Towards creating Methodology for security assessment of cloud containers- an overview of available tools

Aleksandar Jovanović[1,*], Petar Milić[2] and V Saraswathi[3]

[1]Belgrade Metropolitan University, Faculty of Information Technology, Tadeusa Košćuška 63, 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
[3]SRM IST, ECE Department, Kattankulathur, Chennai, India

Abstract

The most popular ways of initializing containerized workloads such as KUBERNETES, GKE, FARGATE and OPENSHIFT, promise the transition towards cloud solution containers by offering commercial, open source or academic-based applications. In the introduction part, we analyze cloud architecture and determine the relation of the cloud and security in the cloud, mentioning conventional architectures.

By the analysis of work related to cloud security assessment and references in the field of container security in the cloud and safety assessment criteria, we make a synthesis of methodological tools available and make a comparison of their applicability, focusing on pros and cons. We present the questionnaire and discuss the results among the experts from IT practice.

The results indicate that, despite commercially-driven advancements in the relatively novel scientific field, there is not an overall consensus on using tools even for delicate questions such as security in the cloud architectures, which should involve the binding application of unique methodology at least for most common cloud frameworks, such as the ones analyzed in the paper. The criteria of previous inspection on cloud container images before the utilization, is of utter importance for creating prospective methodologies. An in-depth survey and a real cloud threat incident analysis is necessary to get more specific results for creating a methodology for assessing cloud container security.

Keywords

containers, security, tools, assessment, cloud, methodology

1. Introduction

There are continuous possibilities and issues that arise with the development of fast internet connections, 5G network development advancements and transfer to automotive and Machine learning technologies and software. One of the most indicative processes that are reflecting these advancements is the adoption of cloud technologies and transfer of enterprises to Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) principles. The problematic of its security is somewhat taken for granted, because the enterprises and relying on the prominent cloud providers, such as Amazon, Google, Microsoft, to supply with methods for accessing cloud security issues in their packages. There are commercial versions made by these companies, such as GKE, Kubernetes, and some that are reflecting the latest academic-based open source research, such as Fargate or Openshift, that operate within the boundaries of their intended use, but focus on one or several central issues that these packages analyze and process, rather than creating a common methodological framework.

BISEC'22: 13th International Conference on Business Information Security, December 03, 2022, Belgrade, Serbia
*Corresponding author.
aleksandar.jovanovic@metropolitan.ac.rs (A. Jovanović); petar.milic@pr.ac.rs (P. Milić); saraswav@srmist.edu.in (V. Saraswathi)

2. Similar studies

A research conducted by Seongmo et al. [1], has indicated a creation of CloudSafe platform, which gave results at a theoretical model of the cloud. In this study, the authors pointed towards a necessity for the testing on a actual cloud system. The study focused on AWS, but had implications for other Cloud providers in the proposed future studies, such as Azure. In the research review study by Gudapati and Gaikwad [2], the authors focused on creating guidelines for cloud security issues, and Nitiashree et al. [3], even proposed a three-stage data security model for cloud computing. All these researches have shown though, that a unique or coherent direction towards a methodology for cloud containers either does not exist or is less usable for the current attacks that arise, but is needed . However, the latter [3] succeeded in creating an Advanced Encryption Standard (AES) algorithm for Data security, with the last layer of the algorithm model, involving cryptography techniques. The study indicated a relation between occurrence of public cloud threats and the security of data which is transmitted from Cloud Service Customer (CSC) to Cloud Service Provider (CSP).

The authors determined the issues such as contemporary threats and methods for addressing them however did no survey among experts to check the findings of its relevance. Some work was emphasized where it was pointed out by Nitiashree et al. [3], that security is the big issue in containers and that future research needs to be conducted in detail about it to solve these challenging issues. Despite these papers' findings [4, 5, 6], no unique methodology or market-based method are issued, other than recommendations made available by CIS [7]. Further more, so far companies have shown interest in creating methodologies, as mentioned by [8] and some involved surveys, such as the research done by Tabrizchi and Rafsanjani [9]. A an annual report on cloud detection security issues determined by Sysdig [10] and other reports made by the private sector as well as the cloud- and other security-approach- reports made available by global IT societies and organizations for security [7], also contribute to the overall consensus on cloud-related issues. A scientific value of these researches is questionable though, as they focus on addressing common threats and commercial uses of the respective companies' software for dealing with threats. That is why this research was suggested and the following methodology applied.

3. Aims and methods

The aim of the paper is to progress towards creating an assessment of the ongoing cloud security problems. According to the analysis of scientific studies related to cloud security assessment, available literature on cloud container security guidelines and safety assessment criteria, we make a synthesis of tools available, opinions of experts and make an overview of container utilization issues, and compare them to our results of the questionnaire among experts in software development.

4. Methodology

Analysis was performed by using a questionnaire, which involved 29 members of the IT sector (see Table 1), that have been using cloud technologies and that pointed towards different issues and aspects of creating a methodology for security assessment of containers. The questionnaire has multiple choice answers and to some questions, the answers were given in the form of professional opinions and statements regarding suggestions and views towards certain IT–base problems. The questionnaire was conducted over a three-month period. The sample was heterogeneous in terms of background of software the interviewees have been applying in their daily work, with the criteria that all of them should have been doing software development for at least one year and are familiarized with Cloud-related problem.

Most of the sample included individuals with more than ten years of experience with software development, both in private companies and academic departments of the University. The sample included 90% of individuals residing in Serbia, but involved either at Serbian companies or international software companies there.

5. Results and discussion

According to the analysis we have performed, there is low level of attention 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 do not have adequate experience in working with cloud security issues which can lead to improper usage and configuration of cloud services. Thus, security issues will not be properly resolved (see Figure 1).

In accordance with previous statements, thus how have some levels of awareness about importance of security in cloud environment, stressed out that confidentiality and availability aspects of cloud security are among highest, as depicted on Figure 2. 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.

Security vulnerabilities in cloud environment can lead to the leak of information about hosted services which is especially expressed if the background containers are executed on one host that shares the same OS kernel, because an imperiled kernel leads to the invalidation of isolation provided by the container mechanism. In align with this statement, results of our analysis presented on Figure 3 confirm these findings. Moreover, results shown on Figure 4 indicate that previous inspection on cloud container images before usage is highly important.

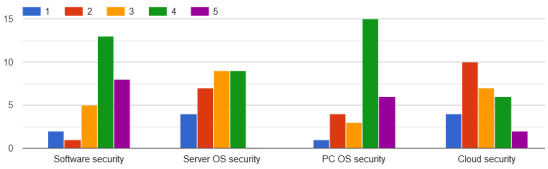

Figure 1: Overall IT security.

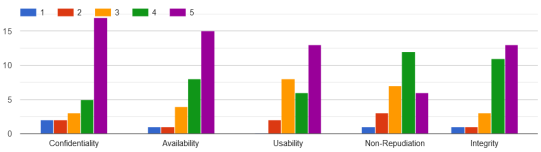

Figure 2: Importance of different aspects of cloud security.

Table 1
Number and percentage of Interviewees broken down by the criteria of experience with software development in general, that were used in the questionnaire performed.

	Number of interviewees (29)	Percentage in the overall sample (%)
0 - 10 years experience, none with CLOUD technologies	**5**(29)	17%
More than 10 years of experience, none with CLOUD technologies	**6**(29)	21%
0 – 10 years experience, 0 - 5 years with CLOUD technologies	**5**(29)	17%
More than 10 years of experience, more than 5 years with CLOUD technologies	**13**(29)	45%

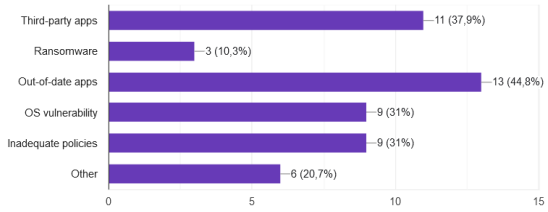

Figure 3: Top breaches causes in cloud environments.

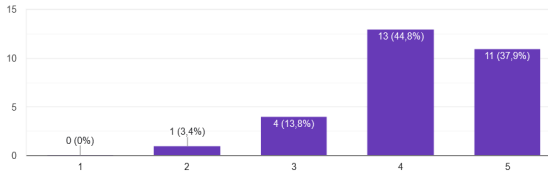

Figure 4: Importance of cloud container images scanning before usage.

Therefore, security issues become the major barrier for further adoption of container as well as cloud computing in general. Outsourced data and services in the cloud environment are subjected to the risks, among which security is a key risk to which a carefully implementation plan must be followed. Usage of security patterns for building secure systems by describing ways to control specific threats fixes vulnerabilities and provides a safe environment for proper utilization of cloud services (see Figure 3).

5.1. Recommendations and future work

As the next, step, an analysis of the international sample has to be performed. For this purpose, one should obtain interviewees who were based in other countries, so as to see if there is significant difference between the analyzed sample in this paper and the internationally-based one. If yes, the aim would be to determine the differences and try to focus on the creation of the overall recommendations for creating methodology for cloud containers assessment in herms of security that would be globally applicable.

Regarding differences in cloud providers, there is a lack of standardized approaches for examination of relevant parts of cloud infrastructures. Variety of realization styles behind cloud services, such as APIs, management tools as well as cloud strategies makes it difficult to explore, but at the same time put a challenge to researchers to make further research to overcome this issue. Either by questionnaire or automatic assessments, revealing detailed key differences between cloud providers will go toward creation of unique approach for their assessments.

5.2. Conclusion

This paper indicated that even though commercially-driven advancements in the a novel scientific field such as CLOUD security, there is not an overall consensus on creating a unique methodology for using tools which involve the binding application or at least common frameworks, in terms of security in the cloud. The survey results analyzed in the paper indicated security patterns for building secure systems and that previous inspection on cloud container images before the utilization is significant for creating prospective methodologies.

The comparison of the results with the literature indicates that a real cloud threat incident analysis is necessary to get more specific results on particular cloud environments in the future and advance towards creating a methodological framework.

References

[1] 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.

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

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

[4] K. Hashizume, D. G. Rosado, E. Fernández-Medina, E. B. Fernandez, An analysis of security issues for cloud computing, Journal of internet services and applications 4 (2013) 1–13.

[5] H. Takabi, J. B. Joshi, G.-J. Ahn, Security and privacy challenges in cloud computing environments, IEEE Security & Privacy 8 (2010) 24–31.

[6] M. U. Shankarwar, A. V. Pawar, Security and privacy in cloud computing: A survey, in: Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014: Volume 2, Springer, 2015, pp. 1–11.

[7] C. Security, the Shared Responsibility Model with CIS, Center for Internet Security (CIS), 2022. URL: CenterforInternetSecurity(CIS) ,CloudSecurityandtheSharedResponsibilityModelwithCIS, (2022),.

[8] N. H. Hussein, A. Khalid, A survey of cloud computing security challenges and solutions, International Journal of Computer Science and Information Security 14 (2016) 52.

[9] 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.

[10] A. Newcomb, Sysdig, container security and usage report, 2021. URL: https://sysdig.com/blog/sysdig-2021-container-security-usage-report/.