EJTAS ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

Potential Risks of Cloud Computing in Financial Institutions in Tanzania: Perspectives from CRDB Bank Plc

Amina Abdul
Department of Informatics, Institute of Accountancy Arusha, PO BOX 2798, Arusha Tanzania

Dr Maria Lauda Joel Goyayi
Center for Applied Data Science, University of Johannesburg, Johannesburg, South Africa

Suggested Citation

Abdul, A. & Goyayi, M.L.J. (2023). Potential Risks of Cloud Computing in Financial Institutions in Tanzania: Perspectives from CRDB Bank Plc. *European Journal of Theoretical and Applied Sciences, 1*(6), 43-53. DOI: 10.59324/ejtas.2023.1(6).05

Abstract:

The adoption of cloud computing introduces a range of potential risks that financial institutions must navigate with prudence. Cloud service providers are entrusted with valuable customer information, and any compromise could have severe consequences, including financial losses and reputational damage. The main objective of this research was to assess the potential risks of cloud computing in financial institutions in Tanzania. This is done in the context of CRDB bank. The research employed a mixed methods approach, incorporating both quantitative and qualitative data collection methods. The data was acquired through questionnaires, specifically targeting the employee population of CRB bank. The data underwent quantitative analysis. The research sampled population is 201 respondents from ICT, legal and procurement departments at the financial institution. Cloud computing poses hazards that financial organizations must carefully manage. Security of sensitive financial data comes first. Any compromise of cloud service providers' client data could result in financial losses and reputational damage. Data privacy risks occur as legislative contexts change. Cross-border cloud services can challenge data sovereignty and local legislation. Another crucial factor is operational continuity. Financial institutions depend on uninterrupted service, putting them exposed to cloud service provider outages and technical issues. Maintaining financial services and client satisfaction are crucial. The regulatory compliance challenge is unique. Cloud computing requires vigilance in local and international legal systems. To retain financial ecosystem confidence, financial institutions must ensure their cloud-based solutions meet industry standards and laws. The study stressed the importance of a holistic strategy to cloud computing in financial institutions like CRDB Bank PLC. Cloud technology has many benefits, but stakeholders must be cautious and implement risk management and mitigation strategies. The conclusions of this study can help CRDB Bank PLC and other Tanzanian financial institutions make educated cloud technology implementation decisions. These decisions must prioritize financial system security, privacy, and resilience. The results also highlight the need for financial industry-regulatory cooperation to keep the regulatory framework up to date with technology.

Keywords: *cloud computing, risks, financial institution, smart contracts, and cloud service providers.*

Introduction

Cloud computing has become a revolutionary technology that presents a multitude of advantages to firms operating in several sectors. The adoption of cloud computing in the worldwide financial industry has experienced a notable increase, mostly driven by its capacity to enhance operational efficiency, elevate consumer experiences, and facilitate accelerated

innovation. Brwon (2022) noted that financial institutions, such as banks, are progressively contemplating the implementation of cloud computing to augment operational efficiency, scalability, and cost-effectiveness. Macha and Massawe (2023) noted that the expeditious progression of cloud computing technology presents financial institutions in Tanzania with the potential for enhanced operational efficiency, cost-effectiveness, and technical innovation. However, in addition to these advantages, cloud computing presents a range of obstacles and hazards that financial institutions must thoroughly evaluate.

In Tanzania, there has been an increasing inclination within the financial sector to embrace cloud computing technologies as a means of modernizing processes and providing improved client experiences (Pazarbasioglu et al., 2020; Mpofu and Mhlanga, 2022). Although cloud computing has indisputable benefits, the migration from conventional on-premises systems to cloud-based infrastructure entails a variety of uncertainties and hazards. The cloud computing industry in developing nations has garnered significant interest from both global and local information technology companies, as well as from national governments and international organizations. As an illustration, IBM has created cloud computing facilities in many countries such as China, India, Vietnam, Brazil, and South Korea. According to REF, several prominent global cloud providers, including Microsoft, VMware, Salesforce, Dell, and Parallels, are actively seeking prospects in emerging markets. It is noteworthy that certain Tanzanian financial institutions have embraced the utilization of cloud computing, which is a significant development. It might be argued that the poor world, particularly Tanzania, has not received such a significant amount of attention in any previous key technological advancements. Despite the existence of a growing body of literature that examines the dangers associated with cloud computing on a worldwide scale, there is limited research exploring the unique risks and challenges that pertains to financial institutions, such as CRDB Bank PLC, thus offering a context of Tanzania. Consequently, considering the financial industry's shift towards technological advancement in Tanzania, it is imperative to comprehend the potential hazards that may arise from the implementation of cloud computing, particularly within the framework of institutions such as CRDB Bank PLC (Philemon, 2020; Tesha, 2022).

The research holds importance due to its investigation into the potential hazards associated with the implementation of cloud computing, particularly within the financial industry of Tanzania using CRDB Bank PLC as a research case. The adoption of cloud-based services raises apprehensions pertaining to the security and privacy of data, adherence to legal requirements, and the ability to maintain operational continuity.

Literature Review

Theoretical Framework

The study adopted the Technology Adoption Model (TAM) by Fred Davis introduced in 1989, which has been widely applied and expanded in the information systems and technology (Wahab, Rose, Uli, & Abdullah, 2009). TAM explains the adoption of new technology by individuals or organizations. TAM is significant to the study on analyzing cloud computing risks in the Tanzanian financial institutions. According to Wahab et al., (2009), One fundamental element within the framework of the Technology Acceptance Model (TAM) is the concept of "perceived ease of use." This element holds considerable significance when assessing the potential risks associated with adopting cloud computing. If employees perceive cloud technology as challenging to utilize, it can elevate the likelihood of errors and security vulnerabilities. Similarly, the component of "perceived usefulness" in TAM is pivotal for evaluating the merits and demerits of implementing cloud computing. It is crucial to gauge employees' perceptions regarding the advantages and drawbacks linked to cloud technology to facilitate well-informed decision-making processes. Furthermore, TAM can be extended to encompass elements related to risk

perception (Acharya and Mekker, 2022), encompassing the evaluation of employees' apprehensions concerning data security, compliance, data sovereignty, and potential financial consequences in the context of cloud computing.

Empirical review

The advent of cloud computing has brought about a significant transformation in the operational practises of enterprises, providing them with enhanced scalability, cost-effectiveness, and flexibility. Financial institutions, specifically, have adopted this technology as a means to maintain competitiveness within a swiftly moving market. Nevertheless, despite the myriad advantages presented by cloud computing, it also presents inherent risks and obstacles. Scott et al. (2019) conducted a study which identified security as a prominent problem in the adoption of cloud computing inside financial institutions. Data breaches pose a substantial danger due to the communal nature of cloud systems and the extensive presence of sensitive financial information, rendering them appealing targets for cybercriminals. A recent investigation conducted by Vinoth et al. (2022) has demonstrated that inadequate authentication mechanisms, deficiencies in access control protocols, and improperly configured security configurations might lead to unauthorised entry. These security breaches not only result in the compromise of customer information, but also give rise to regulatory infractions and substantial harm to reputation. According to Agur et al. (2020), in order to address these security threats, it is imperative for financial institutions to adopt strong encryption, multifactor authentication, and intrusion detection systems. Regular security audits and compliance assessments play a crucial role in verifying the adherence of cloud providers to industry-specific rules and data protection standards.

The study conducted by Chang et al. (2020) has demonstrated that privacy risks arise with the implementation of cloud computing, specifically in relation to data sovereignty. Financial institutions are required to take into account the location of their data storage and processing activities, since they may be subject to the regulations and laws governing data protection in foreign jurisdictions. The alignment between data transfers across international boundaries and the stringent regulatory requirements imposed on financial institutions may not be congruent (Thach et al., 2021). According to Li et al. (2021), in order to mitigate these issues, it is recommended that institutions use cloud providers that provide data localization options, enabling them to securely store sensitive data within designated geographical locations. Furthermore, the incorporation of data classification and access control measures serves to safeguard client confidentiality and guarantee the appropriate utilisation of data.

According to Ryll et al. (2020), the deployment of cloud computing in the banking sector is associated with significant operational hazards. Operational hazards associated with cloud computing encompass potential instances of system downtime, availability concerns, data loss occurrences, and difficulties in the process of data recovery. Cloud service interruptions have the potential to cause significant disruptions to financial operations, leading to financial ramifications and reputational damage. Although cloud providers may issue service level agreements (SLAs) guaranteeing uptime, it is important for financial institutions to recognise that these agreements are not completely reliable. Therefore, it is crucial for them to carefully evaluate strategies for ensuring business continuity in the event of disruptions. According to Naimi-Sadigh et al. (2021), the implementation of comprehensive disaster recovery plans that specifically address cloud-related situations can serve as an effective strategy for financial institutions to avoid operational risks. It is imperative to conduct regular testing of these programmes. The use of redundancy and backup measures can also serve as a means to mitigate the risk of data loss.

Wang et al. (2021) conducted a study which concluded that the issue of vendor lock-in is increasingly perceived as a significant risk. Over the course of time, financial institutions may develop a significant reliance on a particular

cloud provider, resulting in challenges and expenses when attempting to transition to a different provider or transfer apps and data back to an on-premises environment. The presence of this dependency has the potential to restrict flexibility and constrain strategic choices. In order to mitigate the risk of vendor lock-in, it is advisable for institutions to use multi-cloud strategies, wherein they make use of several cloud service providers for distinct services (Ndung'u and Signé, 2020). This particular technique allows individuals or entities to maintain their bargaining power during negotiations and prevent excessive dependence on a sole provider.

The empirical review clearly demonstrates that cloud computing has notable benefits to financial institutions in terms of scalability, flexibility, and cost savings. However, it also introduces substantial dangers that necessitate efficient management. The issues pertaining to security, privacy, operational efficiency, vendor lock-in, and cost management that have been deliberated over in this essay emphasize the necessity of a well devised cloud strategy that integrates comprehensive security protocols, considerations for data sovereignty, contingency planning for disaster recovery, and effective cost management mechanisms. In order to effectively traverse the cloud environment, financial institutions must consistently assess their level of risk exposure, modify their security protocols accordingly, and uphold compliance with rules particular to their industry. Financial institutions may effectively leverage the capabilities of cloud computing while also protecting their reputation, ensuring client trust, and maintaining a competitive advantage in the era of digitalization by proactively addressing these associated risks.

Materials and Methods

The study adopted a quantitative cross-sectional research approach as a broad framework. A cross-sectional study is a research methodology that involves the collection of data at a certain point in time, with the aim of obtaining information for analysis and investigation (ref). Quantitative data is commonly expressed in numerical formats, including measures such as averages, ratios, or ranges. The study targets the employees of CDRB bank. The respondents were selected due to their roles in the three departments namely ICT, legal and the procurement departments. Based on a simple random sampling technique, individuals from the identified departments were selected. The simple random sampling was adopted due to its nature of providing all the respondents equal opportunity to all the respondents in participating in the research. This reduces researcher bias. A questionnaire was used to facilitate effective collection of a substantial amount of data from a sizable sample of 201 individuals which represents 28% of the population size (726 respondents). Gumpili, S. P., & Das (2022) noted that the maximum sample population size should be 30% of the population sample and should not exceed 1000 respondents. This informs the population size of this research.

Results

To achieve the objectives of the research, the respondents were asked whether cloud computing can result in data privacy issues in financial institutions. This was evaluated based on the Likert scale questions. Findings indicated that 89% of the respondents agreed that cloud computing in financial institutions is likely to face data security issues. 9% of the respondents disagreed with the same while 2% neither agreed nor disagreed. Data security is seen as a major risk associated with cloud computing. This is against the backdrop of literature reviewed such as Tesha (2022) who noted that cloud computing services also can enhance data security. The results are as shown in table 1.

Table 1. Perceptions on data privacy in a cloud environment

Cloud computing can result in data privacy issues in the financial institution	Frequency	Percentage	Cumulative percentage
Strongly agree	94	47	47
Agree	84	42	89
Neither agree nor disagree	4	2	91
Disagree	15	7	98
Strongly disagree	4	2	100
Total	201	100	

Source: Research Data, 2023

Regulatory compliance has also been established to pose a major risk for financial institutions with the adoption of cloud computing services. This is based on the results of which 71% of the respondents agreed that regulatory compliance can pose a risk to financial institutions with cloud computing adoption. The regulatory frameworks stipulate how cloud computing services should be adopted. Any failure to comply by the regulatory framework can result in legal suits. These results are in lieu of a study conducted by Ali and Osmanaj (2020) who established that the government regulations must be abided by the companies seeking to adopt cloud computing services. Another study by Kunduru (2023) also established that there is concern among users that regulatory compliance being a challenge in the adoption of cloud computing services. Violation of regulatory frameworks can have a major impact on the company. The results are as indicated in table 2.

Table 2. Perception of Regulatory Compliance

Regulatory compliance can pose a risk to financial institutions with cloud computing adoption	Frequency	Percentage	Cumulative percentage
Strongly agree	62	31	31
Agree	80	40	71
Neither agree nor disagree	12	6	77
Disagree	30	15	92
Strongly disagree	17	8	100
Total	201	100	

Source: Research Data, 2023

The research also established downtime as a major risk in the adoption of cloud computing services. The downtime results in cases where the system fails. From the collected data, 71% of the respondents indicated that they agree that downtimes are a major risk in the adoption of cloud computing services in financial institutions. These downtimes can result in stoppage of service delivery or data breach. This was emphasized by Golightly et al., (2022) who noted that downtimes can disrupt the normal operations of a company. The company can lose both financially and data security wise. This is as shown in table 3.

Table 3. Downtime

Downtime as a major risk in the adoption of cloud computing services	Frequency	Percentage	Cumulative percentage
Strongly agree	60	30	30
Agree	82	41	71

Neither agree nor disagree	6	3	74
Disagree	36	18	92
Strongly disagree	17	8	100
Total	201	100	

Source: Research Data, 2023

The study established that regular monitoring has the potential to minimize the risks of cloud computing in financial institutions. The majority (60%) of the respondents noted that regular monitoring is efficient as shown in table 4. Regular monitoring entails checks on the cloud computing adoption. This is in line with a study conducted by Scott et al., (2019) who focused on cloud computing adoption in financial institutions. They established there is the need for regular monitoring to ensure there are no data security vulnerabilities associated with cloud computing services.

Table 4. Regular monitoring

Regular monitoring can minimize the risks of cloud computing in the financial institutions	Frequency	Percentage	Cumulative percentage
Strongly agree	46	23	23
Agree	75	37	60
Neither agree nor disagree	20	10	70
Disagree	40	20	90
Strongly disagree	20	10	100
Total	201	100	

Source: Research Data, 2023

Furthermore, the study assessed the relationship between the various variables using correlation analysis with the primary aim of first determining whether there is a relationship between the variables being studied. Subsequently, the study seeks to assess the strength and direction of this relationship and establish the effect of the relationship between the variables. The R-value, often known as the correlation coefficient, was utilized to do an analysis on the degree of association between the three variables namely, data privacy, downtime, and regulatory compliance whose relationships are evaluated against cloud computing services. The findings suggest a statistically significant and positive correlation among the three factors. The parameter in question possesses a numerical value that spans from -1 to +1 (appendix 1). A value of -1 signifies a comprehensive negative linear link, while a value of +1 signifies a complete positive linear correlation. The notation is employed to denote the range of values for this parameter.

The study's results indicate that data privacy, downtime and regulatory compliance are related to cloud computing services adoption in financial institutions. The study's findings lead to a clear conclusion. The R-values attained by each of the contexts, either 0.7 or higher, or -0.7 or below, indicate a substantial impact on internet security threats. The most notable outcome, with a value of -0.836, was attained for data privacy making it the one with the highest score.

Discussion

The modern era is characterized by rapid technological advancements that have fundamentally transformed industries and societies. The financial sector, being at the forefront of innovation, has embraced technology to enhance operational efficiency, deliver superior customer experiences, and drive innovation (Gana et al., 2019). Among the transformative technologies, cloud computing has emerged as a game-changer, offering

unprecedented opportunities for financial institutions to scale their operations, optimize costs, and innovate at a faster pace (Agur et al., 2020). However, alongside these opportunities lie many potential risks that demand careful evaluation and mitigation.

Cloud computing has gained momentum in the Tanzanian financial landscape, mirroring global trends. Financial institutions, including banks, are considering the migration from traditional on-premises infrastructure to cloud-based solutions. This shift is motivated by the desire to embrace digital transformation, capitalize on the scalability and agility of cloud resources, and foster innovation in a rapidly evolving sector as established by Kundur (2023). CRDB Bank PLC, as a prominent player in the Tanzanian financial industry, has recognized the allure of cloud computing and is poised to harness its potential. However, the road to digital transformation is not without its challenges and potential pitfalls.

The research findings provide insights into the potential hazards that may arise from the implementation of cloud computing within CRDB Bank PLC, a large financial institution in Tanzania. The study's objective was to complete evaluation of the risks associated with the bank, considering the viewpoints of different stakeholders such as IT specialists, risk managers, and senior executives. The study also investigated the congruence between the current regulatory framework in Tanzania and global norms, with a specific emphasis on mitigating the distinct issues associated with the deployment of cloud computing in financial institutions. The study revealed several dangers that should be considered by financial organizations, such as CRDB Bank PLC, when contemplating the implementation of cloud computing. Data security and privacy provide a discernible risk within the realm of research. The participants voiced apprehensions over the safeguarding of confidential financial information that is maintained in cloud-based systems. Scott et al., (2019) established that the emergence of crucial challenges like data breaches, unauthorized access, and data loss has necessitated the use of sophisticated security measures and encryption systems. The data collected also indicates the potential for service disruptions and downtime resulting from cloud service provider failures or technical issues. Maintaining uninterrupted operational continuity was deemed imperative to mitigate potential disruptions to banking services.

One of the primary obstacles anticipated in the use of cloud computing services by financial institutions is regulatory compliance. This is also echoed by Soon (2021). The findings of the study highlighted the difficulties encountered in achieving adherence to regulatory obligations in Tanzania during the process of shifting to cloud-based services. The requirement to ensure that cloud solutions adhere to the special rules of the banking sector presented a hindrance. The respondents also voiced apprehensions regarding the possibility of developing excessive reliance on cloud service providers, which might potentially result in difficulties when shifting to alternative providers or going back to on-premises solutions.

The participants underscored the significance of conducting comprehensive risk assessments and exercising due diligence prior to the selection of cloud service providers. The authors emphasized the importance of implementing comprehensive security measures and maintaining continuous monitoring in cloud systems. The report additionally underscored the importance of implementing risk mitigation methods and developing contingency plans to effectively manage any interruptions. It was emphasized that inclusion of risk management is crucial in adopting cloud technology as was also established by Kayode-Ajala (2023). Nevertheless, the participants also recognized the potential advantages of cloud computing, albeit emphasizing the necessity of striking a delicate equilibrium between these benefits and a thorough assessment of associated risks. The research highlights the significance of robust governance and accountability procedures.

Conclusion

The research findings highlighted the significance of adopting a well-rounded approach towards the implementation of cloud computing within financial institutions, such as CRDB Bank PLC. Although cloud technology presents a multitude of advantages, it is imperative for stakeholders to maintain a cautious stance towards potential dangers and effectively adopt comprehensive risk management and mitigation techniques. The findings of this study offer CRDB Bank PLC and other financial institutions in Tanzania useful information in making well-informed decisions regarding the deployment of cloud technology. These decisions must prioritize the security, privacy, and resilience of financial systems.

Additionally, the results underscore the necessity of ongoing cooperation between the financial industry and regulatory bodies to guarantee that the regulatory framework progresses in alignment with technological progress. There are various risk mitigation strategies that can be adopted by financial institutions in Tanzania. One of the strategies is implementing robust security protocols. Implementing state-of-the-art encryption, access controls, and intrusion detection systems to safeguard sensitive financial data and customer information (Vinoth et al., 2019). The financial institutions can also explore multi-cloud or hybrid cloud strategies to avoid vendor lock-in and enhance operational resilience. The institutions can also collaborate with regulators to develop cloud-specific guidelines that align with international best practices while addressing the unique needs of the Tanzanian financial sector.

Subsequent investigations may be directed towards the domains of security and compliance. The purpose of this study is to examine the security measures and compliance standards that are currently implemented for CRDB Bank Plc's cloud infrastructure. Evaluate the extent to which they conform to industry norms and regulatory frameworks that are specifically applicable to the financial sector in Tanzania. An additional domain for prospective investigation pertains to data privacy and sovereignty. The research will investigate the ramifications of keeping confidential financial information in cloud computing systems, encompassing considerations pertaining to data sovereignty, legislation governing the transfer of data across national borders, and the potential consequences for safeguarding consumer privacy.

Acknowledgement

I would like to express my sincere gratitude to Institute of Accountancy, Arusha for their invaluable support during the course of this research. Their contributions played a crucial role in the success of this project. I would also like to thank my supervisor for the help throughout the research process. Without the support, this work would not have been possible.

References

Agur, I., Peria, S. M., & Rochon, C. (2020). Digital financial services and the pandemic: Opportunities and risks for emerging and developing economies. *International Monetary Fund Special Series on COVID-19*.

Ali, O., & Osmanaj, V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. *computer law & security review*, *36*, 105396. https://doi.org/10.1016/j.clsr.2020.105396

Brown, S. J. (2022). Influence of Cloud Computing Adaption on Organization Performance: A Case Study of Selected Commercial Banks in Ilala Municipality. *International journal of Engineering, Business and Management*, *6*(4), 32-40. https://dx.doi.org/10.22161/ijebm.6.4.4

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services–The overview, challenges, and recommendations from expert interviewees. *Technological forecasting and social change*, *158*, 120166.

https://doi.org/10.1016/j.techfore.2020.120166

Gana, N. N., Abdulhamid, S. I. M., & Ojeniyi, J. A. (2019). Security risk analysis and management in banking sector: A case study of a selected commercial bank in Nigeria. *International Journal of Information Engineering and Electronic Business, 2019*. 35-43. http://dx.doi.org/10.5815/ijieeb.2019.02.05

Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*, *14*, 18479790221093992. https://doi.org/10.1177/18479790221093992

Gumpili, S. P., & Das, A. V. (2022). Sample size and its evolution in research. *IHOPE Journal of Ophthalmology*, *1*(1), 9-13.

Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In *Cloud security: Concepts, methodologies, tools, and applications* (pp. 249-263). IGI Global.

Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Its Adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

Kelly, S., Ferenzy, D., & McGrath, A. (2017). *How financial institutions and fintechs are partnering for inclusion: Lessons from the frontlines*. Center for Financial Inclusion at Accion.

Kunduru, A. R. (2023). Artificial intelligence advantages in cloud Fintech application security. *Central Asian Journal of Mathematical Theory and Computer Sciences*, *4*(8), 48-53.

Li, F., Lu, H., Hou, M., Cui, K., & Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society*, *64*, 101487. https://doi.org/10.1016/j.techsoc.2020.101487

Macha, D. P., & Massawe, N. M. (2023). *Financial Technology in Tanzania: Assessment of Growth Drivers*. AERC Working Paper FI-007 African Economic Research Consortium, Nairobi.

Mosweu, T., Mosweu, O., & Luthuli, L. (2019). Implications of cloud-computing services in records management in Africa: Achilles heels of the digital era? *South African Journal of Information Management*, *21*(1), 1-12. http://dx.doi.org/10.4102/sajim.v21i1.1069

Mpofu, F. Y., & Mhlanga, D. (2022). Digital financial inclusion, digital financial services tax, and financial inclusion in the fourth industrial revolution era in africa. *Economies*, *10*(8), 184. http://dx.doi.org/10.3390/economies10080184

Mshana, H. C. (2020). *Factors influencing the adoption of cloud computing in public sectors*.Doctoral dissertation, Institute of Accountancy Arusha.

Naimi-Sadigh, A., Asgari, T., & Rabiei, M. (2021). Digital transformation in the value chain disruption of banking services. *Journal of the Knowledge Economy*, 1-31. https://doi.org/10.1007/s13132-021-00759-0

Ndung'u, N., & Signé, L. (2020). The Fourth Industrial Revolution and digitization will transform Africa into a global powerhouse. *Foresight Africa Report*, *5*(1), 1-177.

Neicu, A. I., Radu, A. C., Zaman, G., Stoica, I., & Răpan, F. (2020). Cloud computing usage in SMEs. An empirical study based on SMEs employees perceptions. *Sustainability*, *12*(12), 4960. http://dx.doi.org/10.3390/su12124960

Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. *World Bank*, *54*.

Philemon, B. (2020). *potentials and threats of crypto currency in the financial system in Tanzania*. Doctoral dissertation, Mzumbe University.

Ryll, L., Barton, M. E., Zhang, B. Z., McWaters, R. J., Schizas, E., Hao, R., ... & Yerolemou, N. (2020). Transforming paradigms: A global AI in financial services survey. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3532038

Scott, H. S., Gulliver, J., & Nadler, H. (2019). Cloud computing in the financial sector: A global perspective. *Program on International Financial Systems*.

Soon, S. (2021). 46 Improving the digital financial services ecosystem through collaboration of regulators and FinTech companies. In *FinTech, Artificial Intelligence and the Law: Regulation and Crime Prevention* (pp. 46-63). Routledge.

Tesha, D. S. (2022). *Assessing Factors Affecting Data Privacy in Local Government Authorities in Tanzania*. Doctoral dissertation, Institute of Accountancy Arusha (IAA).

Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845. http://dx.doi.org/10.24874/IJQR15.03-10

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, 2172-2175. https://doi.org/10.1016/j.matpr.2021.11.121

Wang, R., Liu, J., & Luo, H. (2021). Fintech development and bank risk taking in China. *The European Journal of Finance*, *27*(4-5), 397-418.

Yau-Yeung, D., Yigitbasioglu, O., & Green, P. (2020, October). Cloud accounting risks and mitigation strategies: Evidence from Australia. In *Accounting Forum* (Vol. 44, No. 4, pp. 421-446). Routledge.

Acharya, S., & Mekker, M. (2022). Public acceptance of connected vehicles: An extension of the technology acceptance model. *Transportation Research Part F: Traffic Psychology and Behaviour, 88*, 54-68. https://doi.org/10.1016/j.trf.2022.05.002

Appendix 1: Correlation Analysis

			Data security	Enhanced Data Accessibility and Availability	Risk Mitigation Strategies	Compliance and Regulatory Implications
Spearman's rho	Data security	Correlation Coefficient	1.000	.337**	.313**	.245**
		Sig. (2-tailed)		0.000	0.001	0.005
		N	201	201	201	201
	Enhanced Data Accessibility and Availability	Correlation Coefficient	.341**	1.000	.434**	.551**
		Sig. (2-tailed)	0.000		0.000	0.000
		N	201	201	201	201
	Risk Mitigation Strategies?	Correlation Coefficient	.255**	.436**	1.000	.427**
		Sig. (2-tailed)	0.001	0.000		0.000
		N	201	201	201	201
	Compliance and Regulatory Implications	Correlation Coefficient	.255**	.551**	.431**	1.000
		Sig. (2-tailed)	0.005	0.000	0.000	
		N	201	201	201	201