying out some of the repetitive accounting activities carried out by financial officers such as preparation of data, verification of accounts and preparation of reports. Real-time reporting feature goes one step further by facilitating the executives to see the cash flow and the financial performance at all times, not only at the close of the period.



From “5 Key Benefits of Cloud Financial Services for Your Business” by Veritis Group 2025

Risks and Challenges in Protecting Financial and Accounting Data

Despite the many benefits that are associated with the use of the cloud for finance and accounting, it also comes with a lot risks. Some of the most serious risks that are associated with cloud finance include cybersecurity, compliance and regulation, and how to keep data safe, private, and usable. If firms fail to take proper security measures for handling data, it can lead to clients losing their money or harming the reputation of both the firm and the clients. Today, many firms have implemented the use of cloud technology for the storage and management of financial and accounting data. Knowing about these dangers and taking steps to reduce them will help make financial systems more stable and trustworthy.

The most important problem is arguably that cybersecurity issues like data breaches, ransomware attacks, and phishing scams are becoming more common in cloud banking systems. When hackers get into financial data without permission, they usually leak important information like customer data, transaction data, or audit trails (Kafi

& Akter, 2023). Top-most attacked business segments for cyberattacks often include the financial services sector due to the fact that their data is very marketable on the black market. Such attacks can destroy customer trust, especially when they pilfer individual financial information. They are more than an encroachment on the right to privacy. Ransomware is also an enormous concern. Hackers encrypt crucial accounting information after which they will ask for money to decrypt (Baker, 2025). For example, when ransomware has shut down multinationals or access to their accounting data, they have lost millions. phishing attacks disguised as bad mails or messages to steal employees' logins remain the most common modes for cyber attackers to gain access to cloud platforms. Money handlers are the most vulnerable targets as they tend to possess access to secret information. In conclusion, all these vulnerabilities exposit how vulnerable financial and accounting information are on cloud platforms with the lack of the relevant cybersecurity mechanisms.

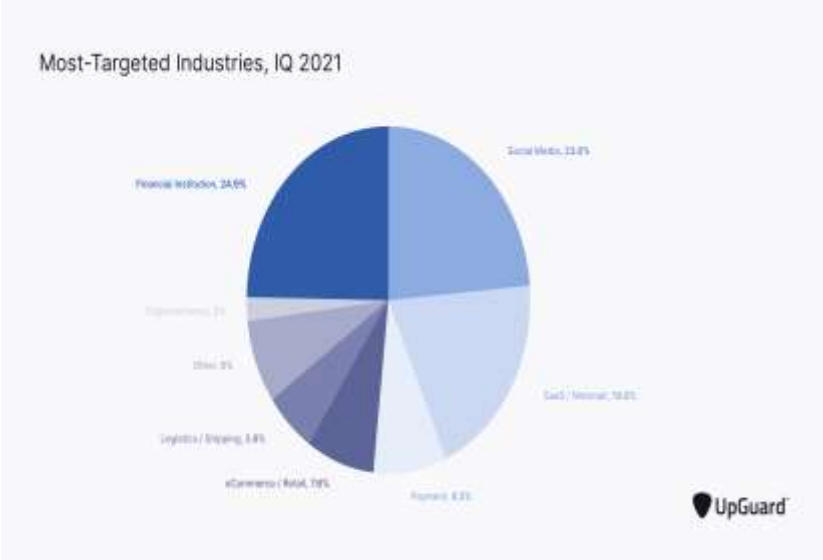
In addition to external risks, regulations and compliance are an issue with the example of cloud computing. There are tight regulations on finances so all are responsible, transparent, and protect the interests of stakeholders. Europe's General Data Protection Regulation (GDPR) is an example of data protection law with stringent requirements on personal and finance data, for instance, obtaining permission, limiting data, and informing people when data breaches are occurring. In the United States, the Sarbanes-Oxley Act (SOX) says businesses must have sound reporting and controls inside the business in order to stop fraud. International Financial Reporting Standards (IFRS) set out how financial statements for businesses operating in more than one country are to be constructed. When finances are kept in the cloud, it becomes very hard to follow regulations when the servers are in different locations with different regulations. For instance, the server located in a different country may have its regulations on data stored on it different from the company owning the data's regulations, even though the company is from somewhere else. It makes the situation legally unclear and perilous for financial businesses. Regulators also want it to be easy to view and check the finances, but this isn't always possible when corporations utilize third-party cloud providers for their infrastructure. It is challenging for accountants and financial managers to make sure that these kinds of suppliers follow the regulations and give them the paperwork they need for audits.

Another problem is how to make data safe, private, and easy to get to. These are also known as the three legs or information protection columns. Information integrity means that the financial records are correct and can be trusted. It will always be hard to say for sure that system errors won't harm data saved in the cloud, whether they are intentional or accidental. For example, if someone changes accounting data without permission or alerting anybody, it could make people think that an organization's finances are better or worse than they really are, which could mislead investors or authorities. And privacy is even worse because the financial data can include business plans, salary details, and other taxable information. If someone or a group looks at this information without permission, it could give competitors an edge in the market or put the company at risk for fraud. To keep things secret, access controls and encryption are very important. However, they need to be updated and kept up to date in order to work. Finally, availability, the last but not the least, is with regard to maintaining financial and accounting data for access whenever required. Cloud systems, though typically stable, are vulnerable to system faults, natural catastrophes that destroy data centers, or denial-of-service attacks on data centers that need not penetrate the data but impact data centers. Even for a momentary availability fault, financial operations will suffer greatly, especially for activities that are timely such as payroll processing, taxable filing, or year-end closing deadlines.

Another issue with the cloud computing shared responsibility model is that most business finance enterprises fail to understand this type of segregation of duty. This is due to the assumption that the service providers will attend to all the issues of security. Such misconceptions will create large gaps in coverage for things such as identification for the users, encryption for the data, and insider dangers. For instance, even with the presence of the service for the protection of the network and the physical servers, a poor password policy in an accounting section will still allow individuals who shouldn't access the sensitive files. Therefore, there is a need to inform the employees on the issue of security in the cloud and assign them specific tasks to perform.

In addition, risk due to inside threat can never be overlooked. Employees or contractors who have rightful access to financial systems can either unknowingly or knowingly ignore data security. In accounting positions, for example, personnel can often only access sensitive audit trails and ledgers, and thus inside threats can turn out to be highly destructive. For example, an employee may alter records for personal gain or leak information to the outside world. Or, irresponsible activities such as opening sites on clouds using unsecured networks may potentially leak financial information unknowingly. To avoid inside threat, rightful access controls, monitoring software, as well as regular sessions for training on best cybersecurity practices are all needed.

The problems talked about are further complicated by fast growth of cyber-attacks. Attackers are constantly creating new and better ways of cracking vulnerabilities in cloud infrastructure, and banks and other financial companies must therefore constantly improve and upgrade their protection. Financial and operational strain is caused because companies are compelled to spend large amounts on security product procurements, staff training, and compliance audits. Even smaller companies can't afford to match these demands and are therefore further exposed to attack. With greater use of the cloud, its attack surface also gets larger, and therefore threats involving financial and accounting implications for securing info will further increase.



From “The 6 Biggest Cyber Threats for Financial Services in 2025” by Kost, 2025

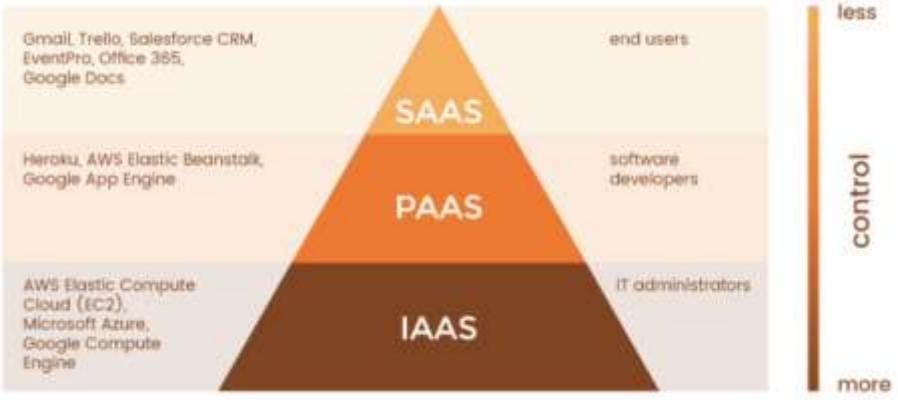
Security Mechanisms and Best Practices for Protection

Encryption, access controls, and authentication limits are some of the best means to protect financial and accounting data in the cloud. Encryption provides assurance that secret financial information cannot be read by individuals who shouldn't read it when the data is kept in the cloud and when it travels over networks. Sophisticated encryption techniques like AES-256 are almost always available on the leading cloud services. These stop data from becoming stolen or tampered with. Access controls are also an additional barrier that limits who has the ability to read or change particular files (Krishnakumar, 2025). Accountants, for example, might see ledgers, but just senior auditors might approve final reports. Good authentication, like multi-factor authentication (MFA), is needed to back that. MFA forces individuals to authenticate who they are by doing something besides entering the passkey once. These additional barriers make it considerably more difficult for individuals who shouldn’t gain access to the data to access the data, for misuses by insiders to happen, and for passwords to get stolen, all all-too-common problems with cloud-based systems.

Cloud service providers (CSPs) are not less responsible for securing data than other enterprises. Amazon Web Services, Microsoft Azure, and Google Cloud are some of the world's largest businesses responsible for securing the hardware that underlies cloud services. This includes physical servers, data centers, and network equipment. They often adhere to world standards such as ISO 27001 and SOC 2, which establish extremely high standards for protecting information. CSPs also offer native security features such as firewalls, intrusion detection systems, and security monitoring tools (Long, 2021). Such technologies enable businesses to enhance their defenses. However, in the shared responsibility model, clients are still accountable for securing their apps, their data, and user access. This means that banks and other financial businesses must thoroughly verify suppliers to ensure that they adhere to industry regulations and negotiate service-level agreements (SLAs) that specify explicitly whom is accountable for securing data.

Keeping backup and disaster recovery plans up to date is another important best practice for keeping financial and accounting data safe from loss or disruption. Most cloud service providers offer automated backup services that copy data to various locations, which lowers the chance of losing data that can't be recovered from hardware

failures, cyberattacks, or natural disasters. In banks, this would mean that important information like transaction reports, payroll, and audit trails may be promptly restored if the system fails. Disaster plans go a step further by listing steps to do to keep a business running during major disruptions. Such strategies involve replicating financial systems to secondary data centers in real-time and practicing on a routine basis how to bring systems back online. If these strategies are not put in place, businesses will lose considerable amounts of money, pay government fines, and spend quite a bit of time down in the event that data becomes unavailable.



From “SaaS vs. IaaS vs. PaaS: Understanding the Differences” by ncube, 2025

There are numerous real-world cases for safe deployments for the financial sector on the cloud that support the validity of the strategies. JPMorgan Chase, for example, has utilized cloud solutions with stronger encryption and monitoring algorithms with the help of artificial intelligence to detect anomalous money flow trends but yet not violate international standards. Deloitte has utilized safe clouds that enable its global accounting team to interact freely. Those clouds have multi-factor authentication mechanisms as well as automated compliance tools, which is also favorable. Small accounting firms have also made money by employing software like QuickBooks Online and Xero, which use safe login methods and online backups all the time to protect customer data. These are examples that show that the cloud could be a safe place to store accounting and financial data if there are ways to encrypt, authenticate, protect service providers, and retrieve data.

New technologies that offer better protection against a wider range of cyber threats are paving the way for the future of keeping accounting and financial information safe on the cloud. Blockchain is probably the most obvious example. It has tamper-proof distributed ledgers that promise to make financial information not just easier to get to but also more reliable.Blockchain makes it nearly impossible for malicious users to alter accounting files without their detection since all the alterations are inscribed across numerous computers. Similarly, an AI-powered protection solution is also altering how financially sophisticated institutions are at recognizing and defending their information. AI can quickly examine millions of online activity records, spotting unusual behavior and taking automatic steps to fix it when it looks like it might be abuse. Compared to how long it would take to do these things with traditional ways, this cuts down on the time it takes to act on them by a huge amount. Also, most banks and other financial institutions use zero-trust security right now. It presupposes that no user, device, or network is completely trustworthy and that all access needs to be authenticated all the time. With increasingly sophisticated cloud infrastructures and cyber-attacks, these types of solutions will likely assume key roles in safeguarding accounting and financial networks.

In order to obtain optimal benefit from these advances, the following suggestions for financial institutions and accountants are possible. Firstly, companies need to invest in recurring training for finance and accounting personnel so that such personnel remain up-to-date with increasing threats to security and compliance needs (Tolossa, 2023). Human mistake is one of the single-largest weaknesses, and keeping staff up-to-date with the latest information makes it less probable that such staff may be phished or that they will misuse their access. Secondly, financial institutions need to implement a multi-layered system for security combining the best technologies for encryption, multi-factor access, intrusion detection, and real-time monitoring. Implementing an in-depth defense measure such as this places barriers in place such that even when one such barrier can be breached, others still exist between

potential hackers and confidential financial data. Thirdly, working arrangements with reputable known-quality providers for cloud services are needed. Institutions need to choose carefully providers' certification, compliance needs, and offering for security before placing confidential financial data in such hands. Fourthly, accountants and financial managers need to fulfill their role in the making of the IT security policies for their companies such that these financial reporting, audit, and compliance needs are taken into consideration by such companies in their overall strategies for the security of an IT.

With the movement towards information technology for the banking industry and other institutions dealing with finances, it is also crucial to think about how to make sure that new ideas will not put information at risk. Even though technologies like blockchain, artificial intelligence, and automation will hopefully make the world quicker and help with the power to make strategic decisions in the future, they will also potentially put things at risk, so they must be used carefully (Porfírio et al., 2024). With the potential for artificial intelligence to identify fraud, this will also potentially give hackers the power to spread misinformation by using algorithms. Blockchain cannot be hacked in theory, but it does have issues with scale power and regulation that need to be fixed before it can become bigger. Institutions will then need to be careful and think ahead when trying out new technologies on a small scale, but they will also need to be strict with regulatory drives and regularly review their risk management processes. If this happens, the banking industry and accounting firms will come up with new ideas, but they will still need to keep the trust, honesty, and safety that are necessary for managing financial data.

From "Finance Cloud Market Size and Growth 2025 to 2034" by Zoting & Shivarkar, 2025.

REFERENCES

[1] Baker, K. (2025). *What is a ransomware attack?* CrowdStrike: We Stop Breaches with AI-native Cybersecurity. https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/

[2] Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15-26. https://doi.org/10.18034/ajtp.v10i1.659

[3] Kost, E. (2025,). *The 6 biggest cyber threats for financial services in 2023*. Third-Party Risk and Attack Surface Management Software | UpGuard. https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

[4] Krishnakumar, V. (2025). *The importance of data encryption in cloud environments*. CloudOptimo. https://www.cloudoptimo.com/blog/the-importance-of-data-encryption-in-cloud-environments/

[5] Long, K. S. (2021). *Cybersecurity Network Monitoring Challenge in Commercial Service Provider Clouds*. MITRE. https://apps.dtic.mil/sti/trecms/pdf/AD1133628.pdf

[6] McKinsey & Company. (2022). *What is cloud computing?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cloud-computing

[7] McKinsey. (2024). *Financial Institutions are shifting their workload to the cloud in 2024*. Human Verification. https://fintech.global/2024/03/09/financial-institutions-are-shifting-their-workload-to-the-cloud-in-2024/
[8] Ncube. (2025). *SaaS vs. IaaS vs. PaaS: Understanding the differences - nCube*. nCube - . https://ncube.com/saas-paas-iaas
[9] Opiyo, B. (2025). *Cloud providers: AWS, Azure, GCP – Dataquest*. Dataquest. https://www.dataquest.io/blog/cloud-providers-aws-azure-gcp/
[10] Pollard, B. (2024). *The Benefits of Cloud Computing in Financial Services*. Adivi. https://adivi.com/blog/benefits-of-cloud-computing-in-financial-services/
[11] Porfírio, J. A., Felício, J. A., & Carrilho, T. (2024). Factors affecting digital transformation in banking. *Journal of Business Research*, *171*, 114393. https://doi.org/10.1016/j.jbusres.2023.114393
[12] Tolossa, D. (2023). Importance of cybersecurity awareness training for employees in business. *VIDYA - A Journal of Gujarat University*, *2*(2), 104-107. https://doi.org/10.47413/vidya.v2i2.206
[13] Veritis Group. (2025). *5 key benefits of cloud financial services for your business*. Veritis Group Inc. https://www.veritis.com/blog/5-key-benefits-of-implementing-cloud-financial-services-for-your-business/
[14] Zoting, S., & Shivarkar. (2025). *Finance cloud market size to surpass USD 217.30 billion by 2034*. Precedence Research - Advisory, Research & Reports. https://www.precedenceresearch.com/finance-cloud-market