EasyChair Preprint

№ 9364

Language Responses of Shortcomings Associated with Architecture Capabilities

Fatima Tahir and Laib Ghafoor

November 25, 2022

Language Responses of Shortcomings Associated with Architecture Capabilities

Fatima Tahir, Laraib Ghafoor

Abstract

In this research we propose a language that responds to these various shortcomings, associated with an architecture capable of interpreting this language. So the language proposed must make it possible to define a security and insurance policy that is adapted to cloud environments: this policy must therefore be as independent as possible. possible of the system and the underlying mechanisms. The architecture should be capable of applying this policy by configuring the security mechanisms present. In Indeed, the objective of the architecture is not to propose a new security mechanism, but to reuse the functionalities of the many existing mechanisms to cover a wide range of needs. In addition, the architecture must be able to adapt to the mechanisms available for the projection of the properties and to reconfigure the mechanisms in failure of one of them.

Keywords: Cloud Computing,

Introduction

First of all, the proposed solution must make it possible to express the security needs of a software architecture hosted in a cloud infrastructure[1]. As the cloud is a heterogeneous environment, the solution must be system independent to which the policy applies[2, 3]. Moreover, in order to cover a wide spectrum of systems and of security needs, we propose to reuse existing security mechanisms since there are currently a large number of them, each one specializing in the

application of a subset of properties[4]. In addition, the various machines to be secured do not not necessarily have the same security echanisms: the solution must abstract the mechanisms so that security needs can be expressed without depending on them explicitly. The second objective of this thesis concerns the updating of the protection throughout machine life. Indeed, the solution must be able to detect changes producing on the system and harming the proper application of the needs (unavailability of a mechanism, problem when applying a property, etc.). When such an event is detected, the proposed solution must also be able to react in order to continue to meet security needs. Finally, the solution must propose an evaluation method the quality of the application, in order to be able to easily compare the application of the same policy on different machines or on a single machine over time[5-7].

The thesis provides an implementation of this architecture. This implementation is able to interpret all of the proposed language in order to apply and ensure a policy. It can also perform the automatic reconfiguration and evaluation phases. It has been tested as part of the Seed4C project on several industrial use cases as well as only in an experiment presented in this document.

II. Related Work

Security properties are the basis for expressing security needs. The set of security properties is commonly seen as a set derived from three main properties: confidentiality, integrity and avail ability CIA: Confidentiality, Integrity, Availability)[8]. The exact interpretation of what these three properties imply varies according to the context of use, but their definition and application are part

essential part of the security evaluation criteria, at the European level and international . Several definitions of these properties exist in the literature we resent here a synthesis.

Historical models

Some security properties, previously defined, can be applied by access control mechanisms[9, 10]. In this section, we therefore detail models of historical access control, which introduced the concepts subsequently taken up by various security policy templates. An access control system is usually modeled using the following three elements: – a set of subjects which are the active entities of the system (for example, the process) ; – a set of objects which are the passive entities of the system, on which the subjects can perform actions (files, sockets, etc.); – a set of permissions that represent the actions allowed between a subject and an object (reading, writing, etc.), or between two subjects (sending a signal). Discretionary Access Control Discretionary Access Control (DAC) is the historical model present by default on the majority of Operating systems. In this model, the management of access rights to a resource is left to the discretion of the owner of this resource. For example, under Unix, the owner of a file can set read, write and execute permissions for himself, for members of the group owning the file, and for all others system users. An access control model can be represented as a matrix, where a line represents a topic, a column represents an object or topic, and each item in the matrix represents a set of subject permissions on the object (or on the second subject). This model was formalized by [11]using the Capability Lists and Access Control Lists (ACLs). He proposes therefore to indicate, in a matrix A, the set D of protection domains (representing program execution contexts, i.e. subjects) on the lines, and the set X of objects on the columns.

Lampson therefore defines the lists of capabilities [9, 12-15] which establish the permissions of a domain d on the set of objects o of the system. It is therefore the set of actions authorized for each domain.

Conclusion:

Cloud computing is an increasingly heterogeneous and dynamic type of environment.

additionally used. Different service and deployment models exist and allow to meet a variety of user needs. The combination of an environment heterogeneous and numerous user applications makes security an essential point but complex to address. Defining security needs can indeed be a task difficult, especially since the user of the service does not necessarily know these needs. However, we have seen that there are risk analysis methods that allow a user to determine his security needs. Thus, in the remainder of this document, we will consider that the user of the service is able to establish the list of his needs, if necessary using one of these methods.

Reference:

[1] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE'08*, 2008: Ieee, pp. 1-10.

[2] S. Achar, "Requirement of Cloud Analytics and Distributed Cloud Computing: An Initial Overview."

[3] S. Achar, "Asthma Patients' Cloud-Based Health Tracking and Monitoring System in Designed Flashpoint," *Malaysian Journal of Medical and Biological Research,* vol. 4, no. 2, pp. 159-166, 2017.

[4] C. Binnig, D. Kossmann, T. Kraska, and S. Loesing, "How is the weather tomorrow?: towards a benchmark for the cloud," in *Proceedings of the Second International Workshop on Testing Database Systems*, 2009: ACM, p. 9.

[5] S. Achar, "Cloud Computing Forensics," *International Journal of Computer Engineering and Technology,* vol. 13, no. 3, 2022.
[6] S. Achar, "Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape," *International Journal of Computer and Systems Engineering,* vol. 16, no. 9, pp. 379-384, 2022.
[7] S. Achar, "Science Gateways: Accelerating Research For Cloud Infrastructure," *International Journal of Information Technology (IJIT),* vol. 3, no. 1, 2022.
[8] R. Chow *et al.*, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009: ACM, pp. 85-90.
[9] S. Achar, "Early Consequences Regarding the Impact of Artificial Intelligence on International Trade," *American Journal of Trade and Policy,* vol. 6, no. 3, pp. 119-126, 2019.
[10] 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.
[11] A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm, "What's inside the Cloud? An architectural map of the Cloud landscape," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009: IEEE Computer Society, pp. 23-31.
[12] S. Achar, "Influence of IoT Technology on Environmental Monitoring," *Asia Pacific Journal of Energy and Environment,* vol. 7, no. 2, pp. 87-92, 2020.
[13] S. Achar, "Cloud-based System Design," *International Journal of All Research Education and Scientific Methods (IJARESM),* vol. 7, no. 8, pp. 23-30, 2019.
[14] S. Achar, "AN OVERVIEW OF ENVIRONMENTAL SCALABILITY AND SECURITY IN HYBRID CLOUD INFRASTRUCTURE DESIGNS."
[15] S. Achar, "Security of Accounting Data in Cloud Computing: A Conceptual Review," *Asian Accounting and Auditing Advancement,* vol. 9, no. 1, pp. 60-72, 2018.