ISSN 2278-3083

Volume 8, No.6, November –December 2019

International Journal of Science and Applied Information Technology

Available Online at http://www.warse.org/ijsait/static/pdf/file/ijsait24862019.pdf

https://doi.org/10.30534/ijsait/2019/248620198

An Infrastructure as a Service Accountability Requirements for Big data: An Interview Study

Hamzeh Alabool[1], Deemah Alarabiat[1] , Laith Abualigah[2], Mohammad Al Shinwan[2], Ahmad Khasawneh[2], Mohammad Shehab[3]

[1]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Abha, Saudi Arabia

[2]Faculty of Computer Sciences and Informatics, Amman Arab University, Amman, Jordan

[3]Computer Science Department, Aqaba University of Technology, Aqaba 77110, Jordan

ABSTRACT

Organizations seek to employ the power of big data (BD) to improve their decision-making and biasness process. Infrastructure as a service (IaaS) enabling them to take advantage of BD. However, increasing the acceptance of BD is difficult due to common issues such as accountability of cloud providers. Securing BD has its own distinctive challenges that are not profoundly different to traditional data. This paper tends to identify and develop an accountability model based using interview study. The study aims to explore the new Accountability Control Areas (ACAs) and Accountability Control Criteria (ACC) that can influence the overall Accountability degree for BD processing over IaaS cloud. The analysis results brought out three ACAs and fifteen ACC.

Key words: Big Data, Infrastructure as a Service; Accountability Control Areas; Accountability Control Criteria, Interview Study.

1. INTRODUCTION

IaaS cloud is very well known as a critical IT resource for organizations that seek to harness the power of big data analyst (BDA) to improve their decision-making. Its importance lies in allowing organizations to scale up or scale down IT infrastructure properties (such as memory storage, CPU) according to their demands. Additionally, the adoption of IaaS cloud could help organizations to save unnecessary expenditure on buying, managing and upgrading IT resources for BD and BDA processing and managing. The use of IaaS cloud play a vital role in shifting the responsibilities of buying, controlling and maintaining of the infrastructure or /and software are shifted from organizations to cloud providers. This will help organizations to focus more on their core business and leaving many IT-related activities to be handled by cloud providers.

However, even though IaaS cloud open new opportunities that are too attractive for processing and managing BD, but this shift is not free of challenges, where the issue of trust between organizations and IaaS cloud providers are critical [1] and [2]. Accountability is one of the most trust control elements that influence the trust degree between IaaS cloud provider and IaaS cloud users [4] and [5]; lack of IaaS cloud provider accountability has corroded public respect for business leaders. Moreover, neglecting this control element will effect badly on the trust relationship and it may lead to break the trust between those parties. Therefore, IaaS cloud providers have to put cloud users in a position where they can trust them. IaaS cloud providers should offer their assurance capabilities beyond the functional properties (e.g., performance, availability and cost) of cloud. For example, they have to offer assurance on different control areas and criteria of Accountability. For IaaS cloud providers, fulfilling the assurances on these ICAs and ICC is difficult unless it is to identify and define the basic accountability requirements that important to maintain the accountability within IaaS cloud.

The main contribution of this study is in identifying and defining set of ACAs and ACC that influence the Accountability of IaaS and that will enhance the level of trust between IaaS cloud providers and users . To do so, qualitative expert interview study on the IaaS cloud accountability requirements (e.g., ACAs and ACC) has been conducted to answer and investigate the following research questions:

- What are the main accountability control areas and accountability control criteria that can influence the overall accountability degree within IaaS cloud?
- How accountability can be guaranteed within IaaS cloud?

In this paper section 2 discussed the background literature in relation to accountability. While, section 3 describes the research methodology used in this study. Sections 4 present the results of the study and answer the research questions respectively. Finally, section 5 presents the conclusions and further work.

2. THEORETICAL

Accountability is a trust control element. It refers to the holistic approach that includes policies, practices, procedures and responsibilities that aim to keep track of IaaS cloud provider internal and external actions. [12] Defined accountability as the *"obligation of an entity to explain how it has acquitted itself of certain responsibilities or why it was act in a certain way"*. According to [11] there are four types of accountability, which are hierarchical, legal, professional and political.

Many different researches ensured that accountability has a significant impact in forming trust. For example, a review that has been conducted by [6] on trust and reputation for web service selection found that accountability is one of the main criteria that used to evaluate trust level. [7] Selected accountability as a key criterion to evaluate trusted computer systems. Furthermore, [8] mentioned that accountability is one of the engineering conditions for cultivating trust online. Other optimization techniques can be used [24-30].

In the domain of cloud computing, [9] discussed that *"accountability is a group of QoS attributes is used to measure various cloud provider specific characteristics. This is important to build the trust of a customer on any Cloud provider. No organization will want to deploy its applications and store their critical data in a place where there is no accountability of security exposures and compliance"*. In IaaS cloud context, lack of transparency and less control over data are the main concerns of cloud users. Such concerns will lead to lack of cloud user‘s trust. [10] pointed out that accountability as one of the most important key performance indicators that should be considered by users when they measure the properties related to the service provider organization. This is because accountability includes policies, practices and procedures as well as assigns the responsibilities of IaaS cloud providers to keep track their internal and external actions.

Accountability as a term cannot give complete details about a property of an entity in an IaaS cloud for BD and BDA activities; it only provides a general description. Therefore, accountability control areas and accountability control criteria have to be identified in order to give more descriptions and details about the property of an entity in IaaS cloud. To do so, two interview questions have been developed to explore these accountability control areas and accountability control criteria.

- What are the main accountability control areas and accountability control criteria that can influence the overall accountability degree within IaaS cloud?
- How accountability can be guaranteed within IaaS cloud?

3. METHODOLOGY

Semi-structured interview (open-ended questions) selected as the main instrument for data collection from the target respondents. Semi-structured interview allows respondents to share their experiences about what are the accountability criteria that influence the use of IaaS cloud for BD purposes. This will help to discover a complex set of ACAs and ACC surrounding Accountability in IaaS cloud from multiple perspectives. For data collection, 10 respondents were interviewed from 4 identified IaaS cloud providers. According to Guest et al in [15] "A sample of six interviews may [be] sufficient to enable development of meaningful themes and useful interpretations". In addition, [16], [17] and [18] suggested (6-10), (6-8) and (5- 25) respondents in phenomenological research respectively. These 10 respondents are highly experienced in their area. The respondents IaaS experiences included solutions engineer, system administrator, technical seals, engineering consultant and technical solutions. The current activates involvement of respondents included IaaS security and networking, two respondents involved in IaaS requirements engineering, IaaS cloud auditing, IaaS cloud evaluation criteria definition, IaaS cloud integration, and technical sales. The Combination of different IaaS cloud experiences with different activities involvement aided to gather rich data that show the opinions of different perspectives.

In this research, qualitative content analysis is used to analyze qualitative data (e.g., interview transcripts). Hsieh and Shannon in [19] explained content analysis as an analytic method for identifying, analyzing and reporting patterns within qualitative data. This research employed directed content analysis [19]. The main strength of directed content analysis approach to qualitative data analysis is that existing theories and/or existing research findings can be supported and extended [19], [20] and [21]. Therefore, this research seeks to extend accountability to IaaS cloud for BD context by identifying the ACAs and ACC that influence Accountability degree within IaaS cloud. In this paper, the analytical approach introduced by [19], [20], [21] and [22] was used to analyze the qualitative data.

4. RESULANTS AND DISCUSSION

The analysis results brought out that accountability could be divided into 4 TCAs, namely: auditability, compliance, governance and locality. These ACAs of accountability along with their ACC are shown in Figure (I) and discussed in the following subsequent sections.

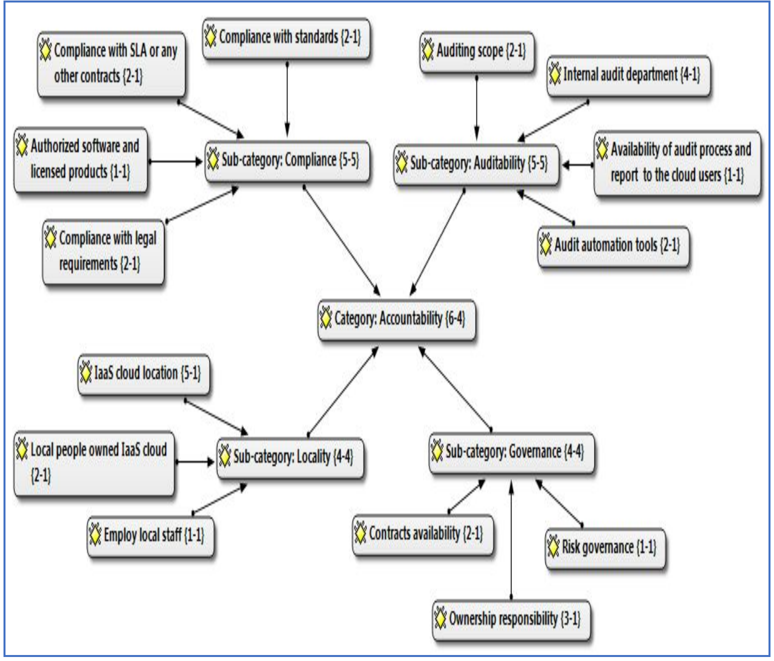
Compliance with SLA or any other contracts {2-1}
Compliance with standards {2-1}
Auditing scope {2-1}
Internal audit department {4-1}
Authorized software and licensed products {1-1}
Sub-category: Compliance {5-5}
Sub-category: Auditability {5-5}
Availability of audit process and report to the cloud users {1-1}
Compliance with legal requirements {2-1}
Audit automation tools {2-1}
Category: Accountability {6-4}
IaaS cloud location {5-1}
Local people owned IaaS cloud {2-1}
Sub-category: Locality {4-4}
Sub-category: Governance {4-4}
Employ local staff {1-1}
Contracts availability {2-1}
Risk governance {1-1}
Ownership responsibility {3-1}

Figure I: Trust Criteria In Context-Based Cloud

1. Auditability

Auditability is a sub-category of accountability. It refers to the process of auditing all IaaS cloud assets against a set of rules and/or standards. It is important to prove that all IaaS cloud assets do not do anything beyond their tasks. Therefore, this is considered as adequate evidence for cloud users to verify that IaaS cloud provider has fulfilled their promise. In this way, the concern regard IaaS cloud transparency will be reduced and this will contribute to increase trust level. The findings brought out that auditability could be divided into 4 TCC, namely: internal audit department, audit automation tools, auditing scope and availability of the audit process and report to the cloud users.

2. Compliance

Compliance is a sub-category of accountability. It refers to verifying the commitment of IaaS cloud providers to follow specific legal requirements, standards, contracts and policies. Failing to comply with a set of requirements committed by IaaS cloud providers will pose uncertainty concerns to the cloud users. From the analysis results compliance cloud be divided into 4 TCC, namely: compliance with legal requirements, authorized software and licensed products, compliance with standards and compliance with SLA or any other contracts.

3. Governance

Governance is a sub-category of accountability. It refers to how IaaS cloud providers manage cloud users expectations, problems and service performance. The IaaS cloud providers should have an appropriate governance framework that provides integral approach to organize and manage the IaaS cloud assets. However, the responsibilities of managing IaaS cloud vary between IaaS cloud providers and cloud users. This will lead to the risk that cloud users will depend on IaaS cloud providers to manage specific risks or quite the opposite. Therefore, IaaS cloud providers need to clarify their responsibilities in managing specific risks. From the analysis results governance cloud be divided into 3 TCC, namely: ownership responsibility, contracts availability and risk governance policy. All respondents stressed the importance of governance to reduce concerns about the responsibilities of managing specific risks that will affect positively on the trust level.

4. Locality

Locality is a sub-category of accountability. It refers to the location of IaaS cloud assets and activities are occurring. Also, it is interested in providing information about the nationality of staff and owners who’s managing IaaS assets. Hide the physical location of IaaS cloud from cloud users will increase the uncertainty concerns and this will lead to reduce trust of cloud users. Most of the respondents mentioned that the majority of cloud users have constraints regard the issue of IaaS cloud geographical locations, including data storage, replication and backup. They confirmed that cloud users always worry about where their data storages, servers and who are the staff they manage their data. From the analysis results locality cloud be divided into 3 TCC, namely: IaaS cloud location, employ local staff, and local people owned infrastructure cloud.

5. CONCLUSION

This paper presented the research findings of identifying IaaS cloud Accountability requirements. The directed content analysis approach that suggested and adopted by Hsieh and Shannon, (2005) has been used to present the ACAs and ACC of integrity. The findings of the qualitative data analysis lead to identify 4 ACAs and 14 ACC. Moreover, the analysis results explained the way in which IaaS cloud providers used the identified ACAs and ACC to ensure the integrity of IaaS that may support their trust level.

REFERENCES

1. Habib, S.M., Hauke, S., Ries, S. and Mühlhäuser, M., 2012. Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing*, *1*(1), pp.1-18.
2. Abbadi, I.M. and Alawneh, M., 2012. A framework for establishing trust in the Cloud. *Computers & Electrical Engineering*, *38*(5), pp.1073-1087.
3. Garrison, G., Kim, S. and Wakefield, R.L., 2012. Success factors for deploying cloud computing. *Communications of the ACM*, *55*(9), pp.62-68.
4. Winkler, V.J., 2011. *Securing the Cloud: Cloud computer Security techniques and tactics*. Elsevier.
5. Adjei, Joseph Kwame. "Explaining the role of trust in cloud computing services." *info 17*, no. 1 (2015): 54-67. https://doi.org/10.1108/info-09-2014-0042
6. Wang, Y., & Vassileva, J. (2007, June). A review on trust and reputation for web service selection. In *Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on* (pp. 25-25). IEEE.
7. Latham, D. C. (1986). Department of Defense trusted computer system evaluation criteria. *Department of Defense*.
8. Friedman, B., Khan Jr, P. H., & Howe, D. C. (2000). Trust online.*Communications of the ACM*, *43*(12), 34-40.
9. Garg, S. K., Versteeg, S., & Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, *29*(4), 1012-1023.
10. Cloud Service Measurement Index Consortium. (2011). Service Measurement Index Version 1.0.
11. Bundt, J. (2000). Strategic stewards: Managing accountability, building trust.*Journal of Public Administration Research and Theory*, *10*(4), 757-778.
12. Alhadeff, J., Van Alsenoy, B., & Dumortier, J. (2012). The accountability principle in data protection regulation: origin, development and

future directions. *Managing privacy through accountability*, 49-82.

13. Denscombe, M., 2014. *The good research guide: for small-scale social research projects.* McGraw-Hill Education (UK).
14. Qu, S.Q. and Dumay, J., 2011. The qualitative research interview.*Qualitative Research in Accounting & Management, 8*(3), pp.238-264.
15. Guest, G., Bunce, A. and Johnson, L., 2006. How many interviews are enough? An experiment with data saturation and variability. *Field methods,18*(1), pp.59-82. https://doi.org/10.1177/1525822X05279903
16. Kuzel, A.J., 1992. *Sampling in qualitative inquiry. In BF Crabtrree and WL Miller (Eds.) Doing Qualitative Research* (2nd ed.), Sage, Thousand Oaks, CA, 1999, 33-45.
17. Morse, J.M., 1994. Designing funded qualitative research. In Norman K. Denzin & Yvonna S. Lincoln (Eds.),*Handbook of qualitative research (2nd ed., pp.220-35).* Thousand Oaks, CA: Sage.
18. Creswell, J.W., 2002. *Educational research: Planning, conducting, and evaluating quantitative*. Prentice Hall.
19. Hsieh, H.F. and Shannon, S.E., 2005. Three approaches to qualitative content analysis. *Qualitative health research, 15*(9), pp.1277-1288.
20. Potter, W.J. and Levine □Donnerstein, D., 1999. Rethinking validity and reliability in content analysis.
21. Mayring, P., 2002. Qualitative content analysis–research instrument or mode of interpretation. *The role of the researcher in qualitative psychology*, *2*, pp.139-148.
22. Elo, S. and Kyngäs, H., 2008. The qualitative content analysis process.Journal of advanced nursing, 62(1), pp.107-115.
23. Garg, S. and Saran, H., 2008, March. Anti-DDoS Virtualized Operating System. In Availability, Reliability and Security, 2008. ARES 08. *Third International Conference on (pp. 667-674).* IEEE.
24. Abualigah, L. M. Q. (2019). Feature selection and enhanced krill herd algorithm for text document clustering. Berlin: Springer.
25. Abualigah, L. M., Khader, A. T., & Hanandeh, E. S. (2019). Modified Krill Herd Algorithm for Global Numerical Optimization Problems. In Advances in Nature-Inspired Computing and Applications (pp. 205-221). Springer, Cham.
26. Abualigah, L. M., & Khader, A. T. (2017). Unsupervised text feature selection technique based on hybrid particle swarm optimization algorithm with genetic operators for the text clustering. The Journal of Supercomputing, 73(11), 4773-4795.
27. Abualigah, L. M., Khader, A. T., Hanandeh, E. S., & Gandomi, A. H. (2017). A novel hybridization strategy for krill herd algorithm applied to clustering techniques. Applied Soft Computing, 60, 423-435.
28. Abualigah, L. M., Khader, A. T., & Hanandeh, E. S. (2018). Hybrid clustering analysis using improved krill herd algorithm. Applied Intelligence, 48(11), 4047-4071.
29. Abualigah, L. M., Khader, A. T., & Hanandeh, E. S. (2018). A new feature selection method to improve the document clustering using particle swarm optimization algorithm. Journal of Computational Science, 25, 456-466. https://doi.org/10.1016/j.jocs.2017.07.018
30. Abualigah, L. M., Khader, A. T., & Hanandeh, E. S. (2018). A combination of objective functions and hybrid Krill herd algorithm for text document clustering analysis. Engineering Applications of Artificial Intelligence, 73, 111-125.