EasyChair Preprint

№ 9365

Uses of Languages in Cloud Computing in Context with Its Security

Mathira Mathel, Krishna Chahudry and Fatima Tahir

November 25, 2022

Uses of Languages in Cloud Computing in Context with its Security

Mathira Mathel, Krishna Chahudry, Fatima Tahir

Abstract

Cloud computing is increasingly used, both by individuals and by businesses. The latter use it for several purposes, for example to store data or to outsource part of the company's software architecture. In this case, the administrator of the software architecture must be able to express his security needs, i.e. define which resources to protect and which actions authorized or prohibited on these resources. A need for security can for example be the need to guarantee the confidentiality of a file, in other words to control which users can access the information of this file, or the confidentiality of a connection between two remote services, i.e. ensuring that the information exchanged between these two services cannot be read by a third party entity.

Keywords: Cloud Computing, Languages,

1. Introduction

Cloud Computing is an emerging technology of this century[1, 2].A language for expressing security needs that can be used in a heterogeneous and dynamic environment must have specific characteristics. This section details the needs that our language must meet. First, a heterogeneous environment implies that the different nodes can use different operating systems. Therefore, resources can follow different naming conventions and the security mechanisms are not necessarily the same[3-5]. It is therefore necessary for language to be able to abstract itself from these two elements. On a system, resources are associated with

an identifier (their name or their path). This identifier depends on the system on which the policy is deployed, it cannot be used to identify resources in our language. Consequently, the language uses the notion of contexts in order to abstract itself from the resource naming system systems[6, 7] , which allows the language to be resource independent. In addition, the security mechanisms used to meet security needs do not are not identical according to the systems or the layers of the system. This is why a language expression of security needs for a heterogeneous environment must be independent of the mechanisms. The language must therefore abstract the security mechanisms and their features using capabilities. It will thus be possible to express needs without specifying which mechanisms will meet them. Thanks to this independence of the mechanisms, the language can also be adaptive: it can adapt to the mechanisms present to offer the best possible protection.

II. Context

Definition of contexts

In the context of cloud computing, the systems to be protected can be heterogeneous[8]. Therefore, a security policy aimed at protecting all systems involved should be as independent of the system as possible, which implies that the language must also be independent of the system[9, 10]. For this reason, the proposed language is based on the notion of contexts associated with the resources to be protected. Indeed, by using contexts to identify resources, it is possible to abstract oneself from their system of naming. This allows the same security policy to be applied on nodes having different operating systems or on different applications but offering the same services: the policy can thus be portable[11, 12].

A context is a character string identifying resources independently of the naming systems used (i.e. resource name or path). The contexts are therefore independent of the system. They can be used on heterogeneous systems where the same resource is named in different ways. A context is made up of a set of attributes. An attribute is the association of a key and a value, denoted key="value", represented in the form of a character string. An attribute provides information about the identified resource.

Conclusion:

This research defined a language for expressing security needs that meets the specific characteristics of cloud computing. Two views are possible for this speech. The first view is the one offered to a security expert: it allows him to administer property definitions from capabilities. These capabilities are the chosen solution to abstract the functionality of security mechanisms and obtain properties independent of the underlying mechanisms. The second view is used by the administrator of the software architecture. He can thus define a security policy by using the prototypes of properties that involve contexts. Contexts are representations abstracted from the real resources, which make it possible to abstract oneself from the operating system or apps used. The policy is therefore independent of both the mechanisms and the system, since the capacities/mechanisms and contexts/resources links do not impact defining properties.

References:

[1] S. Achar, "Cloud-based System Design," *International Journal of All Research Education and Scientific Methods (IJARESM),* vol. 7, no. 8, pp. 23-30, 2019.
[2] S. Achar, "Requirement of Cloud Analytics and Distributed Cloud Computing: An Initial Overview."
[3] S. Azhad and M. S. Rao, "Ensuring Data Storage Security in Cloud Computing."
[4] B. R. Kandukuri, V. R. Paturi, and A. Rakshit, "Cloud security issues," in *Services Computing, 2009. SCC'09. IEEE International Conference on*, 2009: IEEE, pp. 517-520.
[5] S. Achar, "Software as a Service (SaaS) as Cloud Computing: Security and Risk vs. Technological Complexity," *Engineering International,* vol. 4, no. 2, pp. 79-88, 2016.
[6] S. Achar and N. Mazher, "Practices and Limitations of Public Cloud Contracts," vol. 4, ed: International Research Journal of Modernization in Engineering Technology and Science, 2022.
[7] S. Achar and N. Mazher, "A Qualitative Survey on Cloud Computing Migration Requirements and their Consequences," vol. 4, ed: International Research Journal of Modernization in Engineering Technology and Science, 2022.
[8] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," *NIST special publication,* vol. 800, no. 145, p. 7, 2011.
[9] S. Achar, "A Comprehensive Study of Current and Future Trends in Cloud Forensics."
[10] S. Achar, "Enterprise SaaS Workloads on New-Generation Infrastructure-as-Code (IaC) on Multi-Cloud Platforms," *Global Disclosure of Economics and Business,* vol. 10, no. 2, pp. 55-74, 2021.
[11] R. T. Williams, "The paradigm wars: Is MMR really a solution?," *American Journal of Trade and Policy,* vol. 7, no. 3, pp. 79-84, 2020.
[12] W. Ambrose, S. Athley, and N. Dagland, "Cloud Computing: Security Risks, SLA, and Trust," 2010.