Journal of Business and Management Sciences, 2022, Vol. 10, No. 3, 131-137
Available online at http://pubs.sciepub.com/jbms/10/3/4
Published by Science and Education Publishing
DOI:10.12691/jbms-10-3-4

Security Issues and Challenges in Cloud Computing among Public Institutions in Africa

Gladwell Murigi*, Morrisson Mutuku

Department of Management Science, School of Business, Kenyatta University
*Corresponding author: gladwellmurigi@gmail.com

Received June 02, 2022; Revised July 10, 2022; Accepted July 17, 2022

Abstract The idea of storing and managing data on virtualized servers has been brought to life by cloud computing technology allowing apps, individuals and organizations all over the world to connect to data and computing resources anywhere and at any time. Users of cloud computing can share processing power, storage space, bandwidth, memory and software. Because cloud computing is so simple to use, consumers no longer need to invest much in IT infrastructure. However, cloud computing comes with its own challenges with cloud security and privacy being the biggest concerns. Many organizations are uncomfortable with storing their data and applications on systems they do not control. In addition, since cloud services are accessed via internet, there is risk of attack by hackers. It was therefore important to assess security issues and challenges in cloud computing among public institutions in Africa. This study adopted a systematic review of literature. During the selection of studies to be used in a systematic review, the search for empirical studies was done in an extensive manner. Multiple or numerous sources, both printed and computerized were searched.. This study selected studies that were less than 5 years old. In addition, the study selected studies conducted in Kenya, other countries in Africa and around the world. To ensure the quality of the studies, the study selected studies with abstract, introduction, objectives, methods, results/findings and conclusions. The study concludes that challenges and security issues in cloud computing among public institutions include data breach, account hijacking, data loss, denial of service attacks, cloud abuse, malicious insiders, phishing attacks, portability restrictions, backdoor channel attacks, cloud malware injection attacks, shared technology vulnerabilities and lack of confidentiality of corporate data. The researcher therefore recommends that the governments should come up policies to govern and improve cloud computing adoption among public institutions. In addition, the study recommends development of policies to protect data from external hackers and malicious individuals. Policy makers should develop clear policies that require the cloud service providers to safeguard privacy and also security of data they are managing on behalf of institutions. Moreover, the policy makers should come up with policies that guide the provision of penalties to security failures. Also, public institutions should establish an information and communication technology department to come up with strategies to protect data in their organizations.

Keywords: *cloud computing, public institutions, security issues*

Cite This Article: Gladwell Murigi, and Morrisson Mutuku, “Security Issues and Challenges in Cloud Computing among Public Institutions in Africa.” *Journal of Business and Management Sciences*, vol. 10, no. 3 (2022): 131-137. doi: 10.12691/jbms-10-3-4.

1. Introduction

National Institute of Standards and Technology (NIST) defines cloud computing as a model for providing ubiquitous, convenient, on-demand access to a common pool of configurable computing resources that can be rapidly released and provisioned with minimal service provider interaction or management effort. Cloud computing is a method of consuming software or other IT services on demand via Internet. Users can share processing power, bandwidth, memory, storage space and software on this platform [1]. Because cloud computing is simple to use, consumers no longer need to invest much in IT infrastructure. Cloud computing technology has now introduced the concept of storing and managing data on virtualized servers, allowing apps, individuals and organizations all over the world to connect to data and computer resources from anywhere and at any time [2].

Cloud computing is accessible by utilizing the following standard models. Software-as-a-Service (SaaS) is a model in which a customer uses client interface or program interface, such as a web browser, to access provider applications over a cloud infrastructure. Platform-as-a-Service (PaaS) is a service model in which a service provider offers clients access to a cloud-based environment in which they can develop and deploy applications while the provider manages the underlying infrastructure. Infrastructure-as-a-Service (IaaS) is a computing model in which a customer rents processing, storage, networks and other computer resources to deploy and execute software such as operating systems and applications [3].

IaaS, SaaS and PaaS can be employed in private cloud, a hybrid cloud, a community cloud or a public cloud. Although management of the cloud may not always be within the organization, private clouds are exclusively owned and distributed within it. Public cloud refers to a group of services that the general public may access via standard APIs over the Internet. Hybrid cloud is a mix of both public and private clouds. An organisation may use a private cloud for confidential and sensitive information while the rest is accessed via a public cloud. Multiple organizations with similar concerns (e.g., security, missions and interests) share cloud infrastructures in deployment of community cloud. Diverse organizations play numerous roles in implementation models. Some act as providers, offering cloud services to customers, while others act as resellers, aggregating cloud services from providers to provide customers with expanded characteristics and ability [4].

IBM [5], notes that flexibility, efficiency and strategic value are some of the advantages associated with cloud computing. Users can create applications, scale services to meet their needs and use cloud services from anywhere with an internet connection. Furthermore, consumers can obtain apps without being concerned about prices or upkeep of the underlying infrastructure. Cloud services also give businesses a competitive edge by allowing them to use the most cutting-edge technology available. Firms and organisations have also realized that cloud computing has the potential to help them reduce costs [6], and improve coordination between themselves and their suppliers by using the same services from a common cloud computing platform [7].

Figures from Statista [8] indicate that the cloud computing market in Europe was valued 63 billion euros in 2021, and it is expected to grow to 560 billion euros by 2023. Storage, analytics, networking and development tools are among the products and services available to clients and they can help businesses save money and scale more quickly.

Despite China's technology advancements and the world's largest e-commerce market, firms have been sluggish to invest in various IT initiatives that increase operational effectiveness or create a competitive edge, according to McKinsey & Co. [9]. The Chinese government recognizes the importance of the cloud and has announced its commitment to its development. According to a plan released by China's Ministry of Industry and IT, officials seek to grow cloud computing sector by more than 2.5 times its current size by 2019, compared to 2015.

In Morocco a research done by M'Rhaourh, Elachkar, Chafiq and Namir [10] noted that many companies surveyed did not have sufficient knowledge about cloud-based solutions and services. Cloud computing is relatively new to the country, and there is need for more awareness of this technology. In Tunisia, Osei-Opoku, Regaieg and Koubaa [11] indicate that 12.8 per cent of all government institutions were utilizing cloud computing, but 87.2 per cent had not adopted cloud computing. Chinyemba and Phiri [12] observed that in the Zambian public sector, 33 per cent of the institutions had adopted cloud computing and the low adoption was attributed to cyber security readiness.

Infrastructure challenges, anxiety over safety and security of data and government policies are some of the factors that have stalled cloud computing growth in Nigeria. Iwuchukwu, Atimati, Ndukwe and Iwuamadi [13] continue to add that industry analysts opine that if broadband infrastructure limitations are promptly overcome to extend internet adoption, Nigeria has a cloud computing market potential of over $1 billion.

Sithole and Ruhode [14] observed that cloud computing delivers a compelling economic case across the board as digitally-driven change, efficiency and cost control become top goals for the South African public sector. In addition, 26 per cent of public organizations in South Africa have adopted cloud computing and have a holistic multi-cloud management strategy in place today.

In Botswana, Khanda and Doss [15] observed that compared to the private institutions where 65 per cent had adopted cloud computing, only 29 per cent of the public institutions had adopted cloud computing.

Cloud adoption has accelerated in recent years, owing to improved broadband connectivity and more economical data. However, due to lack of information, cost and security concerns and unreliable high-speed internet connection, many private firms and public organizations in East Africa have yet to completely embrace these services [16]. In Tanzania, Kabudi [17] observed that despite getting financing from the government, only 18 per cent of the institutions in the Tanzanian education sector had adopted cloud computing. In Ethiopia, both government and private businesses have yet to adopt cloud computing because they are unaware of the benefits and drawbacks of doing so. Majority of employees in both government and private businesses identified security as a serious concern or impediment to cloud adoption. Furthermore, institutions in Ethiopia have a limited understanding of cloud computing [18]. In Uganda, 6.6 per cent of the institutions in central government had employed cloud computing services, 8.8 per cent had cloud computing under evaluation and 51.6 per cent had no plans of adopting or utilizing cloud computing [19]. According to the NITA-U report from 2012, Ugandan central government institutions tend to be concerned about adopting cloud computing-based services due to a lack of clarity on security risks.

Over the last few years, however, there has been an upsurge in the adoption of cloud technology in Kenya. According to a 2016 study conducted by Communications Authority (CA) and Kenya National Bureau of Statistics (KNBS), 35.6 percent of public sector organizations use cloud computing services, but just 22.9 percent of private sector enterprises do. Cloud computing comes with its own challenges with cloud security and privacy being the biggest concerns.

Dar [20] notes that when an organization adopts cloud technology, they shift business sensitive information to cloud servers where there is little or no control over the data. Many organizations are uncomfortable with storing their data and applications on systems they do not control. It is therefore the cloud provider's job to maintain data security and privacy. Furthermore, because cloud services are accessed via the internet, hackers may target them.

The various issues posed by cloud computing can be mitigated by employing various encryption mechanisms, performing regular backups and selecting the right cloud provider.

2. Literature Review

2.1. Theoretical Review

This is a structure that can support a research theory. Theoretical framework defines and introduces the theory that explains the occurrence of research problem under investigation. This independent paper is anchored on UTAUT and Innovation Diffusion Theory.

2.2. Innovation Diffusion Theory

The above theory was coined by Everett Rogers in the year 1962. The theory has been defined as the diffusion of new ideas, behaviours, or technology within a social system [21]. It is through diffusion that people embrace a new idea, habit, product or technology as part of the social system. Diffusion refers to the spread of an idea through several channels throughout time. The time of adoption is the dependent variable in diffusion study [43].

Relative benefit, compatibility, complexity, trialability and observability are the five primary criteria that determine innovation uptake according to Rogers [22]. The extent to which innovation is considered superior to the program, product or idea it replaces is referred to as relative advantage. The degree to which innovation is compatible with experiences, values and requirements of possible adopters is referred to as compatibility [23]. Kunyoria, Auma and Onditi [24] indicate that complexity of an innovation refers to how difficult it is to comprehend and/or implement. Triability refers to how well an innovation can be tested or explored before committing to adopt it, while observability refers to how well it produces tangible outcomes.

Innovation Diffusion Theory will be used in this study to examine the security issues and also challenges in cloud computing among African public institutions. In relation to relative advantage, cloud computing leads to an improvement in procurement process, flexibility, efficiency, faster service development and fostering of cross-team collaboration. In terms of complexity, cloud computing is easy to use while triability of cloud computing is treated high as it can be tested or experimented. In addition, cloud computing has observable results that are tangible including reduction in cost and improvement in service delivery. However, in relation to compatibility, migrating data to the cloud can be a daunting process, especially if the cloud environment is not able to work with it.

2.3. Unified Theory of Acceptance and Use of Technology (UTAUT)

Venkatesh *et al.* [25] suggested unified UTAUT as a technology acceptance paradigm in “User acceptance of IT: Toward united vision.” The theory illustrates how users intend to utilize information systems and also how they use it. Performance expectancy, effort expectancy, facilitating factors and social influence are direct forecasters of usage intention and behaviour [25]. Age, experience, gender and voluntariness of use influence the effect of four important characteristics on usage intention and behavior [26]. The idea was developed by evaluating and combining components from eight earlier models that were used to explain how people used information systems (theory of planned behaviour, motivational model, theory of reasoned action, model of personal computer use, technology acceptance model, social cognitive theory combined theory of technology acceptance model and diffusion of innovations theory).

The degree to which a person believes that employing a system will assist in enhancing job performance is known as performance expectancy [44]. The measures of performance expectancy entail perceived usefulness, job-fit, extrinsic rewards, outcome expectations and relative edge [27].

Venkatesh *et al.* [44] viewed effort expectancy as the degree of ease associated with the use of an information system. Effort expectancy is constructed from complexity and perceived ease of use. The degree to which an individual entrusts important others s/he feel should employ new technique is the social influence. Subjective norms, social variables, and image conceptions are comparable [28]. Facilitating conditions refer to how confident a person is that a technological and organizational infrastructure exists in order to make system use easier. The enabling circumstances include the equipment and other infrastructure required to use the system.

The performance expectancy construct in cloud computing, should have a beneficial impact on individual's behavioural intention to employ new technology. In terms of effort expectation, consumers are more likely to use a new technology if it is simple to use. Furthermore, the likelihood of use of a new technology is also influenced if a person believes that individuals think s/he should adopt the new technology (social influence). In addition, the presence of technological and organizational infrastructure facilitates the adoption of new technology. UTAUT focuses mostly on good user acceptance behaviour. Some of the primary negative elements that contribute to the slow development rate of user acceptability include security and privacy concerns. Cloud Risk (CR) was created as a new construct to reflect the many risks associated with cloud computing adoption.

2.4. Empirical Literature

In Iran, Mehrtak and Seyed [29] examined the security challenges occasioned by employing healthcare cloud computing. Pubmed, Scopus, Science Direct and Web of Science databases were used to perform a systematic review of the articles published in 2015 to November 2020. In cloud security, the key issues as per the report, were data security, integrity, network security, information confidentiality and availability. In addition, API, data encryption, classification and authentication were security solutions for cloud infrastructure. To guarantee safe communication, data encryption perhaps could be used to retrieve stored data from cloud. In addition, the study took into account a number of key issues that make the engineering process of cloud security difficult.

Hussam, Laith and Yazan [30] conducted a study on challenges and security risks of cloud computing in Malaysia. The study deployed systematic review of literature where literature from journals, articles and books were reviewed. The findings of this study indicated that attacks and threats in cloud security (risk factors) include account as well as service hijacking, abuse of cloud computing, backdoor channel attacks, cloud malware injection attack, cross siting scripting attacks, denial of service attacks, insecure application programming interface, metadata spoofing attack, malicious insiders, phishing attack, SQL Injection attacks, shared technology's vulnerabilities, sniffer attacks, unknown risk profile and Zombie attack (DoS / DDoS).

Al-Issa, Ottom and Tamrawi [31] conducted a survey of e-health cloud security challenges in Jordan. The study deployed a survey research approach and targeted the healthcare industry. Findings indicated that individuals and healthcare providers are concerned about security and also privacy implications of data centralization in the cloud. This data centralization gives attackers a one-stop to steal and also intercept data in transit, and further transfers ownership of data to providers of cloud service, giving healthcare providers and individuals less control over data. As a result, concerns regarding security, privacy, efficiency, and scalability keep cloud technology from becoming widely adopted.

Jones, Irani and Sivarajah [32] examined the risks and rewards of cloud computing in UK public sector. The study focused on three organisational case studies. The study used exploratory research design and qualitative case study enquiries. All three cloud implementations had different outcomes, including important benefits such as increased information management and work practice flexibility, as well as risks including loss of power and ownership of data for enterprises. Other risks include sensitivity of the data and privacy of information, portability restrictions, lack of data ownership, integration restrictions and disaster recovery restrictions.

In Africa, Tshepho, Lungile and Olefhile [33] examined security challenges of cloud computing in records management. Qualitative research approach was employed in this research. It based its findings on a content analysis of literature on cloud computing in records management. Results indicated that cloud computing provides organizations with useful tools for running their firms more efficiently and improving their records management processes. However, if Africa is to benefit from cloud-based records management services, concerns such as records storage, privacy, security, jurisdiction and digital divide must be addressed.

In Egypt, Panhwar, Khuhro, Shehram and Saddar [34] studied security issues in mobile cloud computing. The study adopted systematic review of literature related to cloud computing in public institutions in Egypt. The study categorized security issues in mobile cloud computing in terms of data protection risks, mobile phones security issues, cloud security and privacy issues. The findings indicated that the specific security issues in mobile cloud computing include virus problems, keyword issues, removable media, web-server safety issues, unauthorized WiFi access, theft or loss, malicious software, network penetration, unsupported applications and corrupted data.

In Ghana, Abdallah [35] examined the challenges, threats and security concerns related to cloud computing. The study made use of inductive approach that was based on document analysis. The findings indicated that security issues of cloud computing include data breach, account hijacking, data loss, rejection of service attacks, cloud abuse, inadequacy due diligence, malicious insider, mutual technology vulnerabilities as well as insecure interfaces and APIs. Security policies included data protection, limited cloud usage visibility, metastructure and applistructure failures, identity and access management and security assessment.

In a different study, Bediako-Kyeremeh, Duorinaa and Agyemang [36] studied barriers to adoption of cloud computing in industrial SMEs. The study used mixed methods research and data was collected by use of both questionnaires and key informant interviews. The results indicated that security and privacy issues were the most significant factors affecting adoption of cloud computing in industrial SMEs in Ghana. Security concerns included personal and physical security, unauthorized access to data and data confidentiality.

In Uganda, Suleiman, Sa'id and Shu'aibu [37] studied privacy and security concerns in cloud computing technology adoption. The study used a systematic review of literature and categorized security issues in terms of data privacy and security issues and cloud security issues. The study found that privacy and security concerns in cloud computing technology adoption include breach of data, inadequate due diligence, hijacking of user accounts, abuse of cloud service, denial of services to clients, data loss, insecure APIs, malicious employees, data replication and internal threats.

Moloja and Ruhode [38] examined the factors impacting Cloud Computing adoption in South African Institutions of Higher Learning. The study adopted exploratory qualitative research and focused on two TVET colleges. Qualitative data was collected by use of interview guide from 35 IT stakeholders and analysis was done using thematic analysis. In Matjhabeng TVET colleges, data insecurity, unavailability of internet connection, and infrastructure resources all influence adoption of cloud computing according to the report.

In Northeastern Nigeria, Saidu and Kwadan [39] studied the challenges facing cloud computing adoption in e-learning. The researcher adopted survey research approach and data for this study was collected using sampling procedures among Polytechnics and analyzed using an average coded total. Denial/delay of service, compatibility issues, ICT infrastructure, lack of skilled employees, violation of trust, poor policy, confidentiality, managerial issues, integrity, insufficient user access as well as technological bottlenecks were among the challenges incurred.

In a descriptive research, Rupra [40] investigated the challenges facing the security of cloud computing among Kenyan SMEs. The key research areas for this study were Nairobi, Kisumu and Mombasa, with the top one hundred SME firms as of 2016 forming the study population. The results indicated that the security issues include manipulation from hackers, lack of reliability from providers, loss of control, data breach, lack of liability providers, inconsistency between regulations and trans-national laws and lack of confidentiality of corporate data.

3. Methodology

This study adopted a systematic review of literature. Systematic review encompasses reviewing of the already existing literature as per the formulated objectives and making use of standard methods in the identification, critical appraisal, collection, reporting and analysis of data from selected studies in the review. One of the advantages of systematic review is that it is less costly to review existing literature as compared to collecting data from the field. Also, systematic review of literature reduces the duration of time used in collecting data. Babbie [41] indicate that systematic review comprises of five steps which include identification of relevant work, assessment of quality of studies, summarizing of the evidence and interpretation of the studies' findings.

During the selection of studies to be used in a systematic review, the search for empirical studies was done in an extensive manner. Multiple or numerous sources, both printed and computerized were searched without language restriction. This study selected studies that were less than 5 years old. This period was selected because policies in different countries keep on changing, and hence there may be adjustments in the policies related to cloud computing. In addition, the study selected studies conducted in Kenya, other countries in Africa and other countries around the world. To ensure the quality of the studies, the study selected studies with abstract, introduction, objectives, methods, results/findings and conclusions.

4. Discussions and Findings

Studies conducted on security challenges and issues in cloud computing among public institutions in Africa have focused on different security issues. In addition, these studies have been conducted in different contexts using different methodologies and have varying findings. Different studies conceptualized security concerns and challenges in cloud computing among public institutions in different ways. In their study, Abdallah [35] conceptualized cloud computing in terms of Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS) and Database as a Service (DBaaS). The security issues studied included trust and threats like data breach, malicious insiders, data loss and cloud abuse. Panhwar *et al.* [34] conceptualized security issues in terms of data protection risks, mobile phones security issues, cloud security and privacy issues. Bediako-Kyeremeh *et al.* [36] conceptualized threats and security concerns in terms of data security issues, cloud computing issues and access issues. Suleiman *et al.* [37] conceptualized security issues in cloud computing in terms of data privacy, security issues and cloud security issues.

Al-Issa *et al.* [31] posit that cloud computing characteristics include shared resources, elasticity, wide network access, on-demand self-service, and measured service while cloud computing was conceptualized as SaaS, PaaS, IaaS and XaaS. Moloja and Ruhode [38] conceptualized factors affecting cloud computing adoption in terms of data security, poor internet access, socio economic status, privacy, confidentiality, affordability, government support and complexity. In addition, Saidu and Kwadan [39] conceptualized cloud computing adoption in terms of SaaS, PaaS and IaaS. However, Rupra [40] looked at security challenges in terms of manipulation from hackers, data breach and loss of control. In addition, Tshepho *et al.* [33] conceptualized cloud computing in terms of public cloud, private cloud, community cloud and hybrid cloud. Cloud computing challenges included digital divide, unreliable nature of cloud services and noncompliance with legal requirements.

The empirical studies reviewed were conducted in different parts of the world. For instance, Mehrtak and Seyed [29] study was conducted in Iran, Abdallah [35] study was conducted in Ghana and Al-Issa*et al.* [31] study was conducted in the health sector in Jordan. Further, Jones *et al.* [32] study was conducted in the public sector in the United Kingdom. In addition, Tshepho *et al.* [33] was conducted in South Africa, Moloja and Ruhode [38] study was conducted among Higher Learning Institutions (TVET colleges) in South Africa, Saidu and Kwadan [39] study was conducted among polytechnics in North-eastern Nigeria, Panhwar *et al.* [34] was conducted in Egypt, Bediako-Kyeremeh *et al.* [36] study was conducted in Ghana, Suleiman *et al.* [37] study was conducted in Ghana and Rupra [40] was carried out among SMEs in Kenya. Due to the differences in the socio-economic and political environment, and the public sector policies and policies governing cloud computing, findings from one country cannot be applied in another country.

Most of the research studies reviewed used systematic review of literature including published articles and books as their methodology [29,30,34,35,37]. Further, Al-Issa *et al.* [31] and Moloja and Ruhode [38] studies used a survey research design. Similarly, Saidu and Kwadan [39] study utilized a survey research design and quantitative data was collected among staff working in polytechnics. Also, the study conducted by Rupra [40] utilized a descriptive research design and was carried out among SMEs in Kenya. The quantitative data was analyzed by employing descriptive and also inferential statistics. In addition, Moloja and Ruhode [38] study utilized exploratory research design and qualitative data was collected by use of key informant interviews. Similarly, Tshepho *et al.* [33] used qualitative research approach that involves collection of data by use of key informant interviews. The qualitative data was analyzed by use of thematic analysis and the results presented in a narrative form. Also, Bediako-Kyeremeh *et al.* [36] study used mixed methods research and data was collected by use of both questionnaires and key informant interviews. Abubakar *et al* [35] used qualitative techniques to analyse data from SMEs that had adopted cloud computing.

The studies reviewed observed that there are security issues in adoption of cloud computing services. For instance, Mehrtak and Seyed [29], Hussam *et al.* [30], Abdallah [35], Jones *et al.* [32], Rupra [40] and Tshepho *et al.* [33] found that security issues in the adoption of cloud computing services include data breach, account hijacking, data loss, denial of service attacks, cloud abuse, inadequacy due diligence, malicious insiders, phishing attacks, portability restrictions, backdoor channel attacks, cloud malware injection attacks, shared technology vulnerabilities and lack of confidentiality of corporate data.

In addition, Moloja and Ruhode [38] posit that factors affecting cloud computing adoption include data security, lack of access of the internet and infrastructure resources. Further, Saidu and Kwadan [39] indicate that challenges facing the adoption of cloud computing application include denial / delay of service, ICT infrastructure, compatibility issues, lack of skilled employees, poor policy, trust violation, managerial issues, integrity, limited user access, confidentiality and technological bottlenecks. Furthermore, Al-Issa *et al*. [31] argue that cloud-based data centralization creates numerous security and privacy problems for consumers and healthcare providers and leads to loss of control and privacy of information. Also, Bediako-Kyeremeh *et al.* [36] found that security concerns include personal and physical security, unauthorized access to data and data confidentiality. In addition, Abdallah [35] and Panhwar *et al.* [34] observed that security issues of cloud computing include data breach, account hijacking, data loss, rejection of service attacks, cloud abuse, inadequacy of due diligence, malicious insider, shared technology vulnerabilities as well as insecure interfaces.

5. Conclusions and Recommendations

The study concludes that challenges and security issues in cloud computing among public institutions include data breach, account hijacking, data loss, denial of service attacks, cloud abuse, malicious insiders, phishing attacks, portability restrictions, backdoor channel attacks, cloud malware injection attacks, shared technology vulnerabilities and lack of confidentiality of corporate data. This independent paper recommends that governments should develop policies to govern and improve cloud computing adoption among public institutions. In addition, the study recommends development of policies to protect data from external hackers and malicious individuals. Also, public institutions should establish an information and communication technology department to come up with strategies to protect data in their organizations. Policy makers should develop clear policies that require the cloud service providers to safeguard privacy and also security of data they are managing on behalf of institutions. Moreover, the policy makers should come up with policies that guide the provision of penalties to security failures.

References

[1] Tyagi, A. (2017). A Review Paper on Cloud Computing. International Journal of Engineering Research & Technology, 5(23), 1-2.

[2] Alemu, M., & Omer, A. M. (2014). Cloud Computing Conceptual Security Framework for Banking Industry. Journal of Emerging Trends in Computing and Information Science, 5(12), 921-930.

[3] IBM (2021). IaaS vs PaaS vs Saas. Available at https://www.ibm.com/cloud/learn/iaas-paas-saas. Retrieved 12 March, 2022.

[4] Omwansa, T. (2014). Cloud Computing in Kenya: A baseline survey.

[5] IBM (2018).Benefits of Cloud Computing. Available at https://www.ibm.com/cloud/learn/benefits-of-cloud-computing?msclkid=8ad1aa2fb0ef11ecaaa37a7c8f09b44d. Retrieved 10 March, 2022.

[6] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58

[7] Ceccagnoli, M., Forman, C., Huang, P. & Wu, D. (2012). Co-creation of value in a platform ecosystem: the case of enterprise software. MIS Quarterly, 36(1), 263-290.

[8] Statista (2021). Cloud computing in Europe - Statistics & Facts. Available at https://www.statista.com/topics/8472/cloud-computing-in-europe/?msclkid=57bc9224b0f211ec8b98de0407c0e724. Retrieved 29 March, 2022.

[9] Mckinsey & Co. (2018). Public Cloud in China.Big Challenges, big upside. Available at https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/public-cloud-in-china-big-challenges-big-upside. Retrieved 30 March, 2022.

[10] M'Rhaouarh, I., Elachkar, I., Chafiq, N. & Namir, A. (2020). Adoption of Cloud Computing by Enterprises in Morocco: A survey. International Journal of Scientific &Engineering Research, 11(11), 2229-5518.

[11] Osei-Opoku, E., Regaieg, R. & Koubaa, M. (2020). Review on Cloud Computing Security Challenges. European Scientific Journal, 16, 63-76.

[12] Chinyemba, M. K. & Phiri, J. (2018). An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector. Journal of Computer Science, 14, 1389-1400.

[13] Iwuchukwu, U., Atimati, E., Ndukwe, C.I. & Iwuamadi, O. (2017). The State of Cloud Computing in Nigeria. IOSR Journal of Electrical and Electronics Engineering, 12, 84-93.

[14] Sithole, S. & Ruhode, E. (2021). Cloud Computing Adoption: Opportunities and Challenges for Small, Medium and Micro Enterprises in South Africa. Journal of Could Computing, 23, 89-102.

[15] Khanda, M. & Doss, S. (2018). SME Cloud Adoption in Botswana: Its Challenges and Successes. International Journal of Advanced Computer Science and Applications, 9(10), 468-478.

[16] Wainaina, F. (2020). Harnessing the Power of Cloud Computing in Kenya. Available at https://www.itnewsafrica.com/2020/09/harnessing-the-power-of-cloud-computing-in-kenya/?msclkid=5d626771b0d011ecb4630edb6af2f003. Retrieved March 25, 2022.

[17] Kabudi, K. (2017). The application of Cloud Computing in the Tanzania Education Sector: Case study of Ministry of Education, Science and Technology (MoEST). Journal of Computer Science and Applications, 12, 90-112.

[18] Demissie, S. (2017). Cloud-Computing: Adoption Issues for Ethiopian Public and Private Enterprises. Electronic Journal of Information Systems in Developing Countries, 78, 1-14.

[19] Mugyenyi, R. (2018). Adoption of Cloud Computing Services for Sustainable Development of Commercial Banks in Uganda. Global Journal of Computer Science and Technology, 18(1), 12-34.

[20] NIST (2011). Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-45.pd.

[21] Niu, J. (2020). Diffusion and adoption of research data management services. Global Knowledge, Memory and Communication, 69(3), 117-133.

[22] Rogers, E. (2003). Diffusion of Innovations, 5th Edition. New York: Simon and Schuster.

[23] Mannan, B., & Haleem, A. (2017) Understanding major dimensions and determinants that help in diffusion & adoption of product innovation: using AHP approach. J Glob Entrepr Res. 7, 12, 1-24.

[24] Kunyoria, O. J., Wagude, A., & Onditi, L. A. (2018). Technology Adoption and Lean Manufacturing: A Case of Sony Sugar

Company, Awendo, Kenya. International Journal of Novel Research in Humanity and Social Sciences, 5(6), 20-29.

[25] Venkatesh, V., Thong, J. L. & Xu, X. (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. Journal of the Association for Information Systems, 17(5), 23-45.

[26] Mütterlein, J., Kunz, R.E. & Baier, D. (2019). Effects of lead-usership on the acceptance of media innovations: A mobile augmented reality case. Technological Forecasting and Social Change, 145, 113-124.

[27] Wu, M., Yu, P., & Weng, Y. (2012). A study on user behavior for I Pass by UTAUT: Using Taiwan's MRT as an example. Asia Pacific Management Review, 17(1), 91-111.

[28] Delavari, V., Shaban, E. & Hassanzadeh, A. (2020). Thematic mapping of cloud computing based on a systematic review: a tertiary study. Journal of Enterprise Information Management, 33(1), 161-190.

[29] Mehrtak, M. & Seyed, A. S. (2021). Security challenges and solutions using healthcare cloud computing. Journal of Medicine and Life, 2(3), 29-89.

[30] Hussam, A. S., Laith, M. K. & Yazan, A. A. (2017). A Review of Challenges and Security Risks of Cloud Computing. Journal of Telecommunication, Electronic and Computer Engineering, 9, 87-91.

[31] Al-Issa, Y., Ottom, N.A. & Tamrawi, A. (2019). eHealth Cloud Security Challenges: A Survey. Journal of Healthcare Engineering, 23, 1-15.

[32] Jones, S., Irani, Z. & Sivarajah, U. (2017). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. Inf Syst Front, 21, 359-382.

[33] Tshepho, M., Lungile, L.. & Olefhile, M. (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.

[34] Panhwar, A.M., Khuhro, S.A. Shehram, S.M. & Saddar, S. (2020). Investigation of Security Issues in Mobile Cloud Computing. PalArch's Journal of Archaeology of Egypt, 7(6), 2330-2340.

[35] Abdallah, N. (2020). Issues in Cloud Computing: Challenges, Threats and Security Concerns. Al Dar Research Journal for Sustainability, 4(2), 3-64.

[36] Bediako-Kyeremeh, K., Duorinaa, E. & Agyemang, S. (2019). Cloud Computing in Industrial SMEs: Identification of Barriers to Its Adoption and Benefits of Its Application in Ghana. Stu International Journal of Technology, 1(7), 1-28.

[37] Suleiman, M.M., Sa'id, P. & Shu'aibu, R.B. (2021). Privacy and Security Concerns in the Adoption of Cloud Computing Technology. Journal of Applied Sciences, Information and Computing, 2(1), 33-45.

[38] Moloja, D. & Ruhode, E. (2020). Factors affecting Cloud Computing adoption in Higher Learning Institutions in South Africa: A case of Matjhabeng TVET Colleges. Conference on Higher Education Advances, 12, 1261-1272.

[39] Saidu, A. & Kwadan, S.M. (2020). Factors Challenging the Adoption of Cloud Computing Application in E-Learning among Polytechnics in Northeastern Nigeria. European Journal of Computer Science and Information Technology, 8(2), 38-49.

[40] Rupra, S. (2020). A Descriptive Research on the Security Challenges of Cloud Computing Among Selected SMEs in Kenya. International Journal of Innovative Science and Research Technology, 5, 588-598.

[41] Babbie, E. R. (2017). The basics of social research. Boston: Cengage Learning.

[42] Dar, A. A. (2018) Cloud Computing-Positive Impacts and Challenges in Business Perspective. J Comput Sci Syst Biol, 12, 15-18.

[43] Dearing, J. W. & Cox, J. G. (2018). Diffusion Of Innovations Theory, Principles, And Practice. Health Affairs. 37. 183-190.

[44] Venkatesh, V.; Morris, M. G.; Davis, G. B. & Davis, F. D. (2003). "User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly. 27(3): 425-478.