TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

Cloud Accounting: A Risk Mitigation Perspective

Syed Abdullah Shah
Research Scholar,
Asia Pacific University of Technology & Innovation, JalanTeknologi 5
57000 Wilayah Persekutuan Kuala Lumpur, Malaysia.
syedabdullahshah1997@gmail.com

Geetha A. Rubasundram
Senior Lecturer,
Asia Pacific University of Technology & Innovation, JalanTeknologi 5
57000 Wilayah Persekutuan Kuala Lumpur, Malaysia.
geetha@apu.edu.my

Article Info
Volume 82
Page Number: 1119 - 1128
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *06 January 2020*

Abstract
Modern businesses are moving towards Cloud based applications due to the flexibility, cost effective and business sense. However, there has been a noted hesitation by firms to migrate towards Cloud Accounting. This research aims to explore the reasons behind this reluctance by identifying the major risks that are preventing firms from embracing Cloud Accounting and recommending measures to mitigate the risks. This study deploys a qualitative approach to explore and understand the specific problems and solutions by interviewing Cloud Accounting experts internationally. The findings of this research suggest that Cloud Accounting provides unique features like the global network access, scalability, automation, ERP integration and enhanced measures of security at a fraction of the cost in comparison to the traditional AIS. However, organizations hesitate to embrace the Cloud Accounting services because of the lack of awareness about the concept, threats to data security because of the distributed nature of Cloud infrastructure, short lived business lives of Cloud vendors, and the dependency relation customers fall into because of the lack of transparency. The research believes that these risks are caused by lack of governance, compliance and audit in enterprise risk management framework, which if brought in place will mitigate the identified risks. This study aims to motivate more users to embark onto the Cloud Accounting platformto enjoy the benefit of this business enhancing technology.

Keywords: *Cloud Computing, Cloud Accounting, Enterprise Resource Planning (ERP), Accounting Information Systems (AIS), Enterprise Risk Management Framework*

I. Introduction

Cloud Accounting, a subset of the more popular Cloud Computing has suffered a relatively slow start. Cloud Accounting is seen as a by-product of the Industrial Revolution **(Tugui & Gheorghe, 2014).** Cloud Accounting reflects the characteristics of Cloud Computing, but from an accounting perspective**(Prichici & Ionescu, 2015)**.It provides an all-time access since the accounting data and the related applications are stored on cloud based servers that can be accessed at any time using the internet. The move from traditional accounting platforms to the more sophisticated cloud based platforms provides numerous benefits to an organization such as flexibility, cost savings, competitive advantage, global network access and reduced

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

carbon footprint of the business owners **(Arsenie-Samoil, 2011)**.

Cloud Accounting has transformed the business models of firms. Previously, with the traditional accounting software, a firm faced limitations whereby if it had a new business or channel, it may have to buy separate hardware and software ensuring it'scompatibility with its current technology with possible issues of integration. Currently, cloud financial services provider like Xero or Oracle provide flexible options for business owners to start their new services or business within minutes due to the service facility platform **(Khanom, 2017)**.

Therefore, it is rather surprising that the market for Cloud Accounting has been rather slow. The Cloud Computing market is expected to grow from USD 272 billion in 2018 to USD 623.3 billion in 2023, a staggering 229% growth over a period of five years (**Business Wire 2019).** In contrast, less than 30% of accountants and business owners intend to migrate their accounting work to the Cloud **(Dimitriu & Matei, 2015)**, with the lack of information and research on the risk and threats of Cloud Accounting being a major contributing factor **(Christauskas & Misevicience, 2012)**.

Just like any other technology, Cloud Accounting would revolve around the typical people, process and technology platform within its commercial environment. This would inherently expose it to various types of fraud including but not limited to risk of cybercrime, policy risks, organizational risks, technical risks, legal risks and other risks that give rise to security issues and open threats to the Cloud's cyberspace. An added concern is that Cloud Accounting being a web based service could also limit the end user's physical control over security which may lead to vulnerabilities. In the cyber realm, a vulnerability is a weakness which can be exploited by a threat actor, such as hackers, to perform unauthorized actions within a computer system.

Recent cases on cloud based applications have added on the concerns of end users of the security and integrity of their data. High profile mishaps on cloud based apps such as the recent leaks of the Amazon Simple Storage Service (S3) buckets impacted companies like Verizon, Pentagon, Pocket iNet, Deep Root Analytics and many more, affecting the personal data of hundreds of millions of users **(Okoampa-Larbi, et al., 2017).**

Therefore, this research aims to assess the types of risk that could impact users of Cloud Accounting, taking into account the concepts and characteristics of the platform and to further understand the relevant risk mitigation techniques. There has been a noted lack of research in the area of Cloud Accounting. However, due to the similarities between Cloud Accounting and Cloud Computing, research and references from Cloud Computing would be used to form the basis of discussion where relevant.

Factors Affecting Cloud Accounting Adoption

The process of traditional accounting information systems has been replaced with digital applications, in which information and communication technologies such as electronic data exchange, electronic fund transfer, internet, intranet, extranet, expandable formatting language, expandable business reporting language, relational database management systems, and web tools are used, and the works are carried out in integrated database and web platform in integrated way **(Allahverdi, 2017)**.

The concept "Cloud Computing" emerged with the development and spread of internet and mobile technologies, presents new solutions to the public and private sector and brings an obligation to go toward change in the styles of doing business. Cloud Computing is expressed simplyas the resources and services provided through the internet. The reason for using the word Cloud is that service is provided through internet that is an invisible network **(Boomer, 2013)**. Cloud

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

computing is a concept that is a basis of the share of information and hardware. Cloud computing, which makes this sharing from the service – oriented architecture, on which virtualizing, network, and web software services are built, includes reduced information technologies for the final user, flexibility, reduced cost, services on demand, and many other things. The desire of accounting to utilize the advantages presented by Cloud Accounting and desires of especially large companies to move their work areas to internet led cloud computing firms giving service in accounting area to emerge.As Cloud Computing innovations focus on fast-paced and effective delivery of services to the business environment (and especially the financial accounting field), companies and management service providers (MSP) face radical changes in terms of information technology. Thus, most companies are moving towards a virtually private data center (Private Cloud) in order to maximize application efficiency and reduce server downtime.

A cloud service provider's infrastructure carries consolidation of multiple organizations' high level of confidential data and valuable financial information, which according to **(Eaton, et al., 2019)** makes it a more attractive target for hackers as compared to a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a cloud service provider solution in most cases are higher with respect to confidentiality and data integrity. This is further aggravated in a consolidated cloud infrastructure as the data is under the control of a third party and promotes resource sharing amongst corporate and individual users, increasing risks of data leakage and its subsequent impact on privacy and confidentiality obligations **(Mahesh, 2016)**..

The CIA model is designed to guide policies regarding the confidentiality, integrity and availability of data, for the organizations information security platform. A private data is confidential property of one, and an unauthorized access to someone's data causes loss of confidentiality **(Shankarwar & Dr. Pawar, 2015)**. Modification of data in an unpredicted way and without the knowledge of the owner, is called as loss of integrity. When data is lost or become inaccessible, this situation is called "loss of availability". According to **(Fatima & Yeh, 2012)**, all these losses can make a big impact on the web-based Cloud specially if the data is of financial or accounting nature as it is the core information for any business process. Data integrity is the assurance that digital information is not corrupted and only be accessed by the authorized users. So, integrity involves maintaining the accuracy, consistency and trustworthiness of data over its entire life cycle. CIA triad can be easily maintained in a standalone traditional accounting processing system with proper security measures in enterprise computing environment. However, in Cloud based accounting systems, additional efforts to protect data is required due to the distributed nature of the infrastructure and multi-tenant architecture of the Cloud computing.

All organizations should have policies to establish controls to prevent and detect the unauthorized procurement and use of Cloud services, regardless of management's position on venturing into Cloud contracts. The CSCC *Security for Cloud Computing*, prescribes a series of steps to evaluate and manage the security of their Cloud environment with the goal of mitigating risk, which will be used as the bases to recommend techniques for risk mitigation as these are the only official prescription available till date **(CSCC.org, 2017)**

Most risks associated with cloud platform are caused by loopholes that exist in the complete system arising from the lack of proper governance and compliance being attributed to this innovation. Cloud governance is a part of IT governance which is a subset of the corporate governance that involves having a solid integration between

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

people, process and technology. A major challenge to IT governance in Cloud network is the management of the Cloud environment and the Cloud service providers control over it as the fundamentals of successful deployment; people, process, and technology are all not in CSP's hand. One of the major aspects of Cloud governance, which is security management, remains a major challenge for Cloud service users. Based on a survey among 565 IT managers across US and Canada, 62% participants responded that they are interested in shifting their business on Cloud because of its enormous benefits. However, they are concerned about security, privacy, location of server and compliance. Mimecast (2009) to mitigate these potential risks of extending governance to the Cloud paradigm, organizations should put in place and sustain a practical governance framework to ensure Cloud infrastructure and operations are as secure as traditional IT governance approaches.

Depending on the processes Cloud is supporting, security and retention issues can arise with respect to complying with regulations and laws such as the Sarbanes-Oxley Act of 2002 (SOX), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the various data privacy and protection regulations enacted in different countries. Examples of these data privacy and protection laws would include the USA PATRIOT Act, the EU Data Protection Directive, Malaysia's Personal Data Protection Act 2010, and India's IT Amendments Act. In the Cloud, data is located on hardware outside of the organization's direct control. Depending on the Cloud solution used (SaaS, PaaS, or IaaS), a cloud customer organization may be unable to obtain and review network operations or security incident logs because they are in the possession of the cloud service provider. The cloud service provider may be under no obligation to reveal this information or might be unable to do so without violating the confidentiality of the other tenants sharing the Cloud infrastructure. Therefore, there can be many issues that may demotivate firms from embarking on the cloud accounting journey. However, there could already be solutions in place that could mitigate these concerns and risks.

II. Research Methodology

Due to the level of expertise and depth that is required to assess the objectives of this research sufficiently, a qualitative research will be carried out. The primary data in the study will be collected via having semi-structured interviews in which open ended questions will be asked to the participants. The target population for the purpose of interviews will consist of Cloud experts, Cloud service providers and Cloud service users internationally. The respondents were made aware of the pre-requisite that they needed to have practical and in-depth knowledge of cloud based apps, cloud based accounting, benefits, challenges, risks and other governance or compliance issues. The population of Cloud experts is relatively unknown. However, the researcher used various keywords to search for such experts using business networks online. The researcher approached 30 such experts internationally. However, only 15 agreed to the interviews as the rest were unsure of the discussed scope. Out of the 15, this research only included the results of the interview with 9 of the experts, as the remaining 6 responses were incomplete or insufficient to add value to the scope.

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

III. Research Framework

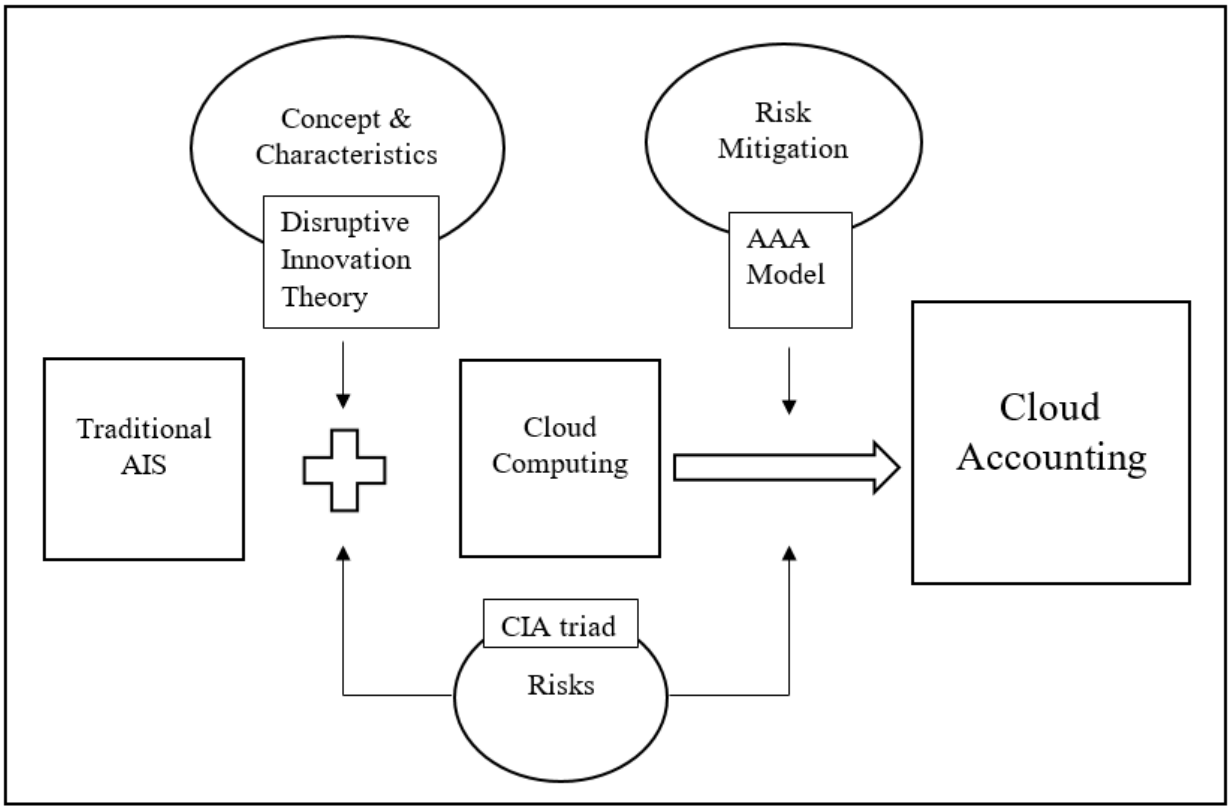

Figure 1: Research Framework (Self Authored)

Analysis& Discussion

The following illustration is a layout of the basic demographical information of the respondents collected prior to conducting the interview session. Variables include the gender, profession, and experience of the respondents in the respective field.

Variables	Frequency (n)	Percentage (%)
Gender		
Male	7	77.8%
Female	2	22.2%
Profession		
Cloud Accountant	1	11.1%
Cloud Service Provider	4	44.4%
Cyber Service User	3	33.3%
Cloud Academic Practitioner	1	11.1%
Experience		
Less than 5 years	2	22.2%
5 – 10 years	2	22.2%
10 – 15 years	4	44.4%
More than 15 years	1	11.1%

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

Countries		
Malaysia	3	33.3%
Pakistan	2	22.2%
Dubai	2	22.2%
Singapore	1	11.1%
Qatar	1	11.1%

Table 1: Profile of Respondents

Table 1 provides the profile of the respondents and reflects the hands on knowledge of the practitioners to answer the questions. Overall, the The initial questions for the interview revolved around the concept and characteristics of the Cloud Accounting platform which would motivate the adoption of the platform. Some of the unique characteristics highlighted included the global network access, scalability and flexibility of using the service infrastructure, enhanced security measures with backup data as to avoid any data loss, pay-per-use method of payment which is relatively cheaper leading to cost savings. Cloud AIS does not require upfront infrastructure costs or hardware and software maintenance costs.This is the greatest motivator driving the adoption levels in SMEs since the firms do not have the resources to have an on premise accounting network **(Cunha, et al., 2017).** The respondents also noted that although the shorter term tactical cost savings were a great motivation, there were also longer term strategic values which impacted the speed time to market or deal with real time information, scalability of the service, broad network access, pay-as-per-use, enhanced security measures, auto backup and reconciliation of the data creating value for money.

The second characteristic of Cloud Accounting that prominently stood out amongst the respondents was the automation and integration of the firm's business process, which would lead to enhancing the accuracy, consistency and integrity of the accounting process. Since the cloud based apps works on fixed algorithms, it is assumed that it would be able to carry out repetitive tasks more efficiently and producing error free results. Cloud Accounting automates the complete business process by providing software solutions for process and plant automation, factory and manufacturing automation, inclusive of manufacturing execution systems, and also machine control and integration which is also supported by the study of **(Xue & Xin, 2016)**.

respondents provided consistent answers to the fifteen questions posed.

When discussing about the risks, the respondents consistently highlighted the issue of data integrity, which is the biggest challenge for a Cloud Service Provider and concern for the Cloud Users. The cloud infrastructure does not only store data but also serves as a platform for data in transit, data in process and when such a huge number of data is being updated or changed in the server every second, ensuring that the data stays in its original state. This is crucial since in a consolidated structure and shared resources, the data is under the control of third parties which increases the vulnerability of data loss and leakage **(Ahmed & Hossain, 2014)**. The respondents emphasized that the existence of any flaw or malware in the database of one user can infect the security and integrity of other user's data, if the infrastructure is not properly segregated or silo based. In contrast to the standalone accounting system, more effort is required to protect data in Cloud Accounting due to the nature of the distributed infrastructure. The added complexity of the international network and on such a large scale makes it difficult for a cloud service provider to

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

perhaps apply updated and consistent measures across the systems. When hosting a network shared among hundreds of organizations it is very difficult to maintain theCIA triad because inside an organization the data rotates within an organization and the team maintaining the data has to assure that the data and the system is available for the use of the employees of that company only. However, the Cloud vendor has to assure that the customer's data remains confidential and accessible by that customer only **(Ahmed, et al., 2017)**.

Cloud Accounting is relatively new, with the service providers largely being start up's or new entrants to the market. This in turn creates skepticism and trust issues pertaining to the going concern of these firms. The respondents emphasized that the cloud vendor's projected longevity is consistently brought up by potential new customers prior to signing on a cloud based service as they are concerned about the potential disruption. Apart from the disruption faced, transition costs and other complexities were also risks that were highlighted in relation to the above point. However, there is a diminishing trend in these worries since many of the cloud service providers had already matured into the market, recording at least five years of experience and growth.

The respondents also conclusively recommended various governance and compliance measures to mitigate risks for a successful cloud deployment. Governance standards provide framework for security controls assessments and authorization, which acts as a shield against the myriad threats enterprises are exposed to in a cloud based system. Governance also ensures that the necessary controls or security measures to safeguard the data stored are in the correct place and the procedures are under continuous supervision and controlled source code ensuring that the system remains free from any bugs and as long as the system is free from bugs the chances of risk occurrence are very low. Moreover, IT governance is also the key to information management function which is crucial for avoiding risk occurrence. Regulatory compliance ensures risk reduction by the cloud service provider by ensuring that they conforms to the rules and laws to protect the confidentiality and integrity of customer data. The respondents also recommended the use of cloud management audit which would provide users with an assessment of the cloud service provider's internal controls and security measures. This would also provide further reliance that the data is properly segregated and maintained in the server, with proper measures in place to ensure any deficiencies or vulnerabilities are mitigated in a timely manner.This provides the Cloud Accounting customers with an assurance that their data will be safe with the Cloud vendor by determining whether Cloud service provider's internal controls protect corporate customer's data asset, data integrity and whether such measures are aligned with the business's overall goals. All of the respondents even suggested that before embracing the technology it is essential for a customer organization to make sure that the Cloud vendor is certified from an independent third party audit entity as it provides an assurance of their effectiveness. Although there are best practices of governance and IT Audit standards that IT firms have to comply with. One thing that the researcher explored during the interview season was that there are actually no obligatory requirements for the Cloud companies yet to get certified from a standardization organization, neither is there any regulatory compliance provisioned specifically for Cloud information systems from the professional bodies of accountancy.

The respondents also stringently recommended the implementation of strict identity and access controls (example two-factor authentication) to prevent data breaches and leakages. Client firms are strongly concerned about the strength and security of the network applications. The main

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

cause of unauthorized access is that the passcodes leading to the network are weak and can be easily trespassed. Even if the service provider's security controls are on point and a hundred percent safe, data can be leaked if the password of the user gets leaked in such security gap with the two factor authentication it is near to impossible to imitate anyone's fingerprint or eye retina print, and this way the data remains safe from the intruders.

The respondents also called to attention that organizations spend enormous amounts of time, energy, and resources selecting the right cloud providers, but do not spend sufficient time creating a cloud exit strategy if things don't go as planned. Some call it "reverse migration" or "unClouding." Put simply, a Cloud exit strategy is exactly as it sounds, a plan to ensure the Cloud services that support your business activities can be replaced efficiently and without disruption **(Opara-Martins, et al., 2017)**. According to the interview participants a healthy exit process is one of the most important measures to mitigate risk as an exit process ensures that any data of the client stored on the CSP's server is to be permanently deleted and cleaned from the database server after handing over customers the only backed up copy of their data. This not only secures the firm's data but also ensures a smooth transition.

IV. Conclusion

The research explored the exclusive features of the Cloud Accounting technology that the traditional accounting systems lacked which will motivate firm's to take the swift shift. Global network access, scalability and flexibility of using the service infrastructure, enhanced security measures with backup data as to avoid any data loss, pay-per-use method of payment which is relatively cheaper leading to cost savings, being a few of them. Additionally, while exploring the differentiating characteristics of Cloud Accounting, the research also identified cost savings as the main element which drives its adoption among SMEs, while larger organizations pursue Cloud Accounting because of all those features like the global access, wide integration and strong security measures which will enhance their overall business efficiency. The respondents also asserted the various benefits in place, including the shorter term tactical and strategic based advantages. This also included the attribute of automation in enhancing the accuracy and consistency in the accounting process. The identification of risks dimensions such as data segregation and isolation, information security and data privacy requirements, service reliability and uptime, disaster recovery, control over quality, cross level compatibility and integration, lack of visibility and complexity in ensuring compliance. The interview extraction showed that assuring data integrity is one of the biggest challenges for a cloud service provider because a Cloud vendor's infrastructure carriers consolidation of multiple organization's high level of confidential and valuable financial data, and in such a consolidated infrastructure a flaw in one user's database can severely affect other's data stored in the same Cloud server if it lacks proper segregation which is probably the most critical concern of Cloud clients as they hold little or no insight on the storage locations of their data and the provision used to segregate their data from other's data impacting the CIA Triad. The concern that the cloud based vendors are short term start-ups was also assessed, however, the respondents disputed this saying that many vendors have been in the industry for more than five years. Governance, compliance and audit trials can be a major key in reducing the chances of risk occurrence. Governance standards provide framework for security controls assessments and authorization, which acts as a shield against the myriad threats enterprises are exposed to in a Cloud system enabling an effective and efficient use of the technology. Governance also ensures that the necessary controls or security measures to safeguard the data stored are in the correct place

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

and the procedures are under continuous supervision and controlled source code ensuring that the system remains free from any bugs hence, decreasing the chances of risk occurrence. Regulatory compliance can ensure risk reduction by CSP conforming to the rules and laws regarding the protection of the customer data with full confidentiality and integrity. It ensures that the CSP is taking aspiring steps followed with a risk-based approach to comply with laws like the; data protection law, data localization law and so on. The respondents also recommended cloud management audit to assess the quality of controls and security in place. The controls include the salient feature which is commonly known as two factor authentication login and requires the users to use their password and finger print or eye scan to access the data. Unlike numeric or alphabetical passwords, imitating finger print or retina scan is near to impossible which reduces the unauthorized access to the data leading to reduced data breaches. One crucial strategy in the service level agreement which can be a key to prevent data breach, known as the exit strategy which ensures the customers a smooth transition without the loss of data at the end of the service relation was also a major highlight amongst the respondents.

Hence, it can be summarized that Cloud Accounting is a robust mechanism that can be advantageous to firm's regardless of size. The lack of information and awareness possibly amongst firms and the executives could be the cause of the slow adoption. Cloud vendors should further market the strategies in lieu of the regulatory compliances as that would provide further trust in moving a to a more cloud based server since all other factors seem to be logical advantages.

References

[1] Ahmed, H. A., Ali, M. H. & Kadhum, L. M., 2017. A Review of Challenges and Security Risks of Cloud Computing. *Journal of Telecommunication, Electronic and Computer Engineering*, 9(1-2), pp. 87-91.

[2] Ahmed, M. & Hossain, M. A., 2014. CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD. *International Journal of Network Security & Its Applications (IJNSA)*, 6(1), pp. 25-36.

[3] Allahverdi, M., 2017. Cloud Accounting Systems and A SWOT Analysis. *Journal of Applied Sciences and Technologies*, 6(4), pp. 81-93.

[4] Arsenie-Samoil, M. D., 2011. Cloud Accounting. *Ovidius University Annals: ECONOMIC SCIENCES SERIES*, 11(2), pp. 782-787.

[5] Boomer, J., 2013. Global Perspectives on Accounting İnformation Systems: Mobile and Cloud Approach. *Procedia Economics and Finance* , Volume 20, pp. 88-93.

[6] Christauskas, C. & Misevicience, R., 2012. Cloud -Computing Based Accounting for Small to Medium Sized Business. *Journal of Applied Accounting* , 13(2), pp. 357-369.

[7] CSCC.org, 2017. *Cloud Standards Customer Council: Security for Cloud Computing Ten Steps to Ensure Success Version 3.0.* [Online] Available at: https://www.omg.org/cloud/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf [Accessed 19 May 2019].

[8] Cunha, C. R., Morais, E. P., Sousa, J. P. & Gomes, J. P., 2017. The Role of Cloud Computing in the Development of Information Systems for SMEs. *Journal of Cloud Computing*, Volume 2017, pp. 1-7.

[9] Dimitriu, O. & Matei, M., 2015. Cloud Accounting: A New Business Model in a Challenging Context. *Procedia Economics and Finance*, Volume 32, pp. 665-671.

[10] Eaton, T. V., Gremier, J. H. & Layman, D., 2019. Accounting and Cybersecurity Risk Management. *American Accounting Association Journal*, 12(2), pp. 1-18.

[11] Fatima, A. A. & Yeh, C.-L., 2012. Cloud Computing: Overview and Risk Analysis. *Journal of Information Systems*, 26(2), pp. 13-33.

[12] Khanom, T., 2017. Cloud Accounting: A Theoretical Overview. *IOSR Journal of Business and Management*, 19(6), pp. 31-38.

January - February 2020
ISSN: 0193 - 4120 Page No. 1119 - 1128

[13] Mahesh, B., 2016. DATA SECURITY AND SECURITY CONTROLS IN CLOUD COMPUTING. *International Journal of Advances in Electronics and Computer Science,* 3(Special), pp. 11-13.

[14] Okoampa-Larbi, R., Twum, F. & Hayfron-Acquah, J. B., 2017. A Proposed Cloud Security Framework for Service Providers. *International Journal of Computer Applications,* Issue 1, p. 158.

[15] Opara-Martins, J., Shahandi, R. & Tian, F., 2017. A Holistic Decision Framework to Avoid Vendor Lock-in for Cloud SaaS Migration. *Journal of Computer and Information Science,* 10(3), pp. 29-53.

[16] Prichici, C. & Ionescu, B. S., 2015. Cloud Accounting - A new paradigm of Accounting Policies. *SEA - Practical Application of Science,* 3(1), pp. 489-496.

[17] Shankarwar, M. U. & Dr. Pawar, A., 2015. Security and Privacy in Cloud Computing: A Survey. *Advances in Intelligent Systems and Computing,* Volume 2, pp. 1-11.

[18] Tugui, A. & Gheorghe, A.-M., 2014. Changing The Role Of Accountancy In The Context Of Cloud-Computing. *Management Intercultural Journal,* Issue 31, pp. 149-157.

[19] Xue, C. T. S. & Xin, F. T. W., 2016. BENEFITS AND CHALLENGES OF THE ADOPTION OF CLOUD COMPUTING IN BUSINESS. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* , 6(6).