CLOUD NETWORK SECURITY TOOL AND MANAGEMENT INFORMATION SYSTEMS SUCCESS OF CIVIL SERVICE IN SOUTH-SOUTH, NIGERIA

OBELEM OTONYE ALALIBO[1] and PROF. (MRS.) ANTHONIA ENEFAA BESTMAN[1]

obelem.alalibo@ust.edu.ng; toniabestman@gmail.com
Department of Office and Information Management, Faculty of Management Sciences, Rivers State University, Nkpolu-Oroworukwo, Port Harcourt, Nigeria

ABSTRACT

Cloud network security tool is the technological tool available on-demand to ensure that organizations databases are not access by unauthorized users. It is essential service provided by cloud service providers. This study surveyed cloud network security tool and management information systems success of civil service in South-South, Nigeria. The study adopted cross sectional survey design. Structured questionnaire designed on a 5-point Likert scale was used to collect data from the respondents and analyzed using descriptive statistics while Spearman's rank order correlations was used as the test statistics. The population of the study of consists of six (6) states in South-South, Nigeria. Ninety six (96) questionnaires were equally distributed to the various states, out of which eighty six (86) copies of the questionnaire distributed were properly completely and returned which stands as our usable number for analysis. The major findings revealed that there is a positive correlation between Cloud Network Security Tool and Management Information System Success of Civil Service in South-South, Nigeria. The study concluded that for effective and proper security of management information system, the civil service in South-South, Nigeria and other similar organizations, should ensure the cloud services prevent network from unauthorized users. Organizations that are able to implement cloud network security tool stand the chance of achieving the goal of information availability, accessibility and accuracy while those that are not able to implement this tool may continue to experience problems of network security in their databases.

Key words: cloud, network, security, availability, accesibility, accuracy, information, MIS

INTRODUCTION

Cloud Network security tool is the technological tool available on-demand or techniques provided by cloud service provider to prevent unauthorized users gaining access into the information system (Achar, Patel & Husain, 2022). The internet is a volatile platform such security enforcement must be taken seriously. Most organization made this delegate mistakes, they quickly to the cloud without proper measures in place. They migrate their information system to the loud without ensuring proper security measures, this singular mistake has caused organizations value digital assets (financial cost). In fact, the present age is described as the information age, where information is now the new oil, it requires proper security even more than the physical assets. Information is the future of the organization. Competitors capitalize on any slightest mistake made by the competing organization. Cloud Service providers protects clients organization or databases operating online (real time) from unauthorized access, use, disclosure, disruption, modification, or destruction. Cloud network security tool increases data quality. The quality of data/information the organization is able to manage defines the organization values which are integrity, confidentiality, reliability, accessibility, availability and accuracy which are information or data quality (Lipi, Rahman & Hasan, 2013). Information and communication technology (ICT) revolution has continued to drive the wide use of computers and other info-tech infrastructure which accelerate data processing and transmission in compliant

organizations (Bestman; Alfred, 2022). The world today is now experiencing dynamic organizational processes, structure and culture which the traditional tools cannot handled.

Information/data is the most important digital asset with which organizations have not taken adequate measures to manage (Duan, 2017). It is the most critical aspect of the organization's assets, but unknowingly sometimes, management and other users of the information system do not have this realization. Instead, they focused more on tangible assets. Tangible assets can be easily recovered or gained back, but any attempt or loss of critical part of the information system, can result to total business collapses. The term "digital asset" in the economic and legal aspects has been classified in the research of Kud (2019) as an information resource derivative of the right in a value and circulating in the distributed ledger in the form of a unique identifier.

Mirrazavi and Hashemzadeh (2016) defined cloud computing as the development and use of Internet-based computer technology. It is the application of information technology tool in the provision of services which include, providing essential software, analysis, specialized job role such as calculations, storage etc. Cloud security provides the tools to ensure technology related capabilities are offered to users as a service and it allows them to access the Internet-based services without having specialized information about these technologies or needs to control the technology infrastructure that supports it (Mell & Grance, 2017). Cloud security tools enhance effective use of the resources provided, it supports the service capacity or increase trust of client to dynamically investing in cloud infrastructure. The innovation in cloud technology requires the training of staff to be familiar with the new technology or authorizing new software (Mirrazavi & Khoorasgani, 2016).

There is lot of benefit in operating global information system. Organizations that are able to migrate to the cloud has lot of benefit over those that are yet to join, but in spite of the hugged benefit, there also disadvantages when proper security measures are not taken as such, there will be abused of resources even by the right access users, hijacking of organizational information, theft of network and resources. It is now imperative to carefully study this concept cloud network security tool and management information systems success of Civil Service in South-South, Nigeria. This research is underpinned by the Activity. Activity theory is based upon the work of Vygotski and his student Leont'ev from their studies of cultural-historical psychology in the 1920s (Verenikina, 2001). It is based on the idea that activity is primary, that doing precedes thinking, that goals, images, cognitive models, intentions, and abstract notions like "definition" and "determinant" grow out of people doing things" (Morf & Weber, 2000).

The following null hypotheses are formulated to guide the study:

H_{01}: There is no significant relationship between cloud network security tool and availability of information in the databases of the Civil Service in South-South, Nigeria.

H_{02}: There is no significant relationship between cloud network security tool and accessibility of information in the databases of the Civil Service in South-South, Nigeria.

H_{03}: There is no significant relationship between cloud network security tool and accuracy of information in the databases of the Civil Service in South-South, Nigeria.

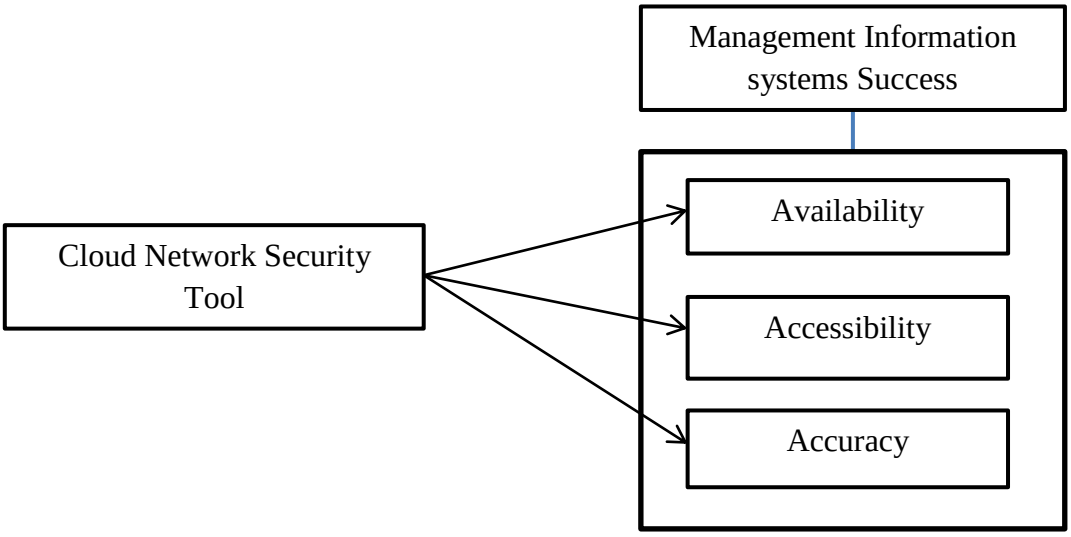

Figure 1: Relationship between cloud network security tool and management information system success of Civil Service databases in South-South, Nigeria.

LITERATURE REVIEW

Cloud Network Security

Cloud network security is the establishment of policies and practices that will enhance the save transmission of data/information from one destination to another via network without the intrusion by unauthorized users of the system usually hijackers (Sankariah, Bhadru & Kumar, 2017). The data/information is encoded from the source and decoded at the destination (Sankariah, Bhadru & Kumar, 2017). Cloud network security uses encryption to protect the data or information transmitted from one destination to another, from the source of the information, it is encoded and, in the destination, the information is decoded (Sankariah, Bhadru & Kumar, 2017). It involves the authorization of access to data in a network, which can be modified by the network administrator (Yu et al., 2010). There are three main aspects of the network security prevention, protection, and security (Yu et al., 2010). Ultimately the overall goal of the network security is to create a connected network that protect against illegal activity while allowing the right user to perform legal operation. Therefore, cloud network does not mean denied access. Basically, an unsecure network refers to "FREE WIFI" which can easily be founded near coffee shops, malls etc. They did not need any means of login to the network (Yu et al., 2010). Organizations network required proper and secured mean of authentication before any user can login to the database.

Cloud network security management is by nature a distributed function (Brandao, 2018). Organizations information systems face the same security threat like the physical environment (Brandao, 2018). In today digital age, security management is a serious concept in organization; information/data is vital assets to all organizations be it small or big organizations, it is the target of any competitors. Internet simply means the connectivity of millions of computers, databases, department databases and external (clients) computers in a network. It be simply be defined as network of computers or organizations, therefore, there is need for individual organization to protect themselves from any external attack. Cloud network security differentiates the groups in network by limited how one user can operate or use the internet (Simarjeet, 2012). Network

security is not feasible without a secure infrastructure that protects data in transit from modification, spoofing, and replay (Simarjeet, 2012). Security management could require human presence to control and modify the security device and evaluate all significant events (Blum & Schreiner, 2009). Cloud simply means remote or distant away from the users (virtual machine). It is basically the monitoring of computers in the network, it identifies members and non-members of the organization (Blum & Schreiner, 2009). There is a correlation between network monitoring and management of system events (Blum & Schreiner, 2009). It helps to detect sophisticated attacks. It is a proactive way of safeguarding organizational assets. It hindered or removed unauthorized users from the network, not allowing them to be connected (Bernstein, 2007). Network security includes device configuration, policy management, real time monitoring enabler and other methods available (Bernstein, 2007). Devices configuration are security policies initiated to provides a similar, intuitive interface across all device types and versions, along with complete support for all device features (Oleg et al., 2002). Network security is a serious concept that requires proper investigation by any successful cloud users (Oleg et al., 2002).

Management Information System Success

The concept blends principles, theories and practices of management. These terms information and system gives rise to a single product called Management Information System (Yang, Tan, Dai, & Guo, 2009). It is the regard to the individual and his ability to use information (Yang, Tan, Dai, & Guo, 2009).

In other words, information itself is not a unitary concept, but has different levels of organization, around which different theories are built and practices evolved. Today there are different concepts of information sciences but only different approaches from the perspective of integrating professional perspectives (Yausef, Mjlae, Abu-Ulbeh & Hassan, 2020). Managers make these investments to address a business need or opportunity, so it is important to identify whether the systems meet the organization's goals or not (Jain & Bhardwaj, 2010). Kim, Kim, Lee, and Lee (2019) described the mission of information systems (IS) as: "the effective design, delivery, use and impact of information technologies in organizations and society.

The term 'effective' seems key. Surely, the Information System Community (ISC) is explicitly concerned with improving the craft of design and the practice of management in the widest sense of both those terms (Yausef, Mjlae, Abu-Ulbeh & Hassan, 2020). Similarly, it looks at information technologies in their context of real people in real organizations in a real society." Based on Keen's view of information systems, the evaluation of the "effectiveness and efficiency" or "success" of information systems is an important aspect of the information systems field in both research and practice. However, the manner in which we evaluate the success of an information system has changed over time both in context, purpose, and impact of Information technology (IT) has evolved. It is, therefore, essential to understand the foundations and trends in information systems success (ISS) measurement and what they mean for the future.

This paper adopted the DeLone and McLean IS Success Model, commonly referred to as the D&M Model. The D&M Model was thus intended to be "both complete and parsimonious" and, as such, has proved to be widely used and cited by many researchers, with over 8,000 published citations to date according to Google Scholar. Figure 2 shows the DeLone and McLean Information System Success Model (DeLone and McLean, 1992).

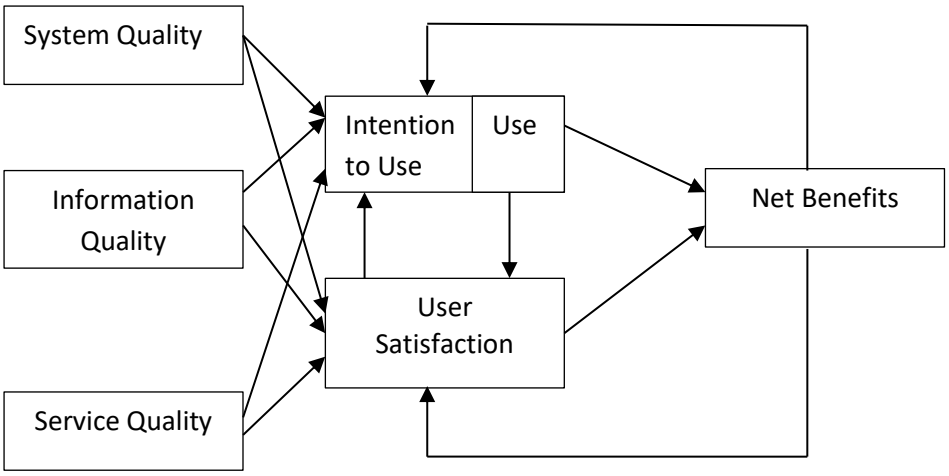

Figure 2. Information System Success Model by DeLone and McLean (2002, 2003

DeLone and McLean, (2002, 2003), adding the variables "Intention to Use" and "Service Quality, collapsing "Individual Impact" and "Organization Impact" into "Net Benefits," and adding feedback loops from "Net Benefits" back to "Use" and "User Satisfaction".

Availability

Information Technology Security (ITSEC) identifies significant difference in the definition of the ICT security parameters. Availability in the context of information technology is the ability of a user to access information or resources in a specified location and in the right format (Tantua & Alalibo, 2019). Availability is the only parameter where the prevention of the unauthorized users withholding is pertains to both information and to resources (Qaisar & Khawaja, 2012). Reference to the resources indicates that availability could not be considered in isolation, but one should always consider it in the context of a technology system that comprises computational resources, processes and humans except from information itself (Nwachukwu, 2014).

Information availability establishes a new standard for system and network that are always on for applications and data that are always available and for end users that are always connected (Nwachukwu, 2014). Availability of information also entails acquiring and also providing means by which users could get necessary information needed. The availability of information justified the existence of the repository or information center (Nwachukwu, 2014). Information Security revolves around the triad of information quality (CIA). CIA triad is the basic model of Information Security although, there exist other models that have the attributes of the CIA triad in common (Mir, et al., 2011). Availability was not considered important and worth of being a part of that document at that time. Recently in a paper, a spark was provided that got attention among the security stakeholders and practitioners towards the fact that Availability cannot be left out (Mir, et al., 2011).

Accessibility

Accessibility is the extent to which information is easily and quickly retrievable (Kadam, 2011). Information should be easy to obtain or access (Kadam, 2011). The measures of accessibility are

essentially, easily retrievable, easily accessible, easily obtainable and quickly accessible when needed (Liu, Yang,Bai, Wang, & Xiang, 2020). Accessibility in general term is used to describe the degree to which a system is useable by a wide range of users as possible. In other words, it is the degree of ease with which it is possible to reach a certain location from other locations. It is one thing for the resources to be available and it is another thing for it to be accessible. Whatsoever is available but not accessible is equally useless (Nwachukwu, 2014). Information system accessibility means advocated that information system should design to accomplish its object, to achieve the goal of the organization (Holmes, Pineres & Kiel, 2006).

Accuracy

Accuracy represents the legitimacy, precision and authenticity with which information is rendered (Ellis & Griffith, 2001). According to (Gill and Buyya, 2018), it is the legal liability issues associated with information stored in the database of the organization. Who is held accountable for the errors? Which party is liable for inexact or incorrect information that leads to devastation of another? (Hawedi, Talhi, & Boucheneb, 2018). It starts with identifying characteristics to check: authority, timeliness, quality, relevancy, and bias (Bell & Frantz, 2014). In some cases, older sources of information can still be sound 50 to 100 years later. Sources published recently tend to be more credible than older sources as new research is conducted. Accuracy also considered the more recent edition, grammar, spelling, and punctuation, the investigation of clarity, flow, and structure (Bell & Frantz, 2014).

METHODOLOGY

The research design adopted in this study is the Cross-sectional survey design. Structure questionnaire was based on the current trend on cloud network security tool (CNST) and management information systems success of civil servant in South-South, Nigeria. The respondents were selected from the six (6) states in South-South, Nigeria, using simple random sampling techniques. The data collected entails demographic profiles and data on cloud network security tool and management information systems success. The Spearman's rank order correlation statistics was used for data analysis.

DATA ANALYSES, RESULTS AND INTERPRETATION

Table 1: Respondent rate on Network Security Tool

	N	Min.	Max.	Sum	Mean	Std. Dev.
To what extent does the network security able to identify the misuse, modification denial of computer network and network accessible resource?	86	1.0	5.0	301.0	3.500	1.3526
To what extent does the network security able to authorization data modification?	86	1.0	5.0	348.0	4.047	1.5255
How effective is the network security able to distribute functions to the various users of the system.	86	1.0	5.0	305.0	3.547	1.4765
To what extent does network security able to carry out device configuration and other policy management in real time?	86	1.0	5.0	324.0	3.767	1.4687
Valid N (list wise)	86					

Source: Research survey, 2023

Table 1 showed that the management of civil service in South-South, Nigeria understand the important of cloud network security tool and are able to implement the security measures to a large extent. The various items analyzed were able above the criterion mean of 3.00 for a 5-point Likart scale.

Table 2: Respondents rate on Availability

	N	Sum	Mean	Std. Dev.
The information in the database are easily retrievable	86	354.0	4.116	1.5295
The information in the database are quickly accessible, there is a clear definition of its pathway.	86	350.0	4.070	1.2251
To what extent does the available information is also accessible to the authrorised users.	86	343.0	3.988	1.4832
How will you rate the facility or infrastructure for information accessibility?	86	363.0	4.221	1.2962
Valid N (list wise)	86			

Source: Research survey, 2023

Table 2 showed the respondent's rate on Availability the civil servant information system are always available for the right users as indicated on the table above. The various items testament were all able the criterion mean of 3.00 for a 5-point Likart scale.

Table3: Respondents rate on Accessibility

	N	Sum	Mean	Std. Dev.
How the store information is described as been legitimate based from the source	86	368.0	4.279	1.3690
To what extent does your data/information are precise to meet customers or client need.	86	289.0	3.360	1.2826
To what extent does the organization established policies to how accountable of inexact or incorrect information in the organization.	86	354.0	4.116	1.2595
To what extent does you organization established the characteristic to check the authority, timeliness, quality, relevancy, and bias	86	289.0	3.360	1.4706
Valid N (list wise)	86			

Source: Research survey, 2023

Table 3 showed that not only the information are available in the organizations database, they are also accessible by the right user even from remote distance as the various mean are above 3.00 (above average) for a 5-point Likart scale.

Table 4: Respondents rate on Accuracy

	N	Sum	Mean	Std. Dev.
To what extent does the information said to be consistent with input/out variables	86	365.0	4.244	.9195
To what extent does your data/information are precise to meet customers or client need.	86	324.0	3.767	1.2525
To what extent does the organization established policies to how accountable of inexact or incorrect information in the organization.	86	317.0	3.686	1.5128
To what extent does you organization established the characteristic to check the authority, timeliness, quality, relevancy, and bias	86	286.0	3.326	1.4262
Valid N (list wise)	86			

Source: Research survey, 2023

Table 4 showed that the information in the civil servants databases is accurate. The various items analyze were all above the criterion mean of 3.00 for a 5-point Likart Scale.

Bivariate Analysis

Table 5: Network Security and Availability

		Network Security	Availability
Network Security	Pearson Correlation	1	.619**
	Sig. (2-tailed)		.000
	N	86	86
Availability	Pearson Correlation	.619**	1
	Sig. (2-tailed)	.000	
	N	86	86

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Research data, 2023.

Table 5 showed the relationship between Network Security and Availability of Management Information System Success. The correlation coefficient shows that there is a strong relationship between Network Security and Availability of Management Information System Success in South-South, Nigeria. The correlation coefficient of 0.619 confirms the magnitude and strength of this relationship and it is statistically significant at ($\rho = 0.01<0.05$). The correlation coefficient represents a strong correlation between the variables. Based on the empirical findings, the null hypothesis **Ho_1** as stated earlier that; there is no relationship between Network Security and Availability of Management Information System Success in South-South, Nigeria is hereby rejected and the alternate hypothesis accepted. Thus, there is a strong relationship between Network Security and Availability of Management Information Management Success in South-South, Nigeria.

Table 6: Network Security and Accessibility

			Network Security	Accessibility
Spearman's rho	Network Security	Correlation Coefficient	1.000	.662**
		Sig. (2-tailed)	.	.000
		N	86	86
	Accessibility	Correlation Coefficient	.662**	1.000
		Sig. (2-tailed)	.000	.
		N	86	86

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Research data, 2023.

Table 6 showed the relationship between Network Security and Accessibility of Management Information System Success. The correlation coefficient showed that there was a strong relationship between Network Security and Accessibility of Management Information System Success in South-South, Nigeria. The correlation coefficient of 0.662 confirms the magnitude and strength of this relationship and it is statistically significant at ($\rho = 0.01<0.05$). The

correlation coefficient represents a strong correlation between the variables. Based on the empirical findings, the null hypothesis **Ho_2** as stated earlier that; there is no relationship between Network Security and Accessibility of Management Information System Success in South-South, Nigeria is hereby rejected and the alternate hypothesis accepted. Thus, there is a strong relationship between Network Security and Accessibility of Management Information Management Success in South-South, Nigeria.

Table 7: Network Security and Accuracy

			Network Security	Accuracy
Spearman's rho	Network Security	Correlation Coefficient	1.000	.636**
		Sig. (2-tailed)	.	.000
		N	86	86
	Accuracy	Correlation Coefficient	.636**	1.000
		Sig. (2-tailed)	.000	.
		N	86	86

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Research data, 2023.

Table 7 showed the relationship between Network Security and Accuracy of Management Information System Success. The correlation coefficient showed that there was a strong relationship between Network Security and Accuracy of Management Information System Success in South-South, Nigeria. The correlation coefficient of 0.636 confirms the magnitude and strength of this relationship and it is statistically significant at (ρ = 0.01<0.05). The correlation coefficient represents a strong correlation between the variables. Based on the empirical findings, the null hypothesis **Ho_3** as stated earlier that; there is no relationship between Network Security and Accuracy of Management Information System Success in South-South, Nigeria is hereby rejected and the alternate hypothesis accepted. Thus, there is a strong relationship between Network Security and Accuracy of Management Information Management Success in South-South, Nigeria.

CONCLUSION AND RECOMMENDATIONS

The literature reviewed and the result analyzed showed that is a significant positive relationship between cloud network security tool and management information systems success of Civil Servant in South-South Nigeria. It is cleared that cloud network security enhanced the accessibility, availability and accuracy of data/information stored in Civil Servant databases in South-South, Nigeria. Ministries that failed to implement this real time tool stand the change of losing their vital information to theft or unauthorized users. It is also necessary that before chosen any cloud organization, the network security strength must be put into consideration. The people doing business with the cloud service provider and the number of years they have been in operation will also give you better understanding of how security reliable their services provided. Civil Servant ministries in South-South, Nigeria that seek to improve the level of availability, accessibility and accuracy of information in their database should employ cloud network security tool.

REFERENCES

Achar, S. Patel, H. A. & Husain, S. (2022). Data security in cloud. A review. *Asian journal of advances in research, 17*(4), 76 – 83.

Bell, C., & Frantz, P. (2014). Critical evaluation of information sources. Retrieved: 15th May, 2023. From: http://library.uoregon.edu/guides/findarticles/ credibility.html

Bernstein, L. (2007). Network management isn't dying, it's just fading away‖, *Journal of Network and Systems Management* 15(1) 419-424

Bestman, E, A., & Alfred, I. (2022). Virtual Communication and Organizational Responsiveness of Indigenous Oil and Gas Companies in Rivers State. *International Academic Journal of Management and Marketing*, 7(1), 41 – 60.

Blum, M. & Schreiner, W. (2009). From IMS Management to SOA based Management. *Journal of Network and Systems Management*, *17*(1(), 33-52

Brandao, P. R. (2018). The Importance of Authentication and Encryption in Cloud Computing Framework Security. *International Journal on Data Science and Technology*, *4*(1), 1-5.

Delone, W. & Mclean, E. (2003). The Delone and Mclean Model of Information Systems Success. A Ten-Year Update. *Journal of Management Information Systems, 19*(4), 9 – 30.

Duan, Q. (2017). Cloud service performance evaluation status, challenges and opportunities. Survey from the system modeling perspective. *Journal of digital communication and network*, *3*(1), 101 – 111.

Ellis, T. S. & Griffith, D. (2001). The Evaluation of IT Ethical Scenarios Using a Multidimensional Scale. *ACM SIGMIS Database*, *32*(1) 75-85.

Gill, S.S. & Buyya, R. S. (2018). Self-protection approach in cloud resource management. *IEEE Cloud Computing*, *5*(1), 60–72.

Hawedi, M. Talhi, C. & Boucheneb, H. (2018)., Security as a service for public cloud tenants (SaaS). *International Symposium on Frontiers in Ambient and Mobile Systems*, 130, 1025–1030.

Holmes J, Pineres S & Kiel D, (2006). Reforming Government agencies Internationally: Is there a role for the balanced scorecard? *International Journal of Public Administration*, 29(1), 1125-1145.

Kadam, Y. (2011). Security Issues in Cloud Computing A Transparent View. *International Journal of Computer Science Emerging Technology*, 2(1), 316 – 322.

Kud, A. A. (2019). Substantiation of the term "Digital Asset": Economic and Legal aspect. *International journal of education and science, 2*(1), 33 – 44.

Lipi, A., Rahman, S. M. & Hasan, M. (2013). Information security in cloud computing. *International journal of Information Technology Convergence and Science, 3*(4), 13 – 22.

Liu, G., Yang, G., Bai, S., Wang, H., & Xiang, Y. (2020). A fast and accurate privacy-preserving multi-keyword top-k retrieval scheme over encrypted cloud data," *IEEE Transactions on Services Computing*, 2(1), 5 – 6.

Mell, P. & Grance, T. (2017). *Definition of Cloud Computing, National Institutes of Standards and Technology:* London, OReilly Media, Inc.

Mir, S. Q. et al. (2011). Information Availability: Components, Threat and Protection Mechanism. *Journal of Global Research in Computer Science, 2*(3), 21 – 26.

Mirrazavi, S. & Hashemzadeh, G.R. (2016). The Impact of Cloud Computing Technology on Organizational Performance; Financial, Customers, Operational (Case Study, Zarin Iran Percelean Industries). *Mediterranean Journal of Social Sciences*,*7*(4), 279 – 288.

Morf, M. E. & Weber, W G. (2000). I/O Psychology and the Bridging potential of A.N. Leon'ev's Activity Theory. *Canadian Psychology*, 81 – 93.

Nwachukwu, V. N. (2014). Availability, accessibility and use of information resource and services among seekers of Lafia Public Library in Nasarawa State, Nigeria. *Information and Knowledge Management, 4*(10), 1 – 12.

Oleg S., Haines, J., Lippmann, R., Wing, J. M. (2002). Automated generation and analysis of attack graphs. *In Proceedings of the IEEE Symposium on Security and Privacy*, 254– 265,

Qaisar, S. & Khawaja, K. F. (2012). Cloud Computing: Network/Security Threats and counter measures. *Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com*, 3(9), 1323 – 1329.

Sankaraiah, B., Bhadru, D., Kumar, G. S. (2017). A review on different Access Contol mechanism in cloud environment. *International journal of computer science and engineering, 5*(2), 122 – 224.

Simarjeet, K. (2012). Cryptography and Encryption in Cloud Computing, *International Journal of Computer Science and Information Technology*, *2*(3), 242-249, 2012.

Tantua, E., & Alalibo, O. O. (2019). Data Protection and Information Management Success of Tertiary Institutions in Rivers State, Nigeria. *RSU Journal of Office and Information Management, 3*(1), 1-17. 2019. www.rsujsib.com

Verinikina, I. (2001). Cultural-historical psychology and activity theory in everyday practice. In Hasan, H. Gould, E., Larkin, P. & Vrazalic L. (Eds.), *Information Systems and Activity Theory*, Wollongong, University of Wollongong Press, 2, 23 – 38.

Yang, B. Tan, F., Dai, Y. S. & Guo, S. (2009). Performance evaluation of cloud service considering fault recovery. *IEEE International Conference on Cloud Computing*, 571– 576.

Yausef, A. B., Mjlae, S. A., Abu-Ulbeh, W., Hassan, A. H. (2020). The Effectiveness of Management Information System in Decision-Making. *Journal of Mechanics of Continua and Mathematical Sciences, 15(*7), 316 – 327.

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. Proceedings of the 29th IEEE *International Conference on Information Communication*, 534-542.