Technology of computing risks visualization for distributed production infrastructures

Dmitrii Voronin[1], *Victoria* Shevchenko[1,*], and *Olga* Chengar[1]

[1]Federal State Autonomous Educational Institution of Higher Education «Sevastopol State University», 299053, Sevastopol, Russian Federation

Abstract. Scientific problems related to the classification, assessment, visualization and management of risks in the cloud environments have been considered. The analysis of the state-of-the-art methods, offered for these problems solving, has been carried out taking into account the specificity of the cloud infrastructure oriented on large-scale tasks processing in distributed production infrastructures. Unfortunately, not much of scientific and objective researches had been focused on the developing of effective approaches for cloud risks visualization providing the necessary information to support decision-making in distributed production infrastructures. In order to fill this research gap, this study attempts to propose a risks visualization technique that is based on radar chart implementation for multidimensional data visualization.

1 Introduction

The term “production infrastructure” is used to designate an economic subsystem that creates optimal conditions for the development of material production, in particular, by creating transport routes, engineering systems and communications, and so on. Such an infrastructure, as a rule, contains a distributed management system.

Interest in distributed control systems arose in the process of increasing the number of sensors, production areas, modernization and complication of standard algorithms for managing technological processes. In such systems controllers, input and output modules, sensors, actuators are spatially distributed.

Areas of Distributed Control Systems (DCS) can be located at any distance from each other, and communication between them will be supported through the provider of cloud infrastructure. This trend has been developing due to the success of object-oriented programming, distributed data warehouses and the active implementation of information technologies for cloud infrastructures.

The maximum benefits of a distributed system are achieved when the controllers operate autonomously, and the information exchange between them is minimized. It is known that most of the emergencies in cloud production infrastructures are the results of ineffective risks management [1 – 6], related to the synchronization and transfer of data from primary controllers to control systems. It should be mentioned that on the one hand – risk

* Corresponding author: shevchenko-vika@mail.ru

management is a rather expensive processes requiring additional significant amount of heterogeneous resources. On the other hand, implementation of cloud risks can lead to irreparable loss, which can give rise to a serious accident at the enterprise. Thus, the existence of these objective contradictions results in conflict situations, requiring balanced and compromise expert solutions that are usually found based on the usage of decision-support systems. In many cases, the effectiveness of the solution is related to the speed of its adoption by the DCS' administrator, which in turn imposes certain requirements on the methods of data visual representation. Occasionally, the lack of visualization method effectiveness can lead to a significant reduction in the quality of accepted managerial decisions. Moreover, cloud risks are very polytypic, and it can be rather difficult to provide adequate comparative description of different risks management scenarios. Therefore, the considered problem of cloud risks visualization for production infrastructures is extremely important.

This paper is organized as follows: section 2 provides a review on risks and vulnerabilities of cloud infrastructures. Classification, assessment, visualization and management problems have been analysed. Then, section 3 describes the formal statement of the risks visualization problem aimed to ensure the effectiveness of the decisions focused on cloud risks management in production infrastructures. Section 4 highlights the particular properties of the proposed visualization technique and section 5 concludes the study.

2 State of the art

Rapidly expanding level of computerization of modern society leads to the need for more widespread use of software tools, including cloud computing technologies. In many cases, risk management procedures are focused on the achievement of the following results: 1) to decrease the probability of undesired events occurrence; 2) to minimize the loss from negative consequences of the emergency situations implementation [2 – 8], arising during the production process. There are two basic approaches to solve the problem of risks management: proactive and reactive [7]. The main purpose of proactive management is to prevent the implementation of undesired events leading to the emergence of risks. Other words, this approach is mainly focused on applying of predictive risk assessments and is used under the conditions of the a priori information deficit about the impact of possible consequences of undesired events emergence. As for the reactive approach, it is characterized by the presence of accurate impact assessments of the arising incidents and its main purpose is to neutralize the negative effects of the events that have already occurred. In more detail, the key features of proactive and reactive approaches are described in Figure 1.

Threats and Vulnerabilities. The work [8] is devoted to different challenges that are specific for cloud computing environments. It focuses on security and privacy services in the cloud and notes that storage outsourcing needs a well-experienced team of professionals and significant costs on the "state of the art" equipment. The advantages of cloud services result in threats and vulnerabilities, i.e. security issues form the main barriers of the widespread use of cloud computing in production management systems [9]. In [9] different approaches of security vulnerabilities identification are discussed based on Amazon Web Services consideration. It should be mentioned, that mobile cloud popularity puts forward new requirements to security ensuring, i.e. the complexity and costs of these systems constantly increase [10]. In work [11] cloud outsourcing used by Swiss companies is considered. Authors believe that the migration procedure highly depends on the company's individual characteristics and therefore visualization approaches should implement adaptation. Thus, the existing threats require effective risk visualization methods that are

able to assess the current situation and to provide determined benchmarks for promising solutions search.

Risk Assessment. Although there are different approaches to risk assessment in cloud environments [12 – 18], for industrial infrastructures this direction remains an open research issue [13]. In [14] authors have offered an approach to the assessment of risks related to information data security. Based on it a special service was implemented [14] to give an actor of cloud environment [15] the information that is useful in decision-making on the work with considered service provider. In [16] authors propose to use protection strategy for cloud risks assessment. The economic-based methodology [17] is supported by an open source toolkit for comparative cloud risk analysis. Software tool ACRAM [18], which consists of the offline and online modules, can assess the risk of being co-located with a possible attacker during cloud mitigation. Many new approaches are based on known decision-making methods, for example, proposed by T.L. Saaty [19] or using the game-theoretical approach [20].

Cloud Risks Classification. Cloud risks classification is not a well-defined scientific problem [2, 21, 22]. In [21] authors distinguish the following groups of risks: information security, operations management, change management, disaster recovery, service level management, interface management, regulations and legislation. ENISA's list of risk scenarios and their categories include the following [1, 22]: policy & organizational, technical, legal, etc. According to the information presented in [2], most of cloud security risks can be categorized using application and network levels, data storage risks, etc. We propose to use the following groups of risks: information, resource, organizational, financial, social, operational, reputation, legal. They will be used to discuss the proposed visualization technique in section 4.

Risk Management in Cloud Environments. In [3] risk factors for cloud computing services have been proposed. They are the following: agreement or contract, privacy, jurisdiction, burglary, natural disaster, system vulnerability, social engineering, mistakes made by employees (intentionally or accidentally), cross-cloud compatibility, etc. The "Analytic Network Process" method is proposed to evaluate relative weight for the risk management matrix [3]. Cloud computing risk management approach that is focused on the "Business-Level Objectives" is given in the work [4]. Multi-faceted "Trust Management System Architecture" [5] supports the user's decisions on cloud migration parameters. The usage of Bayesian networks can be effective for network chances quantification at various levels [23]. The main objective of the research, described in [24], is to explore the flexibility of the existing risk management frameworks. In [25, 26] risk-aware virtual resource assignment mechanisms are considered.

Despite the suggested quantities of different approaches [3, 4, 23–26], risk management in cloud environments still remains an open research issue. The next section is devoted to a formal statement of the risks visualization problem aimed to ensure the effectiveness of the decisions that are focused on cloud risks management in production infrastructures.

3 Problem Statement

In most cases, the cloud environment may be assigned to critical infrastructures that can sometimes directly affect the safety of a whole corporation or even a country. In such systems it was decided to consider the following types of states: safe, operable, pre-critical and emergency. Safe states are included to an operable subset and describe the situation when the cloud system has high stability, i.e. the possibility of direct transition to the pre-critical state is negligibly small. In the case of insufficient effectiveness of dependability assurance procedures, the cloud environment has a degradation tendency, i.e. to transit from the operable states to pre-critical. If reconfiguration processes were not launched timely,

then even a slight error can bring a non-reducing failure leading to a transition to the emergency (absorbing) state.

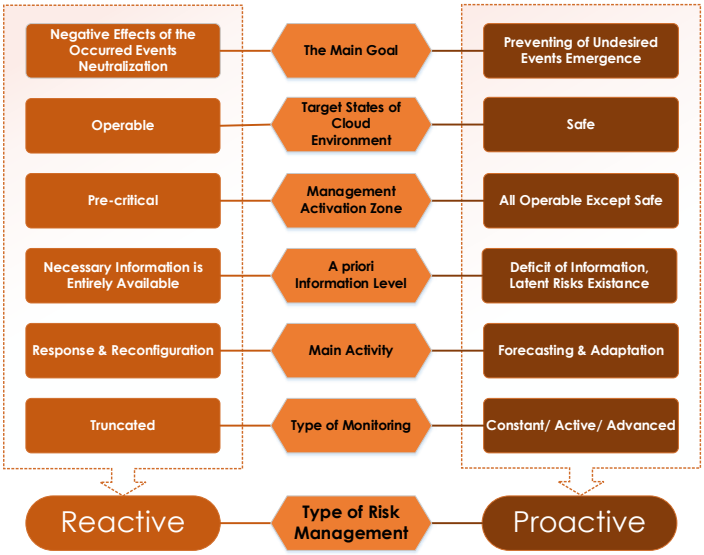

Fig. 1. The key features of proactive and reactive risks management.

Any cloud state can be described in a multidimensional phase risk space. For example, the i-th state denoted as Si is described by a tuple $< \mathrm{R}^{Si}, P^{Si}, \mathrm{Z}^{Si} >$, where R^{Si} – is the risk assessment for state S_i; P^{Si} – is the probability of undesired event occurrence for the state S_i; Z^{Si} – is the amount of negative consequences of undesired event occurrence for the state S_i.

There are various versions of the cloud state space interpretation using different graphical data representation forms: two-dimensional, multi-dimensional, etc. Each of them has the area of effective application, for example, the visual technique that described in [27] can be used for quality estimation of services in cloud environments.

It is proposed to distinguish the three levels of cloud risks (highlighted in different colours). They are the following:

– The "green" level of confident functioning of cloud environment (the states' type is safe);

– The "yellow" level of significant risk (the cloud is in operable state, but the probability of cloud system transition into one of the pre-critical states is too high);

– The "red" level of unacceptable risk (the cloud is in pre-critical state and any insignificant failure may lead to a transition into emergency state). For various subject areas, this "critical threshold" can be different. It will be formed in accordance with the evolving situation, taking into account the specific features of the cloud environment functioning.

The generalized state diagram of cloud environment's life cycle is presented on the figure 2.

From the point of view of cloud environment's operation, transitions between its states can be both beneficial and damaging. "Left-to-right" transitions are the results of degradation processes, "right to left" transitions take place due to successful work of reconfiguration procedures.

The aim of reactive management is to prevent the transitions into the "red" level of unacceptable risk. The purpose of the proactive management is to keep the system only in safe states.

The formalization of problem of the risks visualization technique synthesis is formulated in the following way. The tuple (1) is given. For (2) it is needed to create and implement the optimal visualization technique, denoted as vrt_k and defined in (3) and (4).

$$\langle \mathrm{S}_i, \mathrm{S}_j, \langle \mathrm{R}^{Si}, P^{Si}, \mathrm{Z}^{Si} \rangle, \langle R^{Sj}, P^{Sj}, \mathrm{Z}^{Sj} \rangle, \mathrm{U}_D, \Theta, \mathrm{RVT}_D, \Phi \rangle, \quad (1)$$

where S_i – is the initial state; S_j – is the final state; U_D – is a set of possible alternative variants of risk management;

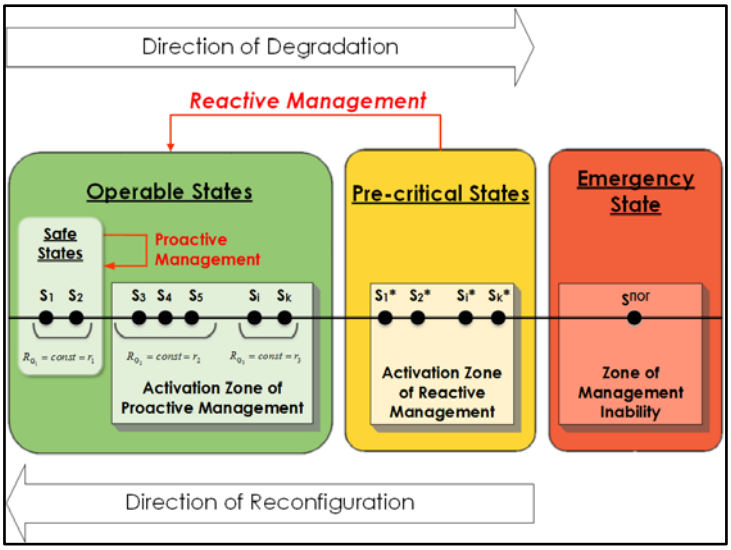

Fig. 2. Generalized state diagram of cloud environment's life cycle.

Θ – is a function that generates management decision for transition from the state S_i to S_j; RVT_D – is a set of possible visualization techniques; Φ – is a function that evaluates the efficiency of risks visualization for management decision u_i.

$$\forall k = \{1,2,\dots,|\mathrm{RVT}_D|\}, \quad (2)$$

$$\mathrm{rvt}_k = \arg \max_{\mathrm{rvt}_k \in \mathrm{RVT}_D} \sum_{i=1}^{|\mathrm{U}_D|} \Phi\big(\mathrm{rvt}_k(\mathrm{u}_i)\big), \quad (3)$$

$$\mathrm{u}_i = \Theta\big(\mathrm{S}_i, \mathrm{S}_j, \langle \mathrm{R}^{Si}, P^{Si}, \mathrm{Z}^{Si} \rangle, \langle R^{Sj}, P^{Sj}, \mathrm{Z}^{Sj} \rangle, \mathrm{U}_D\big). \quad (4)$$

The proposed task formulation is sufficiently generic and it gives an opportunity to consider the problem at a relatively high level of abstraction. The next section highlights the particular properties of the proposed visualization technique.

4 Visualization technique

The proposed technique is based on the concept of visual analytics that has been realized in multidimensional data visualization methodology that in described in [27]. It has the flowing main steps: getting the data of cloud services monitoring; complex quality

indicators calculation; visualization. Basic aspects of relationship between the main stages of the risk life cycle are depicted on the figure 3.

The radar charts are a more compact form of visual representation of the risks assessment results. To construct the radar chart a researcher selects a set of analysing management decisions and a group of cloud risks used for the assessment. Each type of risk from the selected group is plotted on corresponding radar chart axes [27]. The fill colour of radar charts' inner parts may vary, describing the "green", "yellow" or "red" level of considered risk. It can be rather helpful for the low-complemented user to get a brief and easy information about cloud risks in production infrastructures.

Examples of a radar charts used for operational and informational cloud assessment risks are presented on the figures 4 and 5.

Fig. 3. Graphical interpretation of the basic relationships between some of the stages of the risk life cycle.

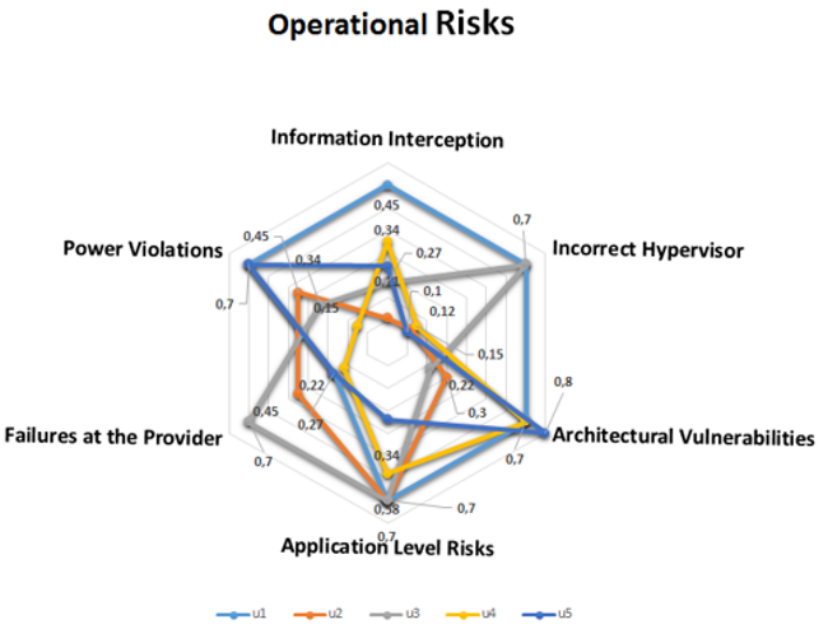

Fig. 4. Example of a radar chart for operational cloud risks

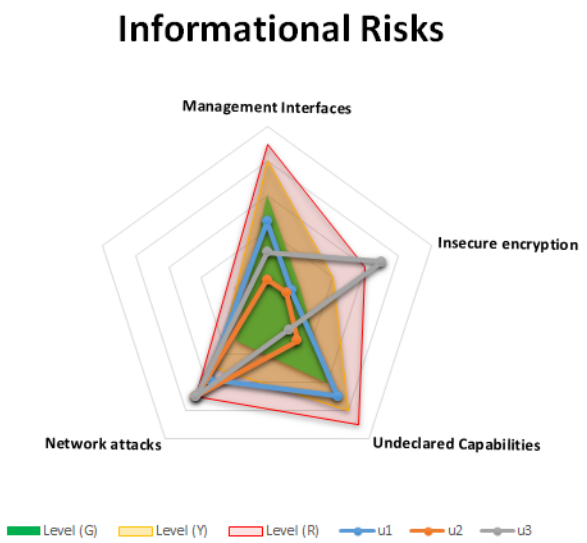

Fig. 5. Example radar chart for informational cloud risks.

Based on the results presented in [28] the following conclusions can be drawn:

- a person perceives 90% of the entire information through its sight;
- about a half of all human brain neurons is involved in the processing of visual information;
- the introduction of imaging elements increases a person's productivity by 17%.

Thus, data visualization is a powerful tool for the enhancing of human perception in the information analysis. Fig. 5 additionally contains levels of information risk using the proposed "red / yellow / green" graduation. This diagram depicts that all considered management strategies are in the critical ("red") zone due to the parameter «Network attacks». The “U2” is the best strategy, the strategy U3 is the worst.

5 Conclusion

The proposed risks visualization technique, dispute from the known decisions, is oriented on providing decision-makers with the necessary information about cloud environments in online mode. This technique can be implemented in the decision-support systems for production infrastructures management. It can be used as a part of visual analytics system that is focused on large-scale production problems solving and risks visual monitoring for distributed management systems. Directions for further research conform to the principles set out in the works [29 – 31].

This work was supported by the Russian Foundation for Basic Research (projects № 15-29-07936, № 18-47-920007, № 18-47-920005).

References

1. *European Network and Information Security Agency. Cloud Computing: Benefits, risks and recommendations for information security*. – ENISA, (2009).

2. T. K. Damenu, C. Balakrishna. *Cloud Security Risk Management: A Critical Review,* Proceedings of the 9th IEEE International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 370–375, (2015).
3. F. C. Ku, and T. C. Chen. *The risk management strategy of applying cloud computing*, International Journal of Advanced Computer Science and Applications, Vol. **3**, No. 9, pp. 18–27, (2012).
4. J. O. Fitó, M. L. Macías, J. Guitart Fernández. *Toward business-driven risk management for Cloud computing*, Proceedings of the International Conference on Network and Service Management, pp. 238–241, (2010).
5. S. M. Habib, S. Ries, M. Muhlhauser. *Towards a Trust Management System for Cloud Computing*, Proceedings of the 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 933–939, (2011).
6. B. Grobauer, T. Walloschek, and E. Stocker, *Understanding cloud computing vulnerabilities*, Security & privacy, IEEE, vol. **9**, no. 2, pp. 50–57, (2011).
7. M. Ju. Ohtilev, N. G. Mustafin, B. V. Sokolov, *The concept of proactive management of complex objects: theoretical and technological bases*, Izvestija vuzov. Priborostroenie., vol. **57**, no. 11, pp. 7–14, (2014).
8. H. Takabi, J. B. Joshi, and G.-J. Ahn, *Security and privacy challenges in cloud computing environments*, Security & Privacy, IEEE, vol. **8**, no. 6, pp. 24–31, (2010).
9. P. Mosca, Y. Zhang, Z. Xiao, and Y. Wang, *Cloud security: Services, risks, and a case study on amazon cloud services*, International Journal of Communications, Network and System Sciences, vol. **7**, no. 12, pp. 529–535, (2014).
10. S. Na, K. Kim and E. Huh, *Threats Evaluation for SLAs in Cloud Computing*, Proceedings of the IEEE International Conference on Convergence Technology, pp.1570–1571, (2013).
11. N. Brender, I. Markov, *Risk perception and risk management in cloud computing: Results from a case study of Swiss companies*, International Journal of Information Management, vol. **33**, no. 5, pp. 726–733, (2013).
12. P. Saripalli, B. Walters, *QUIRC: A Quantitative Impact and Risk Assessment Framework*, Proceedings of the IEEE 3rd International Conference on Cloud Computing (CLOUD 10), pp. 280–288, (2010).
13. M. Theoharidou, N. Tsalis, D. Gritzalis, *In cloud we trust: Risk-Assessment-as-a-Service*, Proceedings of the International Conference on Trust Management, pp. 100–110, (2013).
14. A. Sangroya, S. Kumar, J. Dhok, and V. Varma, *Towards analyzing data security risks in cloud computing environments*, Proceedings of the International Conference on Information Systems, Technology and Management, pp. 255–265, (2010).
15. A. Skatkov, E. Maschenko, V. Shevchenko and D. Voronin, *Actors interactions research in cloud computing environments using system dynamics methodology*, Proceedings of the 18th FRUCT & ISPIT Conference, pp.612–619, (2016).
16. S. C. Zhu, Y. Xu, M. Y. Jin, L. Sheng, *Cloud Computing Security Risk Assessment Based on Level Protection Strategy*, Computer Security, vol.**5**, pp.39–42, (2013).
17. V. Bellandi et al., *Toward Economic-Aware Risk Assessment on the Cloud*, Security & privacy, IEEE, vol. **13**, no. 6, pp. 30–37, (2015).

18. C. A. Chih, Y. L. Huang, *An Adjustable Risk Assessment Method for a Cloud System*, Proceedings of the IEEE International Conference on Software Quality, Reliability and Security, pp. 115–120, (2015).
19. Z. W. Jiang, W. R. Zhao, Y. Liu, B. X. Liu. *Model for Cloud Computing Security Assessment Based on Classified Protection*, Computer Science, vol.**8**, pp.151–156, (2013).
20. A. Skatkov, V. Shevchenko and D. Voronin, *Game-theoretical management model for IT-services of ERP-systems guaranteed level assurance in cloud environments*, Proceedings of the 5th IEEE International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, in press, (2016).
21. M. Carroll, A. Van Der Merwe, P. Kotze, *Secure cloud computing: Benefits, risks and controls*, Proceedings of the IEEE International Conference on Information Security for South Africa, pp.1–9, (2011).
22. E. Cayirci et al. *A cloud adoption risk assessment model*, Proceedings of the 7th IEEE International Conference on Utility and Cloud Computing, pp. 908–913, (2014).
23. N. Poolsappasit, R. Dewri, I. Ray, *Dynamic security risk management using Bayesian attack graphs*, Transactions on Dependable and Secure Computing, IEEE, vol. **9**, no. 1, pp. 61–74, (2012).
24. F. Al-Musawi, A. H. Al-Badi, S. Ali, *A Road Map to Risk Management Framework for Successful Implementation of Cloud Computing in Oman*, Proceedings of the International Conference on Intelligent Networking and Collaborative Systems, IEEE, pp. 417-422, (2015).
25. A. Almutairi, A. Ghafoor, *Risk-aware virtual resource management for multitenant cloud datacenters*, Cloud Computing, IEEE, vol. **1**, no. 3, pp. 34-44, (2014).
26. A. Almutairi, M. Sarfraz, A. Ghafoor *Risk-aware management of virtual resources in access controlled service-oriented cloud datacenters*, Transactions on Cloud Computing, IEEE, vol. **1**, no. 1, (2015).
27. A. Skatkov, E. Maschenko, V. Shevchenko and D. Voronin, *Visual quality estimation technique for services in cloud environments*, Proceedings of the 10th IEEE International Conference on Application of Information and Communication Technologies, Baku, Azerbaijan, in press, (2016).
28. A. Mansaf, and K. A. Shakil, *A decision matrix and monitoring based framework for infrastructure performance enhancement in a cloud based environment*, arXiv preprint arXiv:1412.8029, (2014).
29. Gupta, Smrati, et al. *Cloud Service Offer Selection. Model-Driven Development and Operation of Multi-Cloud Applications.* Springer International Publishing pp. 13-22, (2017).
30. K. Julia, D. Pachamanova, and A. Corbett. *The role of data visualization and analytics in performance management: Guiding entrepreneurial growth decisions.* Journal of Accounting Education, (2017).