The 14th International Conference on Business Information Security (BISEC'2023), November 24th 2023, Niš, Serbia

Custom-made Approaches to Cloud Container Aecurity: A Methodologically Sound Approach based on International Sample Results

Aleksandar Jovanović[1,*], Petar Milić[2]

[1]Faculty of Information Technology, Belgrade Metropolitan University, Tadeuša Košćuška 63, 11000 Belgrade, Serbia
[2]Faculty of Technical Sciences, Department of Computer Science and Informatics, University of Priština - Kosovska Mitrovica, Knjaza Miloša 7, 38220 Kosovska Mitrovica, Serbia

Abstract

Previous available research focused towards examining a sample of programmers' responses regarding cloud container security. In this paper, we performed a comparison of differences between the analyzed sample in this paper and the previous one that we published and which comprised a Serbian-based sample. The research aim of the following paper is to form a analysis of answers in terms of its validity for the overall programmer community. It was determined that there is a slight difference between two samples; however there are not any country-specific types of cloud security issues, based on the sample. There is a tendency of completely globalizing or even neglecting the interviewee's background in discussing results in cloud security literature. And this very aspect is indicative for custom made approaches to security issues, according to parameters such as confidentiality, availability, usability, non-repudiation and integrity, all mentioned and discussed in the paper. The results helped us focus on the creation of the overall recommendations for creating methodology for cloud containers' assessment in terms of security that would be more globally applicable. In particular, the next step is to allow for mathematical models to be applied in the survey results interpretation and also to implement a fuzzy logic mathematical model to create a layer of protection in CCSA.

Keywords

cloud containers, Security, questionnaires

1. Introduction

Cloud environments are susceptible to malicious attacks, like any other form of IT-based architecture. The more data installed and infrastructure facilities installed on the cloud, the more chance it would be attacked at certain point. There is an ongoing tendency to "shift left" when dealing with cloud container security [1]. This means, that as early as possible in the development process of an app lifecycle malicious ruptures should be examined and that this process saves a lot of later costs and time when dealing with securing cloud -based apps throughout their lifecycles.

2. Methodology

Analysis was performed by using a questionnaire, which involved 50 members of the IT sector, that have been using cloud technologies and that pointed towards different issues and aspects of creating a methodology for CCSA (Cloud Container Security Assessment). The questionnaire had some multiple choice answers and some questions had possible answers given in the form of statements and views towards certain cloud container–based themes and problems. The questionnaire was conducted over a twelve-month period. The sample was diverse in terms of background with software use among interviewees but focused on their experience according to that which they have been applying mostly in their daily work. One criterion for further doing the questionnaire is that all of them should have software development experience for at least one year and are at least familiar with Cloud.

Most of the sample included individuals with more than ten years of experience with IT and software development, both in private or public departments and academia. The previous sample conducted in 2022 [2] included 90% of individuals residing in Serbia, involved either at Serbian companies or international software companies there. The current sample in this paper made a more international sample, according to which at least 35% of the interviewees were of EU or US space.

BISEC'23: 14th International Conference on Business Information Security, November 24, 2023, Niš, Serbia
*Corresponding author.
aleksandar.jovanovic@metropolitan.ac.rs (A. Jovanović); petar.milic@pr.ac.rs (P. Milić)
0000-0002-9815-4344 (A. Jovanović); 0000-0003-0427-8379 (P. Milić)

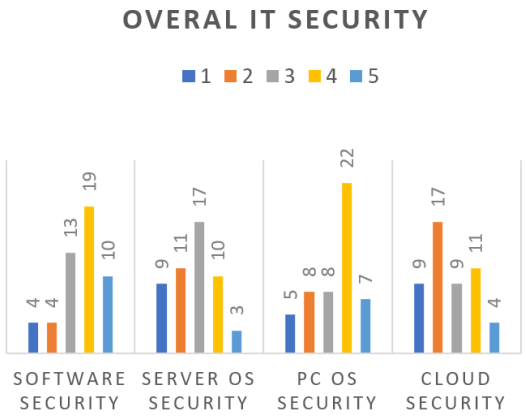

Figure 1: Overall IT security.

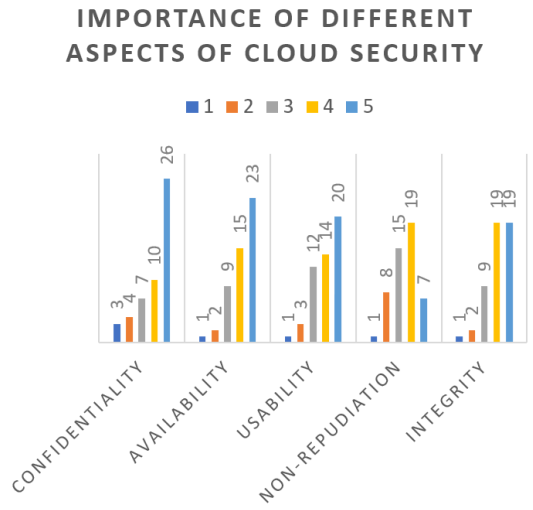

Figure 2: Importance of different aspects of cloud security.

3. Previous research

In the previous study we has conducted in 2022 [2], the results of the paper indicated that commercially-driven advancements remain the real drive for creating theoretical models in the novel scientific field of CCSA. But it also pointed to the fact that there is not an overall consensus on creating a common methodology with binding application or at least emphasizing common security frameworks for assessing security in the cloud. The survey results analyzed in the mentioned paper indicated security patterns for building secure systems. It also pointed to the aspect of previous inspection on cloud container images before the utilization as significant for creating cloud container security methodologies.

The above mentioned study concluded with the comparison of the results of questionnaires used with the literature references and case studies, and indicated a real cloud threat incident analysis as necessary in order to get more specific results on cloud environments ' particularities in the future and to be able to further advance towards creating any kind of CCSA methodology.

4. Results of our current study

Based on the analysis we have conducted here, it can be noted that attention has been paid to the security in cloud environment, and this is depicted on Figure 1. On the scale from 1 - little to none till 5 - highly experienced, we can notice that respondents in our survey showed adequate experience in working with cloud security issues which can lead to proper usage and configuration of cloud services. Thus, security issues will be properly resolved. Also, other general types of security are well represented and respondents are aware of their importance.

In accordance with previous statements, collected responses goes towards confidentiality and availability aspects of cloud security, which is among highest, as depicted on Figure 2. Nowadays, confidentiality represents a fundamental aspect of cloud security, ensuring that sensitive data remains private and protected from unauthorized access, whether it's at rest or in transit [3, 4]. Similarly, availability is equally critical in cloud security, ensuring that cloud services and resources are accessible and reliable for users, minimizing downtime and disruptions to business operations. Keeping in mind the diversity of services that are available through cloud services, it becomes clear why these aspects are major factor motivating the proliferation of security issues.

The presence of security vulnerabilities within a cloud environment can result in the inadvertent exposure of information regarding the services hosted therein [5, 6]. This risk becomes particularly pronounced when background containers are executed on a single host, sharing the same operating system (OS) kernel, as a compromised kernel can compromise the isolation provided by the container mechanism. In accordance with this assertion, our analysis, as depicted in Figure 3, substantiates these findings. Additionally, the data presented in Figure 4 underscores the critical importance of thoroughly inspecting cloud container images before their deployment and use.

Hence, security concerns emerge as the primary impediment to the continued adoption of containers and cloud computing as a whole. When data and services are outsourced to the cloud environment, they become susceptible to various risks, with security being a paramount concern that necessitates a meticulous implementation

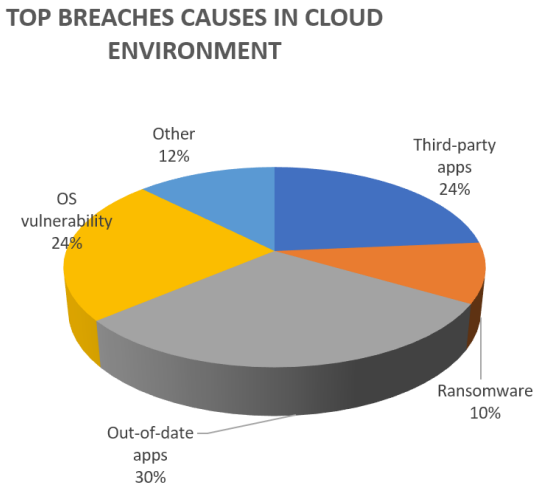

Figure 3: Top breaches causes in cloud environments.

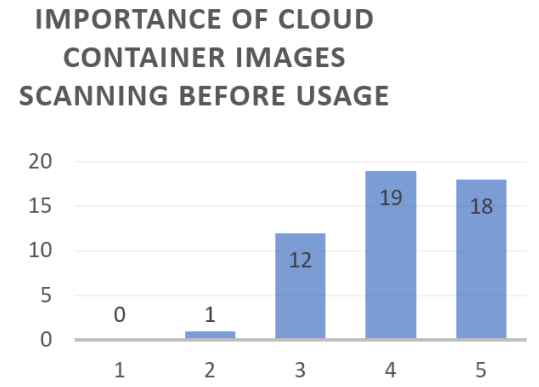

Figure 4: Importance of cloud container images scanning before usage.

strategy. Employing security patterns for constructing secure systems involves outlining methods to mitigate specific threats, remediate vulnerabilities, and establish a secure environment conducive to the effective utilization of cloud services. These patterns offer standardized solutions and best practices for countering common threats and vulnerabilities, thus enhancing the overall security posture of systems and applications. By implementing security patterns, organizations can streamline the development of secure software and systems in cloud environment, reduce the likelihood of security breaches, and fortify their defenses against evolving cyber threats.

5. Comparison with previous research

In comparison with the results from our study published on BISEC 2022 regarding the overall IT security, current results confirm dedication of IT professionals to the general software security. Also, awareness about server security and PC OS security gained more attention, which is in line with survey respondent's orientation toward proper configuration and usage of environment for usage of cloud services. Nevertheless, respondents slightly increased their experience with cloud security issues indicating thus that this aspect is important.

Furthermore, significance of different aspects of cloud security such as confidentiality, availability, usability, non-repudiation and integrity is increased in comparison with the study from BISEC 2022, showing that they are essential in designing a robust cloud security strategy that protects data and services while ensuring they remain accessible and usable for authorized users.

When we come to the top breaches causes in cloud environment, it can be noted that still high percentage is about out-of-date apps. This lead us to conclusion about high significance of regular update of all parts of the information system, as of OS software, app libraries and etc. in order to maintain as much as possible high level of security. Other breaches have balanced values in comparison with results from BISEC 2022. Similarly, the critical importance of thoroughly inspection of the cloud container images before their deployment and use is confirmed.

6. Similar studies of other authors

Seongmo et al. [7] suggested a CloudSafe platform, whereas the authors pointed towards a necessity for testing on a actual cloud system. The study focused on Amazon's AWS, but had implications for other Cloud providers such as Azure too. Gudapati and Gaikwad [8] created common cloud security issues 'guidelines. Nitiashree et al. [9] proposed a three-stage cloud computing data security model. A unique or coherent methodology for cloud containers security assessment is not available and the ones suggested by companies are less usable for the current attacks that are diverse in nature. However, the last mentioned study [9] went ahead to create an Advanced Encryption Standard (AES) algorithm for Data security. The last layer of this algorithm model involved cryptography techniques. Furthermore, the study indicated a relation between occurrence of public cloud threats and data security during the transmission from Cloud Service Customer (CSC) to the Cloud Service Provider (CSP) [10]. This is relevant to understand the direction in which future research should be focusing.

What we noticed from cloud security literature analysis is that there is a tendency of completely globalizing or even neglecting the interviewee's background in discussing results. And this very aspect is indicative for custom made approaches to security issues, in terms of aspects analyzed and described.

7. Conclusion

A thorough inspection of cloud container images is necessary and confidentiality, availability, usability and non-repudiation along with integrity become more significant for cloud environments security strategy which is robust. The next step is the study would be to allow for mathematical models to be applied in the survey results interpretation and also to implement a fuzzy logic mathematical model to create a layer of protection which could solve some if not majority of issues mentioned in this paper and this save time and effort in dealing with cloud security.

Acknowledgment

We would like to thank the programmers and engineers for filling-out the survey on cloud security and for their interest in our research.

References

[1] D. Gonzalez, P. P. Perez, M. Mirakhorli, Barriers to shift-left security: The unique pain points of writing automated tests involving security controls, in: Proceedings of the 15th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 2021, pp. 1–12.

[2] A. Jovanović, P. Milić, V. Saraswathi, Towards creating methodology for security assessment of cloud containers- an overview of available tools, in: BISEC'22: 13th International Conference on Business Security, 2022, pp. 50–53.

[3] A. Tchernykh, U. Schwiegelsohn, E.-g. Talbi, M. Babenko, Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability, Journal of Computational Science 36 (2019) 100581.

[4] P. Yang, N. Xiong, J. Ren, Data security and privacy protection for cloud storage: A survey, IEEE Access 8 (2020) 131723–131740.

[5] H. Tabrizchi, M. Kuchaki Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions, The journal of supercomputing 76 (2020) 9493–9532.

[6] M. Jouini, L. B. A. Rabai, A security framework for secure cloud computing environments, in: Cloud security: Concepts, methodologies, tools, and applications, IGI Global, 2019, pp. 249–263.

[7] S. An, A. Leung, J. B. Hong, T. Eom, J. S. Park, Toward automated security analysis and enforcement for cloud computing using graphical models for security, IEEE Access 10 (2022) 75117–75134.

[8] G. S. Prasad, V. S. Gaikwad, A survey on user awareness of cloud security, International Journal of Engineering & Technology 7 (2018) 131–135.

[9] B. Nithiasree, B. R. Prakash, R. S. Sundar, A survey on cloud security threats and solution for secure data in data stages, 2021 International Journal of Computer Techniques (IJCT) 8 (2021).

[10] M. Toy, Cloud services architectures, Procedia Computer Science 61 (2015) 213–220.